Marianne Wade
Almir Maljević
Editors

A War on Terror?

The European Stance on a New Threat, Changing Laws and Human Rights Implications

Springer

A War on Terror?

Marianne Wade • Almir Maljević
Editors

A War on Terror?

The European Stance on a New Threat, Changing Laws and Human Rights Implications

Springer

Editors
Marianne Wade
Max Planck Institute for Foreign
and International Criminal Law
Freiburg, Germany
m.wade@mpicc.de

Almir Maljević
University of Sarajevo
Sarajevo
Bosnia-Herzegovina
a.maljevic@mpicc.de

ISBN 978-0-387-89290-0 e-ISBN 978-0-387-89291-7
DOI 10.1007/978-0-387-89291-7
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2009930643

For all those who suffer because of terrorism including those who face the terror of anti-terrorist measures

For H.W.R. in memoria

And for Noodle: may all those who face dark nights be blessed with such a bright light

Contents

Contributors

Hans-Jörg Albrecht is currently Director at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany and teaches criminal law, criminal justice and criminology at the University of Freiburg. Furthermore, he is a guest professor at the Center for Criminal Law and Criminal Justice at the China University of Political Science and Law, Beijing, Law Faculty of Hainan University, Law Faculty of Renmin University of China, Beijing, Law Faculty of Wuhan University and Law Faculty of Beijing Normal University. He has life membership at the Clare Hall College at Cambridge University, and professorship and permanent faculty membership at the Faculty of Law of Qom High Education Center in Teheran, Iran. His research interests include sentencing theory, juvenile crime, drug policies, environmental crime and organized crime, evaluation research and systems of criminal sanctions.

Dr. Phillip W. Brunst is a Senior Researcher at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany where he heads the information law and legal informatics section. In recent research projects, Phillip has analysed the balancing act of the right to anonymity in the Internet and its effects on effective prosecution, the dangers of cyberterrorism and various forms of transborder cyber crime as well as international instruments against them.

Olivier Cahn is a Lecturer in the School of Law at the University of Cergy-Pontoise and a Fellow of Canterbury Christ Church University (UK) and the University Robert Schuman, Strasbourg. He is also a Researcher at the Centre de Droit Pénal of the University of Cergy-Pontoise as well as an Associate Researcher at the Centre de Recherches et d'Etudes sur les Droits Fondamentaux at the University of Paris Ouest - Nanterre La Défense. His research interests include the treatment of juveniles, judicial co-operation in the EU and British anti-terrorism law.

Mariangeles Catalina Benavente is an Assistant in the Procedural Law Department and member of the Alonso Martinez University Institute for Justice and Litigatio at the Carlos III University in Madrid. Her current research is focused on the restriction of fundamental rights in the fight against terrorism.

Tufyal Choudhury is a Lecturer in the Law School of Durham University in England and a Research Associate at the Oxford University Centre on Migration Policy and Society. He is also a senior policy advisor to the Open Society Institute's Muslims in EU Cities Project and was commissioned by the UK government for a report on *Muslim Identity Politics and Radicalisation*.

Davor Derenčinović is an Associate Professor of Criminal Law in the Faculty of Law at the University of Zagreb. He is a former Fulbright post-doctoral researcher and lecturer at the International Human Rights Law Institute at DePaul University in Chicago, IL. Currently, he is the Secretary General of the Croatian Academy of Legal Sciences, a member of the Parliamentary Committee for Legislation (Croatian Parliament), and Head of the National Delegation in European Committee for Legal Co-operation (Council of Europe – CDCJ). He is the author of ten books and more than 50 articles on various topics of substantive criminal law and international criminal law.

Marc Engelhart is a Researcher at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany where he is also working on his doctoral thesis. He obtained his law degree from the University of Freiburg in 2003 after studying in Freiburg and Edinburgh. In 2005, he passed his second state examination in law after working inter alia for the Federal Ministry of Justice in Berlin. His research interests are in the areas of criminal procedure law, international and economic criminal law.

Susanne Forster is the Head of Section for the United Kingdom and the Republic of Ireland at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany. Since she joined the Institute in 2005, she has contributed to several projects on comparative criminal law. Furthermore, she is pursuing doctoral research on the UK's anti-terrorism legislation and its impact on human rights. She is a German-qualified lawyer and received her LL.M. from the University of Edinburgh.

Annette L. Herz studied law at the University of Heidelberg in Germany and the University of Bordeaux in France. In 2001, she received a Master of Law Degree (LL.M.) from the University of Edinburgh in Scotland. From 2002 to 2005, she was a research assistant at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany. Since 2005, she has been the Assistant to the Managing Board of the Bundeskriminalamt in Wiesbaden, Germany. Her research projects and publications are on the subjects of trafficking in human beings, criminal investigation methods as well as criminal policy.

Wolfgang Hetzer was the Head of Unit at the Federal Chancellor's Office between 2000 and 2002. Since 2002, he has been the Head of Unit of the Intelligence: Strategic Assessment & Analysis in the European Anti-Fraud Office (OLAF). He is the author of numerous publications on organised crime, money laundering, economic law, police law, secret services and European criminal law.

Michael Kilchling is a senior researcher in the Department of Criminology at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany. His main research interests include organized crime, money laundering and the financing of terrorism, confiscation and asset recovery, penal sanctions and sanctioning systems, victim/offender mediation and other forms of restorative justice, victimology and juvenile justice. He lectures on criminal law, criminology and penology at the Faculty of Law at the University of Freiburg, and as guest lecturer abroad. He has been a member of several international expert groups such as the Crime Proofing Steering Group of the EU Commission, DG Justice and Home Affairs, and the Group of Specialists on Assistance to Victims and Prevention of Victimisation at the Council of Europe, which prepared Recommendation R(2006)8 on Assistance to Crime Victims. In December 2005, he worked at the International Monetary Fund in Washington, DC, as a visiting expert on European legislation on asset confiscation. Currently, he is a member of the informal working group of the European Commission on seizure, confiscation, freezing and asset recovery. Further information is available at http://www.mpicc.de/ww/de/pub/home/kilchling.htm.

Damjan Korošec is a Professor of Criminal Law in the Faculty of Law at the University of Ljubljana in Slovenia. He has held a scholarship of the Alexander von Humboldt Foundation for research in Germany (at the Max Planck Institute for International and Foreign Criminal Law in Freiburg, 2003–2004) in the field of International Criminal Law and several Research Scholarships of the Max Planck Society in Germany.

Almir Maljević is a Senior Lecturer of Criminal Law in the Faculty of Criminal Justice Sciences at the University of Sarajevo and an Associate Researcher at the Max Planck Institute for Foreign and International Criminal Law. He is co-editor of the Cross-Border-Crime Colloquium Series as well as the Victimologist. His research interests include criminal collectives and conspiracy, organised criminal activities, police corruption, money laundering and juvenile delinquency.

Víctor Moreno Catena is a Professor of Procedural Law and the Director of the Alonso Martinez University Institute for Justice and Litigation at the Carlos III University in Madrid. He is also a standing member of the Spanish General Codification Commission. He is currently working on the reform of the Spanish Criminal Procedure Code and is the head researcher of a Science and Technology Department grant-maintained team that is working on the restriction of freedom rights in trials for terrorism.

Paul J. Rabbat holds an LL.B. from the Université de Montréal as well as an LL.M. in International Criminal Law from the University of Sussex. From 2005 to 2008, he worked at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany where he was Head of Section for International Criminal Law. During this period, he also lectured at the Law Faculty of the University of Mannheim.

In September 2008, following the completion of his contribution to this book, he accepted a position as Associate Terrorism Prevention Expert at the Terrorism Prevention Branch of United Nations Office on Drugs and Crime in Vienna.

Ulrich Sieber is Director at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany, an honorary professor and faculty member at the law faculties of the Albert Ludwigs University of Freiburg and the Ludwig Maximilian University of Munich, as well as guest professor at the Renmin University of Beijing, the Beijing Normal University and the University of Wuhan in China. He is the president of the German Association for European Criminal Law, the speaker of the International Max Planck Research School for Comparative Criminal Law in Freiburg, a member of the board of directors of the International Association of Penal Law (AIDP) and vice-president of the Association Internationale pour la Défence Sociale. His main areas of research deal with the changing face of crime, criminal law and legal policy in today's global risk society. His major project areas are comparative criminal law and European criminal law, especially with respect to organized crime, terrorism, economic crime and cybercrime. For more details and publications, see http://www.mpicc.de/sieber.

Tony Smith is a Pro Vice-Chancellor (Government Relations) and Dean of Law at the Victoria University of Wellington as well as the Director of the NZ Centre for Public Law. Previously, he was a Cambridge University Professor of Criminal and Public Law and a Fellow of Gonville and Caius College. He is the author or joint author of numerous books and articles. He was a Member of the International Panel of Advisers in the Appeal of Abdulbasset Al Megrahi (Lockerbie) at Camp Zeist, Holland. He is on the Editorial Boards of the journals, *Criminal Law Review*, *Cambridge Law Journal* and *Journal of Financial Crime.* He is also a barrister and Honorary Bencher of the Middle Temple.

John R. Spencer is a Professor of Law at the University of Cambridge. His interests include criminal law, criminal evidence and comparative criminal procedure. He is a QC (honoris causa), an Academic Bencher of the Inner Temple, and holds an Honorary Degree from the University of Poitiers.

Jürgen Stock is Deputy Head of Section at the Bundeskriminalamt (BKA - German Federal Police) and a visiting professor for criminology and criminal science at the School of Law of the Julius Liebig University in Giessen. He has had a full professorship since February 1998 and was the founding rector of the Police College for Higher Professional Training in Saxony-Anhalt. Since November 2007, he has been the elected Vice-President for Europe on the Executive Committee of ICPO-Interpol. He is a member of the Institute for Criminology at the Justus Liebig University in Giessen, a member of the American Society of Criminology and the European Society of Criminology and a member of the managing board of the New Criminological Society. He has lectured and has carried out research in the United States and the Middle East and is the recipient of research prizes from the University

of Giessen and the Police Management Academy in Muenster. He is also the author of numerous publications on the subjects of criminology, criminal proceedings and police science.

Marianne Wade is a senior researcher at the Max Planck Institute for Foreign and International Criminal Law where she works in the European Criminal Law Section. Her work focuses on structural development of a European criminal justice system, the potential of a European public prosecutor as well as of the supra-national law as a whole. She has previously completed a comparative study on the role of prosecution services in national criminal justice systems alongside projects concerning terrorism and surveillance.

Thomas Wahl joined the European Criminal Law Section of the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany in 2004. Since October 2005, he has been Head of the Department. The general focus of his research is on dealing with the legal instruments adopted at the level of the European Union and the Council of Europe, especially those which harmonise criminal law, foster mutual cooperation between law enforcement authorities and establish the central players responsible for the deduction, investigation, prosecution and prevention of crime. At present, his main fields of research concentrate on mutual legal assistance in criminal matters, data protection in police and judicial co-operation in Europe and terrorism-related aspects of the European Union.

Sabina Zgaga studied law at the Faculty of Law at the University of Ljubljana in Slovenia. She served her apprenticeship at the High Court of Ljubljana. Currently, she is a Ph.D. student and works as a research assistant at the Chair for Criminal Law at the Faculty of Law at the University of Ljubljana in the field of international criminal law, substantive criminal law and criminal procedure.

Introduction

Marianne Wade and Almir Maljević

Although the worries about terrorism paled in comparison to the economic crisis as a topic during the last US election, one can find plenty of grounds to assume that they remain issue number one in the minds of politicians in Europe. As the German houses of Parliament prepare to call in the mediation committee in the discussion of legislation which would provide the Federal Police – thus far mandated purely with the post-facto investigation of crime – with powers to act to prevent acts of terrorism, Spain's struggle with ETA and the British Government licks its wounds after a resounding defeat of its latest anti-terrorist proposals by the House of Lords, one cannot but wonder whether post 9/11, the Europeans are not even more concerned with terrorism than their US counterparts. A look at media reports, legislative and judicial activities in either Britain or Germany clearly underlines that those two countries are deeply embroiled in anti-terrorist activity. Can it be that Europe is embroiled in the "War on Terror"; constantly providing for new arms in this conflict? Or is it a refusal to participate in the "War on Terror" that fuels a constant need for Parliaments to grapple with the subject; begrudgingly conceding one increasingly draconian measure after the other? The question as to where Europe stands in the "War on Terror" is a fascinating one, but one, which is difficult to answer.

Discourse on terrorism, even when held firmly within the bounds of criminal law, have been fundamentally marked by the discussion of the "War on Terror" declared by the outgoing US administration in reaction to the attacks of the 11 September 2001. Even Council of Europe and European Parliament reports focus on US practices and European acquiescence to it.[1] Academic debate in Europe has been marked by references to the blurring of boundaries, the erosion of old legal

M. Wade (✉)
European Criminal Law Section, Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: m.wade@mpicc.de

[1] *See* in particular paragraph 80 of the European Parliament Resolution; *see also* http://www.europarl.europa.eu/ sides/getDoc.do?type = IM-PRESS&reference = 20070209IPR02947&language = EN

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_1, © Springer Science+Business Media, LLC 2010

categories, and the appearance of new ones; amongst other things the discussion has focused on the genesis of war in criminal law.[2]

The assumption is often of a general trend though interestingly analysis frequently centres on international agreements or, above all, developments within the USA or possibly the UK.[3] In reading, one frequently gains the impression of overall flux and fundamental change, though one is not always presented with specific examples of such change aside from the two jurisdictions mentioned.

Given that even the vocabulary of the "War on Terror" has been controversial within the European context, the necessity of exploring more deeply the actual changes made to legal orders in Europe appeared self-evident. Whilst the importance and impact of US policy in the anti-terrorist area is undeniable, it seemed meaningful to identify a debate not dominated by the extremes of that context, to enable discovery of whether European nations are actually embroiled in a "War on Terror," whether and how the fundaments of their broader punitive legal systems are changing as a response to the current terrorist threat.

An initial attempt to approach this debate was made in a special edition of the European Journal on Criminal Policy and Research,[4] and it is continued and deepened here. Even within this setting, it remains a piecemeal and non-comprehensive effort. Whilst attempts were made to ensure a spread of countries were represented and a number of important issues addressed, this volume can only cover legal orders representative of the circles found within Europe, and it proved impossible to cover all major issues. The financing of terrorism and the participation of private security firms are two aspects to which this book can not extend though they deserve focal attention.

One central feature of this book, however, is that alongside striving to depict the variety of approaches to terrorism identifiable across Europe, it also recognises the "Europeanisation" of this issue. It is interesting to note that the ferocious debate surrounding criminal justice matters at European Union level is paralleled by quieter harmony in relation to terrorism. Whilst the Member States are unable to agree whether EU structures provide the competence for a Framework Decision on Procedural Rights in Criminal Proceedings (even in the most watered down of forms), they have unanimously assigned the European Police Office (Europol) responsibility for assessing Europe's collective vulnerability.[5] The influence of international organisations, the EU in particular, and their impact upon anti-terror work in the region is explored fully to provide an overview of how much unity such a threat can bring into our diversity.

The book is structured to explore developments in Europe from a variety of angles: the perspective of a new threat (Sect. 1) which might warrant the declaration of a "War on Terror," the emergence of new, supra-national actors and law-makers

[2] *See*, e.g., Sieber (2008), Jacobs (2004); Segato and Origgi (2009).

[3] For example, Gearty (2006) p. 105; Warbrick (2004), notable exceptions are provided by Beckman (2007); von Hippel (2005); and Walter et al (2004).

[4] Wade (2007).

[5] *See* Europol (2008).

(Sect. 2) influencing the national responses to terrorism (Sect. III), the process of change within individual European legal orders, and the consequence these changes have for human rights protection throughout Europe (Sect. IV).

1 A New Threat?

The new threat is linked above all to the nature and ferocity of Al-Qaeda, the organisation's stated aim being to kill as many of its enemies as possible, including civilians.[6] In other words, whilst one may argue about the existence of "new" terrorism [and indeed the largest number of threats stem from other forms terrorism than Islamist, see Europol (2008) p. 16], the threat potential of the extremist Islamist terrorism, which currently dominates our concern, is greatly enhanced by the intent that such acts cause mass casualties and – central to the associated policing nightmare – by the perpetrators' willingness to sacrifice their own lives in committing these acts.[7] Furthermore, the threat is non-specific in attacking a lifestyle and thus a much broader group of countries or their citizens anywhere. The threat potential is international because of a certain random nature stemming from by the breadth of defined legitimate targets.[8] The US's closest allies see themselves as particularly and most obviously threatened[9] but there can be little doubt that an increased threat is perceived across Europe, even amongst countries opposed to the Iraq war. This book thus gathers information from a number of less-discussed jurisdictions. In addressing the new threat centrally, it focuses on Germany, a state which is perhaps exemplary of those striving for a very different path than that embraced by the "War on Terror" and potential new threat forms.

This collection thus opens with threat analyses examining the new threat posed by terrorism: *Stock and Herz* provide a threat assessment from the point of view of the German Federal Police, one of interest because it represents not only the perspective of Europe's largest state and, arguably, geographic heart but also the threat as seen through the eyes of a service not strongly accustomed to a terrorist threat in recent times and a regime not strongly embroiled in the "War on Terror." Indeed the German government of the time gained a high profile for its opposition to US policy, and German military participation in NATO troops in Afghanistan regularly meets criticism for the restrictions placed on it. Nevertheless, even this country sees itself exposed to a serious threat by international terrorists.

---

[6] *See* Laqueur (2004); and with the characteristics of principled evil-doers, thus harder to deter and deal with – Tesón (2005), p. 70–3.

[7] Spence (2007), p. 5; *see also* Cornish (2005), p. 147 et seq.

[8] *See*, e.g., al-Zawahiri's threat to France and Germany cited by Szyszkowitz (2005), p. 45.

[9] For an assessment of the threat to the UK, *see* Wilkinson (2007a) p. 31. Assessing the situation of other European countries in accordance with the criteria presented is also sadly illuminating. For a more detailed assessment, *see* Makarenko (2007).

Brunst underlines the universal threat of terrorist activity portraying the potential dangers presented by terrorist use of the internet. His contribution clearly illustrates the difficulties faced by national law enforcement communities in combating a potentially technically complex, borderless threat which may seek to strike in a number of ways at a variety of targets. The threat potential of the internet be it as fund-raising medium and means to actual attacks is a very modern aspect of the threat scenario as currently assessed.

Attempts to summarise the European reaction to this threat have come to conclusions such as the following: "If there is a common European stance on counter-terrorism, it is based on the idea that the fight against terror is a matter of law enforcement, not the "war" that is claimed by the Bush administration."[10] Thus, one would not expect any legal changes as radical as those seen in the USA – indeed of the 46 Council of Europe member states, only the UK has derogated from the European Convention on Human Rights since 2001.[11] Nevertheless, the disparity of perceived threats and sense of appropriate reaction has been regarded as the hampering factor to a co-ordinated EU response (though by 2007 this had, apparently, largely been overcome[12]). So far academic work on European reaction to the current terrorist threat has traced changes in Germany,[13] France,[14] and Italy,[15] a notable virtual non-reaction in Spain,[16] structural and cultural though not legal change in Greece,[17] and to a lesser extent in the Nordic countries[18] with Turkey as focussing on quite different terrorist threats.[19]

2 Supra-National Actors

Recent years have seen a decisive response to such threats through the forming or strengthening of law enforcement communities that, like the perceived threat, transcend the traditional national boundaries of criminal justice systems. These are tackled in the book's second section: the international front. Above all, this section recounts and analyses the actions of major international organisations that have

[10] Dworkin (2008); Warbrick (2004), p. 6; for a taste of this difference, *see*, e.g., French Foreign Minister Hubert Vidrine quoted in von Hippel (2005) p. 2. Note, however, that some European leaders were willing to embrace the idea of a "war on terrorism" but not a war against Iraq – *see* O'Brien (2005), p. 19; Myrdal (2005), p. 103; Ramos (2005), p. 128.

[11] Zedner (2005), p. 523.

[12] *See* Spence (2007), p. 1–3.

[13] Szyszkowitz (2005), p. 48 et seq.

[14] O'Brien (2005), p. 26.

[15] Sagramoso and Nativi (2005), p. 82 et seq.

[16] Ramos (2005), p. 125; though a certain amount of institutional reform is clearly present; Jordán and Horsburgh (2005) 135, 137 et seq.

[17] Dokos (2005), p. 74.

[18] Myrdal (2005), p. 109 et seq.

[19] *See*, e.g., Beckman (2007), especially p. 118 for Spain; Dagron (2004); Rau (2004); Oellers-Frahm (2004); Martínez Soria (2004); and Güney (2004).

provided the framework for supra-national anti-terrorist work. It is particularly in this field that the United Nations has emerged as a legislator and a controversial enforcer of preventive and punitive mechanisms to try to counter the terrorist threat. *Rabbat* reviews this work exploring the still unsettled definition of terrorism,[20] the sanction regime established by Security Council Resolution 1267, and the preventive measures of 1373, the work resulting from that as well as analysing the unprecedented position assumed by the UN in combating terrorism.

This theme is echoed by *Wahl* as he traces the emergence of the EU as an anti-terrorist acteur. Given the great controversy surrounding the very idea of a competence to demand use of the criminal law by the European Communities,[21] one may well be surprised at the extent to which the member states have chosen to concentrate their efforts in combating terrorism within the ambit of the European Union. The numerous measures taken and policy strands being pursued are a significant step towards forming the desired area of freedom, security, justice, as well as a common legal area, and may be taken as indicative of the importance attached to this subject as well as the common need seen and stance taken.

Sieber illustrates the potential of the international organisations in their new roles within and beyond Europe detailing the means and mechanisms found under the umbrella of international organisations to provide for the fight against cyber-terrorism. His contribution illustrates boundaries and hindrances to successful cooperation as well as the potential offered by the European context to overcoming these.

Finally, in this section a common viewpoint and action is analysed by *Albrecht and Kilchling* in their exploration of common efforts to compensate the victims of terrorism. This contribution illustrates the complexity of the topic displaying the need faced by states not only to reach agreement in a defensive or aggressive stance against terrorists but also to display a nuanced solidarity in dealing with longer term, less high-profile issues raised. If the threat against citizens is not only global in origin but also in where it strikes to hit them – tragically illustrated by the recent targeting of UK and US citizens in Mumbai hotels, compensation systems are faced by challenges, which transcend the traditional boundaries and categories of any tort laws.

3 National Responses to Terrorism

The third section provides detail of the ramifications the terrorist threat has had for legal systems across Europe providing analysis of how these have changed in the face of the new threat perceived. The contributors have built on this work detailing great variety of experience ranging from systems in which little has been done beyond the required adaptation of the law in line with the international obligations

[20] For a far-reaching analysis of the many aspects of this point, *see* Saul (2006), in particular pp. 1–9; for the (supra-national) European context, *see* Symeonidou-Kastanidou (2004), p. 14–31.

[21] *See* cases C-176/03 and C-405/05 of the European Court of Justice, and Vervaele (2006) in eucrim, Fromm (2008).

outlined in the previous section (e.g., Slovenia and Croatia) to systems in which fundamental shifts have occurred, placing areas of the criminal law in a war-like context (e.g., the UK). One cannot over-emphasise that Europe consists of a number of very different states, reflected in this section by accounts of the very different approach taken by Spain and the UK in response to 9/11 (the latter's described as parallel to the US approach and thus very different to that foreseen by the European Commission[22] though the more common line found within the EU as well as the Spanish case do provide examples of positions changing).

Whilst *Korošec and Zgaga* and *Derenčinović* in turn portray the situations in Slovenia and Croatia, respectively, as impacted only to a limited extent by the priority lent to the fight against terrorism by fellow European states – the impression is of systems embroiled in controversial debate as to what the legal norms mean for their systems but less deeply affected and indeed fairly untouched by the "War on Terror." *Maljević* portrays the collapse of law in the face of pressure generated by the US "War on Terror." The poignant illustration of a country whose courts robustly reject any such "war" (and indeed whose law is immune to any such scenario) bowing to the desire and pressure to disown its citizens and expose them to a fate of arbitrariness and suffering is the cautionary tale of a European country betraying its tradition and legal mindset. This example at once portrays both the revulsion of European legal principles at the enemy status imposed by the USA on persons via the "War on Terror" and their impotence when confronted by the limitations of realpolitik when a more powerful country declares a war and suspects the less influential country's citizens of complicity.

Readers may draw comfort from *Hetzer's* account of the robust court rejection of such means in relation to the air safety act in Germany. His contribution details the Federal Constitutional Court's refusal to bow to Government desire to weigh the value of a lesser number of citizen's lives against the potential to save many more. One may take heart at the Court and author's clear expression of the difference between law and war and the fact that the German legal order has maintained such principles despite the urgent need felt by some to diverge from it. The argument and indeed this case as well as the attempts at reform by the Government providing for steps towards a certain degree of "War on Terror" detailed may leave one concerned about the health of our legal orders or our commitment to them. This contribution shows them prevailing in some contexts – outside that of emergency, of course – and it is important to recognise that the "War on Terror" is neither accepted nor underway in much of Europe. The broader context, such as reports on illegal renditions,[23] however, clearly displays that the war's darker shadows reach into even the robuster corners of Europe.

Finally, in this section, *Choudhury* illustrates how the language and context of a "war" or indeed even a concerted criminal justice effort to fight a phenomenon on terrorism can have profound effect on communities associated with the threat. In this section, the diversity and complexity of a community – Muslims in the UK – associated with risk and all too often portrayed in broad brushstrokes as a danger is

[22] *See* Watson (2004), p. viii.

[23] *See*, e.g., the Venice report; Kurnatz case.

presented, and the bluntness and destructive nature of instruments such as the "War on Terror" are clearly illustrated. Given that the majority of victims of terrorist attacks are Muslims,[24] the fight against terrorism is displayed as reinforcing the marginalisation of communities struggling to integrate and avoid the traps of deprivation and poverty within wealthy European societies.

4 Human Rights Implications

The final section of this book turns to an analysis of the human rights implications of changes made to European criminal justice systems in response to the terrorist threat clearly identified since the attacks of 2001 (and to a lesser extent though certainly reinforced by the Madrid bombing in 2004, the attacks in London in 2005 and ensuing threats).

Developments are traced in the larger European jurisdictions because of their experience with terrorism of various kinds but also their capacity to participate in the international fight against terrorism. The later, as well as the symbolic potential of any act of terrorism in them, perhaps makes them prime candidates also for future terrorist attacks at least in their Government's eyes.

Of these states, Spain and the UK have experienced direct and tragic victimisation by Islamist terrorists in recent years. It is therefore particularly interesting to contrast the approaches taken. The British situation forms a focal point; this nation having taken up a position at the forefront of the European anti-terror campaign[25] as well as participating in the US "War on Terror." Changes made to the law both within and outside the criminal justice system as well as policies enforced and alterations proposed in the UK, Spain, France, and Germany are analysed in detail.

Forster details the background and current status of perhaps the most controversial of measures to be found within Europe in the anti-terrorist context; the UK control order scheme. Her contribution describes the awkward progress from detention without trial measures directed against foreign citizen the Government is unable to deport (displaying that that this response is in fact a tight-rope walk of security interests in the context of human rights requirements in particular article 3 of the European Convention on Human Rights – though certainly not the one human rights advocates would wish for) to the current scheme that applies to both foreigners and nationals. The robust reaction of the courts to Government measures and their refusal to accept that the UK must submit to a state of war in which high standards of human rights protections do not apply are an illustration of the checks and balances of European legal systems and indeed the potential of court scrutiny.

It is this stringent scrutiny which *Spencer* details the Government as trying to avoid in its desire to force British courts to accept telephone tap evidence without

[24] Aslan (2006) xii et seq.

[25] *See*, e.g., the position adopted by the UK presidency of the EU – *see* The UK Presidency of the EU (2005).

knowing full details of how it was garnered. Although this account provides a snapshot picture of a highly controversial current debate, the end and result of which cannot be foreseen, it provides a valuable insight into the workings of governance in Europe and the mindset of Governments as they attempt to provide for measures they define as necessary within the current terrorist threat context, but which are abhorrent to the legal system as it has stood for decades if not centuries (compare with *Hetzer* for the equivalent efforts of the German government).

Wade analyses such proposals as part of a greater trend that undermines the standing and importance of criminal law alongside the guarantees associated with it; first and foremost, of course, in relation to liberty securing rights on the part of suspects (or anyone associated with suspected terrorist organisations) no longer afforded the privilege of being considered innocent until proven guilty but also in relation to the central function of criminal law: to punish the guilty even-handedly and proportionately to the crimes they make themselves culpable for. In such trends, readers may well recognise a system stretched to its limits, unable to cope with the challenges it faces; thus in flux, shaking at its very foundations with the outcome of such a process unforeseeable.

Smith plots these developments within the context of fundamental constitutional change in Britain, identifying the workings of the mechanisms and various levels of governance in action. He identifies outliers but also their correction by balancing processes and reminds us that Europe has faced greater challenges and indeed developed into what it is today by facing them and finding acceptable solutions to them.

In contrast to UK developments, *Catena* and *Benevente* identify the criminal justice system as the prime mode of the fight against terrorism in Spain. Although their account provides clear evidence of attempts by the Executive to introduce specialist procedures associated with lower standards of protection for fundamental rights, the far-reaching check on such provisions provided by the Constitutional Court (a feature conspicuous only by its absence in the UK though this is set to change in 2010) is impressive. Nevertheless, the exceptional way in which suspected terrorists are treated is evident though this cannot be described as symptomatic of a "War on Terror" but far more the highly specific treatment of suspected criminals considered particularly dangerous. Although the anti-terrorist measures introduced in Spain represent departures from fundamental principles there, in international comparison, it must be stated that these are mechanisms well known in many other criminal justice systems and well rooted in European criminal procedure. Departure from traditional standards of human rights protection is certainly no where near as great in Spain as in the UK.

A similar approach is identified in France by *Cahn*. As a fierce opponent of the "War on Terror," it is not surprising to see that the French Government has gone to some lengths to ensure its measures against suspected terrorists remain well within the realms of ordinary criminal law. Nevertheless, the special treatment afforded to such suspects – as in Spain – must lead one to speculate that these jurisdictions may have declined to declare suspected terrorists to combatants in a war but have nevertheless chosen to treat them as significantly other within their criminal justice systems.

Engelhart explores a fundamental shift in the German system detailing the extent to which intelligence services can become involved in criminal proceedings. Although this contribution displays clearly that there are many hurdles to the inte-

gration of intelligence service information into the criminal process, it is interesting to note that the very robust separation of these institutions of the last 60 years appears to be actively eroded as the roles of institutions and priorities within the system shift in the face of the terrorist threat. Despite the robust approach taken by the system to retaining its constitutional values, here is strong evidence that the current climate is causing a number of fundamental changes.

Although the contributions appear above all to negate the notion of a "War on Terror" in Europe, they must nevertheless be viewed as accounts of great change within Europe caused by the desire to combat the current terrorist threat and placing the traditional legal orders there under strain. Only time will tell what lasting effect the current dynamic in European legal orders will have on them. European societies are deeply affected by the current terrorist threat and communities within them by the policies which seek to counter it. The ramifications of changes made to legal orders as well as emerging supra-national governance systems are likely to affect life in Europe for far longer than one might expect a war of any kind to last. Even if Europe does not wage the "War on Terror," its ramifications are likely to be felt there for generations.

The editors owe thanks to Klaus Krebs, Sarah Schultz, and Wendelin Neubert for their valuable assistance.

References

Aslan, R. (2006) No god but God. New York; Random House.

Beckman, J. (2007) Comparative Legal Approaches to Homeland Security and Anti-Terrorism. Aldershot and Burlington: Ashgate.

O'Brien (2005) France in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Cornish, P. (2005) The United Kingdom in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Judgement in case C-176/03 available under www.curia.eu.int

Judgement in case C-405/05 available under www.curia.eu.int

Dagron, S. (2004) Country Report on France in Walter, C., Vöneky, S., Röben, V., and Schorkopf, F. (eds) Terrorism as a Challenge for National and International Law: Security versus Liberty? Berlin: Springer.

Dokos, T. (2005) Greece in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Dworkin, A. (2008) EU governments should welcome today's ECHR ruling on torture. European Council on Foreign relations commentaries. 28 February. Available at http://www.ecfr.eu/content/entry/commentary_dworkin_on_saadi.htm

Europol (2008) EU Terrorism and Situation Report 2008. The Hague.

Fromm, I. (2008) Urteil 23.10.2007 – C440/05 Rahmenbeschluss 2005/667/JI des Rates vom 12.7.2005 zur Verstärkung des strafrechtlichen Rahmens zur Bekämpfung der Verscmutzungen durch Schiffe ist nichtig. Zeitschrift für internationale Strafrechtsdogmatik, 168–177.

Gearty, C. (2006) Can Human Rights Survive? Cambridge: Cambridge University Press.

Güney, N. (2004) Country Report on Turkey in Walter, C., Vöneky, S., Röben, V., and Schorkopf, F. (eds) Terrorism as a Challenge for National and International Law: Security versus Liberty? Berlin: Springer.

von Hippel, K. (2005) Introduction: Europe Confronts Terrorism in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Jacobs, G. (2004) *Bürgerstrafrecht und Feindstrafrecht.* In: HRRS 3/2004, S. 88–95.

Jordán, J. and Horsburgh, N. (2005) Spain Part II: Islamic Extremism in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Laqueur, W. (ed.) (2004) Translation of World Islamic Front (1998) "Jihad against Jews and Crusaders" pp. 410–12 in Voices of Terror. New York; Reed Press.

Makarenko, T. (2007) International Terrorism and the UK – Assessing the Threat in Wilkinson, P. (ed) (2007) Homeland Security in the UK. London and New York: Routledge.

Martínez Soria, J. (2004) Country Report on Spain in Walter, C., Vöneky, S., Röben, V., and Schorkopf, F. (eds) Terrorism as a Challenge for National and International Law: Security Versus Liberty? Berlin: Springer.

Myrdal, S. (2005) Nordic Responses in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Oellers-Frahm, K. (2004) Country Report on Italy in Walter, C., Vöneky, S., Röben, V., and Schorkopf, F. (eds) Terrorism as a Challenge for National and International Law: Security Versus Liberty? Berlin: Springer.

Ramos, A. (2005) Spain in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Rau, M. (2004) Country Report on Germany in Walter, C., Vöneky, S., Röben, V., and Schorkopf, F. (eds) Terrorism as a Challenge for National and International Law: Security Versus Liberty? Berlin et al: Springer.

Sagramoso, D. and Nativi, A. (2005) Italy in von Hippel, K. (ed) Europe confronts Terrorism, New York: Palgrave Macmillan.

Saul, B. (2006) Defining Terrorism in International Law. Oxford: Oxford University Press.

Sieber, U. (2008) Blurring the Categories of Law and War.

Segato, L. and Origgi, M. (2009) Italy in Sundberg, K. and Winterdyk, J. (eds.) *Transforming Borders in the al-Qaeda Era* Taylor and Francis.

Spence, D. (2007) Introduction: International Terrorism – The Quest for a Coherent EU response. London: John Harper.

Symeonidou-Kastanidou, E. (2004) Defining Terrorism in European Journal of Crime, Criminal Law and Criminal Justice, Vol. 12/1, 14–35.

Szyszkowitz, T. (2005) Germany in von Hippel, K. (ed) Europe Confronts Terrorism. New York: Palgrave Macmillan.

Tesón, F.R. (2005) Liberal Security in Wilson, R.A. (ed) Human Rights in the "War on Terror." Cambridge: Cambridge University Press.

The UK Presidency of the EU (2005) *Justice and Home Affairs Purpose Statement*. Available online at: http://www.eu2005.gov.uk/servlet/Front?pagename = OpenMarket/Xcelerate/ShowPage&c = Page&cid = 1079979841177-

Vervaele, J. (2006) The European Community and Harmonization of the Criminal Law Enforcement of Community Policy. In Eucrim 3–4, 2006, pp. 87–92.

Wade, M. (ed.) (2007) Fear v Freedom – Special Edition of the European Journal on Criminal Policy and Research, 1–2. New York: Springer.

Walter, C., Vöneky, S., Röben, V., and Schorkopf, F. (eds) (2004) Terrorism as a Challenge for National and International Law: Security versus Liberty? Berlin: Springer.

Wilkinson, P. (2007a) The Threat from the Al-Qaeda Network in Wilkinson, P. (ed) Homeland Security in the UK. London and New York: Routledge.

Warbrick, C. (2004) The European Response to Terrorism in an Age of Human Rights, European Journal of International Law, November.

Watson, G. R. (2004) Foreword: The Importance of Transatlantic Dialogue in the Fight against Terrorism in Finjaut, C., Wouters, J., and Naert, F. (eds) Legal Instruments in the Fight Against International Terrorism. Leiden and Boston: Martinus Nijhoff.

Zedner, L. (2005) Securing Liberty in the Face of Terror: Reflections from Criminal Justice, Journal of Law and Society, Vol. 32, No. 4, December, pp. 507–533.

Part I
A New Threat

Chapter 1
International Terrorism – German Police Perspective: The Current Threat Environment and Counterstrategies from the German Police Perspective

Jürgen Stock and Annette L. Herz

1.1 Introduction

International terrorism motivated by Islamist ideology[1] has claimed several thousand victims thus far. Not only the Arab countries and countries with an Islamic tradition are affected. We are repeatedly confronted with attacks in Africa, in South-Eastern and Central Asia, and also in Europe. Following the attacks committed in

J. Stock and A. Herz
e-mail: juergen.stock@bka.bund.de; annette.herz@bka.bund.de

[1]The concept of "Islamism" is employed here – in the manner defined by the security authorities – as designating a religiously motivated form of political extremism. Basically, at the present time, there is no generally recognized (political-)scientific definition of extremist crime or of terrorism as a form of politically motivated crime, because these concepts depend to a greater extent than other crime phenomena on the respective form of government and constitution as well as on any changes that may occur in state interests and/or assessments of protected interests (Eisenberg, 2005, section 45 margin no. 143; Jesse, 2004, p. 8; Singer, *Kriminalistik* 2004, p. 32). Thus, whether a type of conduct is judged to be "extremist" depends on the perspective of the observer. In this connection, the objectives pursued, the means employed the degree of organization, and the relative intensity can serve as criteria for orientation and making judgements (Müller, 2004, p. 486). Political extremism is generally understood as the antithesis of the constitutional democratic state and is used as a collective term for efforts that are directed against the core elements of the free and democratic constitutional system. If this approach is taken, the problem of differentiating between "fight for freedom" and "terrorism" does not arise in a constitutional democracy [Pfahl-Traughber, *Kriminalistik*, 2003, p. 202 (204)]. Another criterion for orientation is provided by Section 46 of the German Penal Code, according to which German criminal law does not treat an individual's political convictions as constituting either justification or grounds for exemption from punishment, but only takes them into account when fixing the penalty [Neubacher, *MschrKrim*, 2002, p. 290 (298)].

One core concept of Islamist ideologies is the idea that the power of the state does not rest with the people who authorize the laws that are in force, but instead the system of government is established by God. This claim to absolutism stands in permanent contradiction to the highest principles of the free and democratic constitutional system such as the sovereignty of the people, the principle of majority rule, or the right to exercise parliamentary opposition. When coupled with a willingness to pursue these goals using violence, the terrorist potential is evident.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_1,

New York, Madrid, and London, but in particular following two attempted attacks within Germany in 2006 and 2007,[2] more than ever before public attention in Germany has been focused on international terrorism. The attacks and attempted attacks within Europe have made two developments clear: On the one hand, it is no longer possible to hope that 11 September 2001 was a one-time occurrence. On the other hand, we can see that international terrorism has arrived in the heart of Europe. Europe – including Germany – is no longer "just" a safe haven for terrorists and a place to make preparations, but is also a theatre of operation.

The threat situation and the images of terror transmitted directly by the media influence the way the public thinks and acts and, last but not least, its subjective feeling of security. For the security authorities, 11 September 2001 revealed a new dimension of vulnerability. When seeking effective countermeasures, the fact that there are no longer any taboos for the perpetrators with regard to their choice of instruments and targets has to be taken into account. Their acts are apparently not limited by any value systems, including that of Islam, and they operate unfettered by any home or social ties. This means that the responsible security authorities have to anticipate attack scenarios whose manner of commission and impacts differ fundamentally from known forms of violence. In view of these new massive threats, the state, as a guarantor of freedom and security, must take all measures feasible provided these do not interfere with the core of the rights to freedom and are not disproportionate with the aspired gain in security.[3]

At the same time, the phenomenon of international terrorism motivated by Islamism cannot be understood by employing simple interpretative and explanatory approaches. Explanations that focus on singular aspects such as theology, ethnicity or socio-economic factors do not go far enough when searching for answers to questions about motivation, ideology, and organizational structure. For example, the victims of Islamist attackers are often Muslims as well that points to internal conflicts in the Islamic world among other things and stands in contradiction to the bold and simple assumption of a "conflict of cultures."

The concept of terrorism, on the one hand, is based on the terrorist organization as defined in sections 129a and 129b of the German Penal Code. In addition, serious politically motivated crimes of violence (offences listed in section 129a of the German Penal Code) – crimes that are committed on the basis of planning as part of a long-term campaign, usually by groups that divide up their tasks and operate covertly – are regarded as terrorism. Parts of section 129a of the German Penal Code can be traced back to the Council Framework Decision of 13 June 2002 on combating terrorism, which strives to harmonize the definitions of terrorist offences in the Member States (OJ L 164 of 22 June 2002, p. 3ff.). According to the Framework Decision, certain serious offences are to be subjected to punishment if, given their nature or context, they may seriously damage a country or an international organization where committed with the aim of seriously intimidating a population, or unduly compelling public authorities or an international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country, or an international organization [Art. 1(1)].

cf. Tröndle/Fischer, 2007, section 129a, margin no. 4 ff.

[2] cf. the comments to be found below in 1.3.2.

[3] Compare Di Fabio, *NJW* 2008, pp. 421–425.

1.2 Early Role of the Bundeskriminalamt, Germany's Federal Criminal Police Office

In Germany, law enforcement and the prevention of criminal offences are generally tasks handled by the police forces of the German states. However, in connection with international terrorism, the Bundeskriminalamt (BKA) has extensive own powers of investigation. Thus, the BKA carries out police law enforcement duties with regard to numerous cases of internationally organized crime – including the formation of terrorist organizations in Germany and abroad (sections 129a, 129b subsection 1 of the German Penal Code), as well as cases involving the criminal offences named in section 129a subsection 1 nos. 1 and 2 of the German Penal Code and related offences – if offences committed outside of Germany are concerned and a jurisdictional venue has not yet been established. The BKA is also responsible for cases of computer sabotage (section 303 of the German Penal Code) if the security of the Federal Republic of Germany or sensitive parts of facilities of vital importance are threatened.[4] In addition, the BKA carries out law enforcement tasks at the request of a state authority, by order of the Federal Minister of the Interior or on behalf of the Office of the Federal Prosecutor General.[5] So far, only when the BKA provided support to Federal or state police forces or the Federal Police (BPOL, previously the Federal Border Guard), did the BKA have preventive powers in its capacity as a central agency.[6]

It is necessary to differentiate between the work of the state criminal police forces and the BKA as opposed to the work of the intelligence services which, irrespective of any penal relevance, act to ward off anti-constitutional activities as well as threats to the security interests of the Federal Republic of Germany.[7] Thus, one of the tasks of the constitutional protection authorities is the collection and analysis of information about security-relevant activities in the Federal Republic of Germany that are anti-constitutional, whereas the Federal Intelligence Service concentrates on intelligence from abroad that is of significance for the foreign policy and security of the Federal Republic of Germany.[8] In contrast to the police authorities, the intelligence services do not have any executive powers and are not bound by the principle of mandatory prosecution.[9]

---

[4]cf. section 4 subsection 1 sentence 1 nos. 3a, 4, and 5 of the BKA Law.

[5]Section 4 subsection 2 sentence 1 of the BKA Law. As to the tasks of the BKA, cf. Kerner/Stierle/Tiedtke, *Kriminalistik* 2006, p. 292 (295 ff.).

[6]Section 2 subsection 1 of the BKA Law. As to current legislative developments, cf. the comments to be found below in 1.5.1.

[7]See Engelhart, this volume.

[8]Section 3 of the Law on the Protection of the Constitution, section 1 of the Law on the Federal Intelligence Service.

[9]Under the principle of mandatory prosecution, public prosecution offices and the police are obliged to take action in relation to all criminal offences which may be prosecuted (section 152 subsection 2 of the German Code of Criminal Procedure).

The present contribution provides a description of both the current threat environment created by international terrorism and the necessary counterstrategies from the German police perspective. It begins by describing the threat represented by the terrorist crime phenomenon in terms of organizational structure, crime profiles, and perpetrator motivation. This is followed by comments on in which form, and to what extent, international terrorism threatens German interests as well as how German legislators have reacted. The focal point of the contribution lies on describing counterstrategies on the part of German security authorities, particularly with regard to the reorientation of the German security architecture. The latter mainly concentrates on strengthening the network that links security authorities among each other and to other players in charge that are already assuming an active role in the fight against international terrorism or those that still have to be sensitized accordingly (holistic approach).

1.3 General Threat Situation

1.3.1 Overall Situation

The attacks committed since the early 1990s by terrorists motivated by Islamist ideology represent a turning point towards a globalization of terrorist activities. Beginning with the first attack on the World Trade Center in New York in 1993, a development can be discerned that has been directed worldwide primarily against the USA, the UK, and Israel and/or Jewish facilities, and reached a high point when the World Trade Center was attacked on 11 September 2001. The subsequent attacks in Madrid on 11 March 2004 and in London on 7 July 2005 plus the attempted attacks in Germany in July 2006 and September 2007 demonstrate that the target spectrum of Islamist terrorist groups has been expanded to cover the entire "Western hemisphere" of democratic countries, including the countries of Western Europe. In addition, the Arab Islamic world continues to be the classical theatre of operation for Islamism and Islamic terrorism.

The military involvement of Western countries in the Arab Islamic world and the counterterrorist measures within Western countries that have resulted from the attacks are used by Islamist extremists for propaganda purposes with a view to gaining the sympathy of moderate Muslims as well. The best-known Islamist group is Al-Qaida (the Base), which was founded in 1988 in Peshawar (Pakistan). Osama Bin Laden, who founded Al-Qaida, made the first attempt to unite the fragmented Islamist movement into a global political power.[10] Al-Qaida's objective is to gradually eliminate American and Western influence in the Islamic countries.[11] In contrast, for example, to the attacks perpetrated by the left-wing extremist Red Army Faction

[10] Tibi, 2002, p. 27 (28). cf. also Klink, 2004, p. 89 (91 ff.); Raisch, *dnp* 2004, p. 30 f.

[11] Müller, 2004, p. 480 (496).

(RAF) in Germany during the 1970s and 1980s, international Islamist terrorism is characterized by a different organizational structure, different crime profiles, and different motives.

1.3.2 Germany

On 31 July 2006, two young Lebanese males, travelling on regional trains towards Hamm and Koblenz, simultaneously activated two explosive devices hidden in suitcases ("Suitcase Bomb Case"). The security agencies determined that despite being ignited the bombs had failed to detonate because of a fault in construction. Subsequent tests revealed that a detonation of the explosive devices would, in both cases, have led to a considerable shock wave together with a fireball. Burned-out carriages, derailed trains, dead and seriously injured persons on open stretches with difficult accessibility for rescue teams would have been the possible consequences. On 18 December 2007, one of the suspects was put on trial at the Higher Regional Court (HRC) of Düsseldorf on charges of attempted murder and attempted causing of an explosion. The other suspect was convicted in Beirut on 18 December 2007 and sentenced to 12 years imprisonment.

On 4 September 2007, at a small location in North Rhine-Westphalia (Oberschlehdorn), German police arrested three young men – that is, two German nationals converted to Islam and one Turkish national – who, as members of the terrorist association Islamic Jihad Union (IJU),[12] were suspected of plotting simultaneous explosive attacks in Germany. Another suspect was arrested in Turkey on 6 November 2007. Further suspects are still under investigation. The plotters, who had not yet precisely fixed the targets, had their sights on facilities primarily frequented by US Americans, such as discotheques, bars/restaurants, or airports. If these attacks had materialized they would most likely have caused hundreds of deaths and casualties. The suspects were found in possession of material for building bombs whose explosive force would have far exceeded those used in the London attacks: 730 kg of hydrogen peroxide with a potential impact of 550 kg of explosives.[13]

---

[12] IJU is an Uzbek organization formed by former members of the Islamic Movement of Uzbekistan (IBU) in March 2002. IJU is regarded as an independent group with close ties to Al-Qaida. The group initially concentrated on regional goals, but has by now expanded its activities to the worldwide Jihad. The IJU staged bomb attacks against the US-American and Israeli embassies in Tashkent, Uzbekistan on 30 July 2004 as well as several other attacks against Uzbek facilities. On 11 September 2007, the security authorities discovered a publication on the Internet in which the IJU claimed responsibility for the planned attacks in Germany. Among other things, it was claimed that the attacks had been intended to be carried out against the Ramstein US-Air Base, against American and Uzbek consulate facilities and against German facilities abroad. The justification given was that both countries were playing a part in the "injustice and the brutal policy against Muslims and the Islam." The IJU's aim had been to keep the German Federal Armed Forces from further using the airport in Termez, Uzbekistan as a hub for their Afghanistan mission.

[13] The London bomb attackers used explosive devices of 2–3 kg.

However, these two attempted attacks were not the first that had been staged from German territory. For instance, in December 2000, an explosives attack on the Strasbourg Christmas market planned by members of the MELIANI group was thwarted. The HRC of Frankfurt sentenced four defendants to terms of imprisonment ranging from 10 to 12 years, among other things for conspiracy to commit murder and to detonate explosives. Members of the now-neutralized Al-Tahwid terrorist cell were sentenced to between four and eight years of imprisonment by the HRC of Düsseldorf for membership in a terrorist organization in connection with plans to attack Jewish facilities in Berlin and Düsseldorf. In November 2005, three presumed members of the Ansar Al-Islam (AAI) ("followers of Islam") organization were charged by the HRC of Stuttgart with having planned an attack on the Iraqi Prime Minister at the time, ALLAWI, during his visit to Germany in December 2004. In April 2005, the Tunisian National G. Ihsan was sentenced to three years and nine months' imprisonment by the superior Court of Justice of Berlin, inter alia for illegal possession of weapons and falsification of documents. The charge of founding a terrorist organization could not be substantiated adequately; however, the court assumed that G. Ihsan had entered Germany as a "jihadist" with the objective of committing an explosives attack in Berlin in connection with the start of the war in Iraq in March 2003. On 8 January 2007, the HRC of Hamburg sentenced E. M. Mounir to 15 years' imprisonment for membership in a terrorist organization and aiding and abetting murder in connection with the terrorist attacks of 11 September 2001 (so-called Hamburg cell).

Several convictions of AAI and Al-Qaida followers for logistic and financial support for these terrorist organizations show that Germany is of particular importance as a supply base and platform for agitation. One case that illustrates this is that of A. M. Lokman, who was sentenced to seven years' imprisonment in January 2006 by the HRC of Munich for membership in a foreign terrorist organization, gang-type facilitation of illegal entry, and fraud. Among other things, he was charged with having recruited in Germany, as a member of the terrorist group AAI, so-called "holy warriors" for Iraq. This judgment can be considered a judicial precedent in the sense that it is the first conviction after a new section, 129 b, had been added to the German Penal Code in connection with passage of the so-called First Anti-Terror Package (ATP).[14,15] On 5 December 2007, M. K. Ibrahim who had been trained in Al-Qaida training camps in Afghanistan before 11 September 2001 was sentenced to seven years' imprisonment by the HRC of Düsseldorf for financial and logistic support for Al-Qaida and recruitment of new Al-Qaida members.[16]

---

[14] cf. the comments to be found below in 1.5.1.

[15] In addition, the HRC of Stuttgart sentenced B. Burhan to 2 years and 6 months' imprisonment on 26 September 2007 and the HRC of Munich sentenced K. A. Farhad to 5 years and 6 months' imprisonment as well as A. I. Dieman to 3 years and 3 months' imprisonment on 9 July 2007 and 25 June 2007, respectively. These sentences were pronounced for membership of and support for AAI, (inter alia) pursuant to section 129b of the German Penal Code.

[16] Two other defendants were sentenced by the court to 6 years' imprisonment and to 3 years and 6 months' imprisonment, respectively. On 24 January 2008 and 21 February 2008, the HRC of Schleswig sentenced two defendants to prison terms of 5 years and 9 months and of 2 years, respectively, also for support for Al-Qaida.

Thus, Germany is part of an endangered area of global dimensions where international terrorists are active. It has to be assumed that as yet unidentified Islamist networks and cells exist, networks and cells that are integrated into functioning cross-border structures and, to a large degree, can plan attacks independently based on their own capabilities and means available.

At present, police measures are focusing on Al-Qaida activists and IJU members, apart from Ansar Al-Islam supporters. After preparations for terrorist attacks have been uncovered in Oberschlehdorn, investigative proceedings are being conducted against further suspects. It cannot be ruled out either that as yet unidentified IJU members or sympathizers keep planning attacks or are instructed by the IJU leadership in Pakistan to restart preparations for attacks. It is the long-term goal of the security authorities to shed light on the structures and environment of the IJU in Germany and Europe. At present, several dozens of persons who are considered to be in the wake of Islamist terrorist organizations are under surveillance (as so-called "potentially dangerous persons"). If followers of Islamist terrorist organizations concentrate on the financial and propaganda support for these organizations from Germany, the "Islamist centres" existing mostly in big cities and serving as contact points for political and religious purposes have to be placed under surveillance as well.[17] Consequently, the measures taken by security authorities must also aim at "drying up" such supporting systems, for example, the collection of "donations" by Islamist welfare organizations.

In 2007, the Office for the Protection of the Constitution recorded information about 30 Islamist organizations active in Germany with potential human resources estimated at 33,172 followers, which represents about 1% of the more than three million Muslims living in Germany.[18] These "human resource" figures should not be equated with the much smaller number of violence-prone terrorists motivated by Islamist ideology. On the contrary, extremist activities that elevate a fundamentalistically interpreted Sharia above the value system of the German constitution are a potential threat. In view of the above, even Islamist organizations that do not conduct terrorist activities in Germany – such as the "Islamische Gemeinschaft Milli Görüs" (IGMG) – may represent a threat.[19] Here concerns are focused on extremist religious agitation aimed at destabilizing constitutional democracies from within.[20]

At the same time, a great number of German nationals have been victims of terrorist attacks in foreign countries. Some examples are the attack on a synagogue

[17] Pfahl-Traughber, *Kriminalistik* 2003, p. 202 (206); Müller, 2004, p. 480 (498). For detailed comments about the situation with respect to corresponding centres in the UK, *see* Alexiev, *Internationale Politik* 2005, p. 92 (93 ff.).

[18] Verfassungsschutzbericht (Report of the Office for the protection of the Constitution) 2007, p. 185.

[19] With regard to the "Islamische Gemeinschaft Milli Görüs e.V.", see Verfassungsschutzbericht (Report of the Office for the Protection of the Constitution) 2007, p. 217 ff.

[20] Krause, *Internationale Politik* 2004, p. 75 (78 f.).

on the Tunisian island of Djerba on 11 April 2002, where a car bomb killed 21 persons, including 14 German tourists; the bombings on the Indonesian island of Bali on 12 October 2002 that killed 197 persons, including 6 Germans; the suicide attacks in Kabul that killed soldiers of the German Federal Armed Forces and injured many others, some of them seriously, on 7 June 2003 and on 14 November 2005; the murder of 2 members of the Federal Police Special Forces unit GSG 9 who were shot to death in an ambush near Fallujah on 7 April 2004 while escorting a German convoy from Amman to Bagdad as well as 3 German police officers assigned to the German Embassy in Kabul who were victims of a terrorist attack on 15 August 2007. Germans were also among the victims of the terror attacks in Madrid on 11 March 2004 and in London on 7 and 21 July 2005. Since 2001, a total number of 58 Germans have been killed in terrorist attacks committed in foreign countries and 119 have been injured.[21]

1.4 Phenomenology

At the present time, any assessment of international terrorism motivated by Islamist ideology can only be provisional. Thus far, virtually each new attack has forced the security authorities to reconsider and further develop their assessments of this phenomenon. The following section gives an overview of the differing modi operandi, offender profiles, and motives registered so far.

1.4.1 Perpetrators and Organizational Structure

After Al-Qaida's operational basis had been considerably weakened by the Allied Forces' invasion of Afghanistan in October 2001, the overthrow of the Taliban regime and numerous successful searches for wanted persons, we are now witnessing the organization gaining new strength.[22] The numerous attacks committed in December 2007 and in January 2008 in Algeria and Mauritania for which the so-called Al-Qaida in Islamic Maghreb assumed responsibility and the fact that the different types of perpetrators identified in connection with Islamist terrorism still orientate themselves to the ideology of international Jihad[23] propagated by Al-Qaida leader Osama Bin Laden and his deputy Ayman Al-Zawahiri are, among other

[21] As of 15 May 2008.

[22] cf. Verfassungsschutzbericht (Report of the Office for the Protection of the Constitution) 2007, p. 182 ff.

[23] Jihad means efforts to spread the Islamic faith.

things, proof of this.[24] At the same time, the spectrum of violence-prone Islamists gets more and more heterogeneous with every attack or attempted attack.

While the attackers of 11 September 2001 were considered to be directly controlled by Al-Qaida, the attacks committed in Madrid are attributed to so-called non-aligned mujahedin, self-styled "holy warriors," who act independently of Al-Qaida. An autonomous cell was responsible for the attempted attacks committed in Germany by means of suitcase bombs. Another phenomenon is that of the so-called "home-grown" terrorists,[25] which came to notice for the first time during the attacks in London. Three of the London bombers belonged to the second generation of immigrant families and have mostly been socialized within the UK.

Since the events of Oberschlehdorn, the phenomenon of radicalized converts has become one of acute importance in Germany: Two of the three suspects are German nationals converted to Islamic faith who were trained in the handling of explosives in IJU training camps in Pakistan to commit terrorist attacks in Germany. According to what has been established so far by the security authorities, the suspects were integrated into an international network of the IJU that has close contacts with Al-Qaida. Of course, converts must not be subjected to general suspicion. Several thousand people convert to the Islamic faith in Germany every year; their total number is estimated at 18,000 persons in Germany. Only radicalized converts pose problems. In the past, some cases came to notice in Germany and in other Western countries where converts were involved in terrorist activities. For example, it has been established that German converts travelled to combat areas like Chechnya or to terrorist training camps. Al-Qaida and associated terrorist organizations systematically recruit converts for their purposes as they know the respective target country's mother tongue and infrastructure, and can move more discreetly because of their Western European appearance.

---

[24] For the purpose of assessing the complex structure of the threat potential of international terrorism, including Al-Qaida and groups and individuals associated with it, already at the beginning of 2005, British security authorities prepared a corresponding three-tier-model: "'Tier 1,' describing individuals or networks considered to have direct links with core Al-Qaida; 'Tier 2,' individuals or networks more loosely affiliated with Al-Qaida, and 'Tier 3,' those without any links to Al-Qaida who might be inspired by their ideology." It is now assumed that the attackers of London and Madrid were merely inspired by Bin Laden and thus can be classified under Tier 3 (Intelligence and Security Committee – Report into the London Terrorist Attacks on 7 July 2005, p. 27).

[25] "Home-grown" terrorist is a colloquial expression used for the first time by UK media in 1999. There is no generally accepted definition. By "home-grown" terrorists, we usually understand Islamists who were born and/or socialized in countries having a democratic government and social system. Despite of their structural integration (e.g., place of work, residence, membership in clubs, and associations), they devote themselves, in the course of their further development and for various religious, social, cultural, and psychological reasons, to Islamist ideology and start refusing democratic government and social systems. Therefore, the expression may comprise people with a migrant background as well as converts professing the Islamic faith [cf. Verfassungsschutzbericht (Report of the Office for the Protection of the Constitution) 2007, p. 192 f.].

Another strategy consists in recruiting Europeans to commit suicide attacks in foreign countries: Information gathered so far gives reason to believe that the bombing of a US military base in Afghanistan on 3 March 2008 which killed, according to what is known so far, at least two US soldiers apart from the perpetrator was committed by the Turkish national C. Cüneyt who had grown up in Germany.

In addition, there is the problem of Jihad fighters socialized in Europe who took part in terrorist combat activities, for instance in Afghanistan or Chechnya, and return to Europe.

1.4.2 Offence Profile

1.4.2.1 Targets for Attacks

The terrorist attacks that have been perpetrated since the events of 11 September 2001 in the USA have taken on a new dimension in terms of magnitude, damage caused, and modus operandi and, consequently, have left a permanent mark on the global security situation. In contrast to Germany's RAF, which still tried to make its objectives and actions understandable to the general population, not only do Islamist terrorists consciously accept the risk of killing thousands of innocent and uninvolved persons but also intentionally try to cause a large number of victims.[26] At the same time, no typical modus operandi can be identified; almost any form of attack is conceivable. Targets with a symbolic nature that is economic (e.g., World Trade Center), political (e.g., embassies), or religious (e.g., synagogues) are no longer the main focus of terrorist attacks. To an increasing extent, terrorism motivated by Islamist ideology also takes aim at so-called "soft targets" – places that are normally not classified as threatened and/or are difficult to protect such as the public transport system.

1.4.2.2 Importance of the Modern Media

To an increasing extent, Al-Qaida and other terrorist organizations are exploiting the media as a means of waging psychological warfare. They especially use the Internet to obtain the greatest possible public attention, disseminate propaganda material, and recruit new members and sympathizers. Bin Laden, his deputy Ayman Al Zawahiri, and, until his death on 7 June 2006, the Al-Qaida leader in Iraq, Abu Musab Al Zarqawi, have been propagating the ideology of violent international

[26]cf. Müller, 2004, p. 280 (494); Krause, *Internationale Politik* 2004, p. 75 (76 ff.); Hauschild, *Internationale Politik* 2005, p. 32 (36). Religion is viewed as providing unlimited justification for violence and extermination of the adversary: The terrorist's enemy is also the enemy of God. Al-Qaida's founding declaration includes a fatwa that calls for "killing Americans and their allies, military personnel, and civilians as a prescribed obligation of every Muslim to be fulfilled in every country where this appears possible to him" [Klink, *Der Kriminalist* 2003, p. 341 (342)].

Jihad particularly by sending audio and video messages. Since 2001, about 30 threat messages have been seized on the Internet. In these messages, Al-Qaida and other terrorist groups threatened Europe and explicitly Germany (in about half of the cases) with attacks. On 12 November 2002, Osama Bin Laden had threatened the US allies with further attacks in a tape-recorded message on the occasion of the Djerba and Bali bombings. In this context, he explicitly mentioned Germany, apart from other countries. In a video message of 10 March 2007, the Global Islamic Media Front calls upon the governments of Germany and Austria to withdraw their troops from Afghanistan. This threat was repeated on 19 November 2007. The IJU also repeatedly uttered threats against Germany and Europe. For example, an IJU statement with regard to the planned attack of Oberschlehdorn of 4 September 2007 was published on a Turkish website on 11 September 2007. After the repeated publication of cartoons depicting the Prophet Mohammed, Osama Bin Laden threatened Europe with retaliation measures in an audio message seized on 20 March 2008. In the video message, Bin Laden calls upon his followers and sympathizers to carry out violent actions. In addition, Bin Laden (in a video message of 21 March 2008) and Al-Zawahiri (in an audio message of 24 March 2008) made threats of retaliation against those states that support Israel in the Middle East conflict. Although these statements were mainly addressed to the Arab world, there is a risk that they may be taken as a justification for attacks against Jewish facilities also in Germany.

Apart from being used to disseminate propaganda and calls for attacks, the Internet is used to distribute specific instructions for planned attacks. Nowadays, we can even speak of "open universities" for terrorism and virtual training camps. Topics like hacking, encryption methods, possibilities offered by steganography (hidden storage or transmission of information), or the manufacture of so-called dirty bombs are being discussed. The case of the so-called "suitcase bombers" in Germany shows that the risk that groups or fanatic individual offenders are incited to action by these threat messages or regard them as justification for attacks has to be taken seriously. Both suspects stated that their indignation at the Mohammed cartoons was the motive for their action.

1.4.2.3 Logistic and Financial Structures

If one takes a look at the logistic and financial efforts made in connection with terrorist attacks or plans for attacks motivated by Islamist ideology within Western states, a clear trend towards simplification can be identified: The attacks of 11 September 2001 were preceded by planning and preparation activities lasting several years (e.g., the obtaining of pilot licenses). These activities required considerable financial resources. The most recent attacks and attempted attacks show a new development: Improvised explosive devices were used to commit the crimes. The perpetrators used industrial explosives (Madrid), homemade explosives (London, Oberschlehdorn/Germany), or a manipulated gas bottle and fuel (attempted attacks on regional trains in Germany). The instructions needed to

build improvised explosive devices can be found on the Internet; the necessary material can be purchased legally at relatively low prices. While the investigation into the London bombings showed that the expense was less than 8,000 GBP,[27] the costs for the attempted attacks on regional trains in Germany were probably less than 200 euros. This is a further indication that, besides an ideological commitment, the perpetrators do not necessarily depend on an infrastructure in the form of a larger group to provide them with logistics and finances for the preparation of attacks that could potentially cause immense damage.

According to the security authorities, another question requiring clarification is the possibility of links between international terrorism and organized crime. Because of the different objectives pursued by these two fields of crime (while political ideology or religion is the main motivation for terrorist activities, organized crime is driven by the economic objective of maximizing profits), "business" contacts are possible that would permit each side to profit from the criminal structures of the partner. For example, it is suspected that Al-Qaida terrorists use the services of professional people-smuggling networks, and that in Colombia and Afghanistan, there is a connection between the financing of terrorism and illegal drug trafficking. However, no substantiated information on systematic links that go beyond simple business relations is on hand at the present time.

In summary, when motivated terrorist attacks regarding the phenomenology of Islamist, the following should be kept in mind: The fact that a centrally controlled organization with fixed command and hierarchical structures is lacking enables terrorist groups to respond more flexibly if intervention from the outside is attempted. At the same time, the following factors make it more difficult for the security authorities to carry out preventive and repressive measures: the structure of globally associated organizations and cells that operate independently of each other as well as activity by individuals who "only" have an ideology in common, the phenomenon of suicide attackers, "home-grown" terrorists, and radicalized converts, and finally, the fact that attacks with considerable impact can be committed with limited financial and logistic resources.

1.4.3 Motivation

As is true of all forms of terrorism, terrorists motivated by Islamist ideology assume that social change can be brought about by the use of violence. The particular danger posed by Islamist terrorism is due to the fact that the terrorists – who believe they are obeying a divine "commandment" to commit terrorist acts and do not consider themselves criminals – are determined to go to the limit and are willing to sacrifice their own lives.[28] Extremist Islamism differs from other forms of political extremism

[27] Report of the Official Account of the Bombings in London on 7 July 2005, 2006, p. 23.

[28] cf. Müller, 2004, p. 480 (491 ff.).

such as the German RAF due to its radical interpretation of the Islamic faith, the way it strives to unify religion and politics in the form of a theocracy, and its basically totalitarian orientation. Its paramount objective is to set up an Islamic religious state based on Sharia law.[29] Terrorists motivated by Islamist ideology view terrorism and all forms of conventional and unconventional war as legitimate means of fighting a "Holy War."[30] While attacks on Allied troops in Iraq or Afghanistan aim at driving "unbelievers" off "holy Islamic ground," by means of terrorist attacks in Europe and the USA, the perpetrators hope that these societies will pressure their governments to withdraw from Arab Islamic countries. Furthermore, ideas of revenge and retaliation are involved – due to military activities by the USA and their allies in the Iraq war or incidents such as the publication of the Muhammad caricatures which are taken as an insult to Islam. Besides this more group-oriented motivation, religious expectations such as immediate entry into Paradise for successful acts of martyrdom probably play a significant role in the case of suicide attackers.

It is disputable whether Islamist terrorism is to be seen more as a political strategy that employs religion solely as a source of motivation and legitimation, or whether we are dealing with a new form of religious fundamentalism that does not predominantly make any claim to political but religious power. The response to this question is crucial: In contrast to terrorism directed at political goals, the current form of fundamentalist terrorism represents a new threat characterized by extreme violence and lack of compromise that is likely to place strict limits on the development of counterstrategies. Because of the basic convictions that underlie a fundamentalist orientation, such terrorist views are not subject to negotiation. Only preventive long-term counterstrategies that tackle radicalization processes at the roots would appear to be successful here.[31]

1.5 Suppression Approaches

1.5.1 Statutory Measures

In the field of international terrorism, the impacted countries face serious danger situations, some of which are perceived as warlike threats that penetrate their societies, (also) from outside the country, while the violence-prone actors are not

[29] Pfahl-Traughber, *Kriminalistik* 2003, p. 202 (206); Backes/Jesse, 2002, p. 13ff. *See also* Tibi, 2002, p. 27 (33 f.) on the origins of fundamentalism in Islam.

[30] Backes/Jesse, 2002, p. 18. For detailed information about jihad, *see* Tibi, 2002, p. 27 (29 ff.); Elger, 2001, p. 146 f. According to this, in principle, the Koran does permit the use of force as one means of spreading the Islamic faith, but only if strict rules are observed – for example, not attacking civilians and forewarning the enemy – and thus forbids all forms of terror. Accordingly, the classical jihad war must be differentiated from jihad terrorism.

[31] *See also* Ignatieff, *Internationale Politik* 2005, p. 52 (53).

representatives of a state with a monopoly on power (so-called asymmetric warfare). This new type of threat, which results in overlaps of internal and external security for the countries in question, requires a reorientation of security strategies. At this point, the discussions about in-country deployment of Germany's Federal Armed Forces in connection with the World Cup games and the confrontations concerning the German Aviation Security Act should be mentioned.[32]

On the basis of the experience gained by the German police while fighting RAF terrorism, the response to the attacks of 11 September 2001 involved organizational, police strategy, and legislative levels. During the last years, the legal framework for combating terrorism in the Federal Republic of Germany has been expanded and supplemented, and especially in this connection Germany's Federal Parliament passed two so-called Anti-Terror Packages shortly after 11 September 2001 – on 9 November 2001 and 14 December 2001.

The first ATP focused on substantive legal changes, and in addition to eliminating the so-called "religious privilege" in the legislation on associations,[33] it included the introduction of section 129b of the German Penal Code.[34,35] Since amendment of the law, religious communities fall under the Associations Act and can be banned if their objectives or activities contravene existing laws or the constitutional order or the spirit of understanding among the peoples of the world. Thus, in the future, extremist groups are prohibited from pursuing illegal objectives by making reference to their "religious privilege." Section 129b of the German Penal Code also makes it possible to prosecute criminal and terrorist organizations outside of Germany.

The main objective of the second ATP (the so-called Counter-Terrorism Act/TBG or ATP II)[36] was to ensure that the security authorities will be able to identify terrorist activities, and in particular preparations for them, at the earliest possible stage. Also taking into account the experience gained in the USA, the security authorities were supposed to be granted the necessary powers to collect and exchange data between each other with a view to improving the efficiency of their work in the battle against international terrorism. In cases where the BKA in its function as a central office has information about criminal offences, the BKA can now collect data to supplement information already on hand or to conduct analysis projects without

[32] At the present time, Germany's Basic Constitutional Law only provides for deployment of the Federal Armed Forces inside the country in cases of domestic emergency or natural disaster (Article 87a IV, 35 II 2 of the Basic Law for the Federal Republic of Germany). On 15 February 15, 2006, the Federal Constitutional Court declared that section 14 III of the Aviation Security Law, which made it possible for the air force to shoot down an aeroplane being used as a weapon while tacitly accepting the risk of killing uninvolved passengers, was in conflict with the right to life and with the guarantee of human dignity. It was stated that this legal provision is only compatible with the fundamental rights in question if the operation is directed at an unmanned plane or at a plane with only attackers on board. *See also* Hetzer, this volume.

[33] Federal Law Gazette (BGBl) 2001 I, p. 3319.

[34] Federal Law Gazette (BGBl) 2002 I, p. 3390.

[35] cf. Körper, *dnp* 2001, p. 20f.; Schrader, *Kriminalistik* 2003, p. 209; Roell, 2003, p. 125 (131 ff.).

[36] Federal Law Gazette (BGBl) 2002 I, p. 361.

having to clarify in advance if the police forces of the Federation or the states already have this information (section 7 subsection 2 of the BKA Law).[37]

It is intended to make both the preparation of serious terrorist acts of violence and instructions for committing such crimes punishable acts in Germany. Initiating or maintaining relations with a terrorist organization is also intended to be a criminal act in the future if this is aimed at receiving instructions with regard to the commission of attacks. Since criminal liability pursuant to sections 129a and b of the German Penal Code requires the existence of a terrorist organization (a group composed of at least three members), Islamist perpetrators, however – other than, for example, the RAF – often operate in loose networks or on their own without being firmly integrated into hierarchically organized groups; the planned new provisions are also intended to be applicable to perpetrators who are not part of an organization.[38] Specifically, this means that whoever receives or provides training in order to commit a terrorist act of violence, whoever procures explosives, arms, or essential substances for the production of explosives or arms or finances a terrorist attack (new section 89a of the German Penal Code) shall be punished with imprisonment for not more than 10 years. Whoever disseminates or procures "terrorist instructions," for example, designed to build bombs or weapons – for instance, via the Internet – shall be punished with imprisonment for not more than 3 years (new section 91 of the German Penal Code). This legislative initiative shall also implement the Council of Europe Convention on the Prevention of Terrorism signed by Germany that entered into force on 1 June 2007.

Furthermore, the BKA shall be granted powers designed to ward off danger in the field of international terrorism in future cases of danger involving more than one federal state, where jurisdiction of a state police authority is not identifiable or where the highest state authority requests the BKA to take charge of the matter.[39] If information about a crime possibly being planned in the field of international terrorism is received at the BKA without any immediate indication about which state has jurisdiction, the BKA currently cannot take action until there is initial prosecutorial suspicion. To supplement the information if it has to take any necessary measures to avert danger, the BKA then has to turn to the state police forces. If initial prosecutorial suspicion is confirmed, the BKA is then responsible for taking the necessary law enforcement measures. Efforts are being made to avoid the multiple changes in

[37] Körper, *dnp* 2001, p. 20 (21 ff.); Roell, 2003, p. 125 (135 f.). The Act Supplementing the Counter-Terrorism Act/TBEG [Federal Law Gazette (BGBl) 2007 I, p. 2] extends and expands the powers created by the Counter-Terrorism Act (TBG), especially with regard to the Federal Office for the Protection of the Constitution. The Act Supplementing the Counter-Terrorism Act (TBEG) is limited to a period of 5 years.

[38] Draft bill aimed at the prosecution of the preparation of serious acts of violence (GVVG).

[39] Art. 73 (1) No. 9a of the Basic Law for the Federal Republic of Germany that entered into force on 1 September 2006 granted the Federation corresponding legislative powers [Federal Law Gazette (BGBl) 2006 I, p. 2034]. The BKA law is being revised in an effort to provide the BKA with the investigative measures necessary to ward off danger in the field of international terrorism, which are comparable to those of the state police forces.

jurisdiction that occur between the time information is received about a possible terrorist attack, the taking of measures by the German states to ward off danger, and criminal investigations by the BKA. This also corresponds to a time-tested principle of police work, namely that measures to avert danger and law enforcement measures should be handled by the same police authority. Otherwise it could take longer to react, and the danger of information loss is greater.

Apart from statutory measures, the counterterrorism objectives laid down by the Federal Government set the direction for the police and administrative measures taken in view of the new threat situation in the Federal Republic of Germany. These can be summarized as follows: destroying terrorist structures by intensifying pressure through searches and investigations, pre-emptive prevention of terrorism, expanding international co-operation, eliminating the causes of terrorism, protecting the population, as well as taking precautionary measures and reducing the vulnerability of the Federal Republic of Germany.[40]

1.5.2 Criminal Prosecution

In the face of the special threat situation created by Islamist terrorism, during the last years, the German criminal justice authorities have intensified the pressure exerted by searches and investigations with the aim of uncovering the structures of terrorism. The achievement of this objective is documented by the large number of investigations: Currently, 189 investigative proceedings with Islamist-terrorist background are being conducted, 112 of them by BKA.[41] Most of the BKA's investigations are concentrated on the organization-related offences covered by sections 129a and 129b of the German Penal Code, whereas other offences include homicides, money laundering, and violations of aliens legislation.

In addition to intensifying the pressure exerted by the law enforcement authorities, another important approach to suppression of terrorist structures is to deprive them of their financial basis. Since the amendment of the Money Laundering Act (GWG) in 2002, suspicious transaction reports are also being used in the battle against terrorist financing.[42] The statutory definition of the offence to be found in section 129b of the German Penal Code was included in the catalogue of money laundering offences (section 261 of the German Penal Code). Also in 2002, the Fourth Financial Markets Promotion Act that included provisions aimed at prevention of crime through improved transparency and identifiability of payment flows with a terrorist or money laundering background was introduced.[43] An EU Directive of 26 October

[40]These objectives can be found on the website of the Federal Ministry of the Interior at http://www.bmi.bund.de (10 April 2008).

[41]As of 14 April 2008.

[42]Federal Law Gazette (BGBl) 2002 I, p. 3105.

[43]Roell 2003, p. 125 (133 ff.).

2005 defines the term terrorist financing for the first time. According to this Directive, both the provision and the collection of financial means are recorded.[44] At an international level, almost 100 countries now co-operate closely in the field of prevention and prosecution of money laundering as well as financing of terrorism, with the central office established at the BKA to receive and analyze the suspicious transaction reports (Financial Intelligence Unit, FIU) being the central point of contact for Germany.[45] The FIU creates the prerequisites for central collection of relevant criminal information that can be used to combat money laundering – also in connection with terrorism – and analyzed in support of law enforcement measures. However, they also carry out investigations themselves. Between 2002 and 2007, an average of about 100 reports was made annually for suspected financing of terrorism.

1.5.3 Prevention

In order to fight international terrorism motivated by Islamist ideology successfully, besides intensified law enforcement measures, above all the prevention of new attacks and protection of endangered persons and facilities, that is, preventive measures, are of decisive importance. Furthermore criminal law, to an increasing extent, is understood as helping the State to carry out its task of providing security by means of prevention. This is demonstrated by the growing tendency to introduce abstract offences of endangerment that do not refer to the actual criminal act but rather to relevant conduct prior to commission. For example, in sections 129a and 129b of the German Penal Code, mere membership in a terrorist organization is subject to punishment even if no specific acts that would constitute an actual offence have been carried out as yet.[46] In the context of crime control policy, abstract offences of endangerment are of special relevance when the protection of supply and information systems is concerned, because in a highly networked society like ours, such systems are particularly vulnerable and in need of protection, and the same applies to state security.

---

[44] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing took effect on 15 December 2005. The reporting obligation was extended to include suspicion of money laundering or financing of terrorism, now covering also existing customer relations. The Directive has to be incorporated into national law by 16 December 2007. A corresponding law will presumably be passed in Germany in summer 2008.

[45] Section 5 of the Money Laundering Act (GWG). cf. Kerner/Stierle/Tiedtke, *Kriminalistik* 2006, p. 292 (297 f.).

[46] However, in order to be considered a member of an organization, a person has to participate in the everyday activities of the organization – by acts which in itself can be legal – in order to demonstrate his/her membership. cf. Tröndle/Fischer, 2007, section 129a, margin no. 20, section 129, margin no. 24.

1.5.4 Freedom and Security

With the attacks in London in July 2005, Western Europe lost its status as one of the world's last regions where suicide perpetrators were not part of terrorists' known modi operandi. Fanatic perpetrators, who are absolutely determined to do anything and who are prepared to give everything – even their lives – are not deterred by the prospect of punishment. The general and special preventive effect of criminal law has no impact here. This has resulted in the demand for supplementing the classic police methods designed to solve crimes. This has generated a new prevention paradigm making the early abstract crime detection and the specific crime prevention a core element of the activities performed by law enforcement policy and security authorities to an extent not previously known. In this connection, the following question arises: How far should, or must, the State go to protect its citizens effectively?

In 1970s, above all in connection with the student protests at the time, discussions of this question were focused on the right of the individual citizen to defend himself against state intervention in connection with his right to personal liberty. Today we are experiencing a return to the classic core duty of the State, ensuring internal and external security. Attributing the changed perspective on the role of the state that can be noted during the last years solely to the threat of international terrorism would certainly be too short-sighted. Rather, this is the result of a long-term process. However, the terrorist attacks of the last years with their random impact on the civilian population probably did function as a catalyst.

With regard to freedom and security, a relationship of tension between them prevails whenever fundamental rights, in their function as the rights of citizens to ward off state interference, place limits on the actions of the State. However, freedom and security are also mutually dependent. The view that fundamental rights are solely the rights of citizens to ward off state interference is now outdated. Instead, it has been recognized that obligations to protect are based on the constitution insofar as the principle of the rule of law obligates the State to protect its citizens.[47] As a result, the State must be in a position to ensure internal security.[48] In the light of new threat scenarios created by international terrorism, the State governed according to the rule of law must respond and remain true to itself at the same time. A central criterion in this context is the efficiency of new measures and their use in compliance with the principle of proportionality.

It is crucial to the law enforcement authorities to know how the investigative powers have to be designed and further developed so that they can efficiently meet

[47]The obligation of the State to respect fundamental rights when it takes action in connection with the duty to protect to be found in Article 1 (1) p. 2 of the Basic Law for the Federal Republic of Germany.

[48]Thus, the Federal Constitutional Court states: "An obligation to protect not only the individual but also all citizens can be found in the Basic Law. Carrying out this duty effectively requires the competent state institutions to be in a position to react appropriately to the circumstances presented by each individual case." [Federal Constitutional Court decision 46, 160 (165)].

the expectations of the legislators and the Federal Constitutional Court – that is, effective crime suppression, warding off danger, and protection of citizens and State – also and above all in view of terrorism. At the same time, the question arises as to how the control mechanisms to which the police are subjected are designed in the context of new investigative powers in order to satisfy the rule-of-law principles and to efficiently deal with fear of abuse among the population.[49]

1.5.5 Investigative Measures

Covert investigative measures such as telephone intercepts and surveillance of private premises have proven to be importance for successful law enforcement in the fields of organized crime and international terrorism. In the light of the fact, however, that perpetrators are increasingly using modern information technology for criminal purposes – and not only for propaganda purposes but also for communication related to the preparation and carrying out of offences – classic undercover measures often prove to be pointless. Good examples in this context are the following catchwords and phrases: use of encryption software, Internet-based telephony (Voice over IP, VoIP), use of open WLAN access points of uninvolved third parties, non-stationary use of public Internet services, use of Web space, file-sharing, joint e-mail accounts shared by several individuals, and access to Internet cafés.[50] Telecommunications interception measures pursuant to section 100a of the German Code of Criminal Procedure cease to be sufficient when perpetrators exchange relevant information by other means than the telephone or the Internet, or – if they do – use encryption technologies. One measure of investigation viable to counter these deficiencies is described by the term "online searches." In this case, special software is employed to covertly search the data storage systems of a computer used by a targeted person for information relevant to the investigation without the target knowing it.[51]

On 27 February 2008, the German Federal Constitutional Court (BVerfG) ruled that the measure of online searches could be justified by purposes of both aversion of danger and criminal prosecution, but that it was not backed by the current legal order.[52] Thus, the existing basic rights and the special objects of protection [deduced, for years, by the BVerfG itself from the general right to personal privacy (section 2 subsection 1 in connection with section 1 subsection 1 of the German constitution)], notably the "right of informational self-determination," do not offer

[49]As a rule, of all institutions in Germany, the German police is the one most highly trusted. Corresponding surveys show that police have held a top position for years – even higher than the judicial authorities – as currently shown by a survey published by the Leipzig market research institute in April 2008, according to which 85% of the 1,000 persons interviewed expressed their trust in the police.

[50]See also Brunst, this volume.

[51]cf. Hofmann, *NStZ* 2005, p. 121; Buermeyer, *HRRS* 2007, p. 154 (158 ff.).

[52]1 BvR 370/07 and 595/07.

sufficient protection against high-level intervention as constituted by online searches. Hence, the BVerfG defined a new object of protection, namely the basic right to the "guarantee of confidentiality and integrity of information technology systems." In this context, the following guideline (valid for, inter alia, the legislator) must be observed: An interference with basic rights is subject to judicial reservation. In the case of aversion of danger, a concrete danger to major protected interests must exist. On the contrary, it is not imperative that the danger to be warded off be imminent, which is why it is not necessary for the danger to constitute a current threat. The Federal Constitutional Court also demands that the protection of the core area of private sphere[53] be defined by legal norms. To this end, the court established a "two-tier model": according to this model, when online searches are ordered and carried out, it must be sought that there be no interference with the core area, if possible. However, if the law enforcement authorities develop information relevant to the core area – which in fact seems to be inevitable when computer hard disks are subjected to online searches – standard rules governing the deletion of data and the prohibition of further use must be set up for the evaluation phase.

As of 1 January 2008, telecommunication providers in Germany (fixed line and mobile phones) are obliged to store communications data for a period of 6 months.[54] The same will apply to Internet access providers as of 1 January 2009. The passing on of data to the police is regulated by section 100g of the German Code of Criminal Procedure and section 113a, b of the Telecommunications Act. In accordance with these laws, an individual case must be associated with a serious offence; the measure is subject to judicial reservation.[55] An internal study carried out by the

[53] What exactly is part of the core area is not stipulated by law and depends on the individual case. To what extent communication is protected depends mainly on the contents communicated and on the intensity of a measure. The starting point always is the question of whether the human dignity of persons involved is at risk (cf. Meyer-Goßner, section 100c margin no. 13 ff.).

[54] Sections 113a subsection 1, 150 subsection 12b of the Telecommunications Act (TKG), newly introduced by the law on the new regulation of interception of telecommunications and other undercover measures of investigation and on the implementation of directive 2006/24/EG [Federal Law Gazette (BGBl) 2007 I, p. 3198]. With its mandatory 6-month storage period, the German legislature geared itself toward the lower end of the range provided by the EU directive. However, as the enforcement of action relating to breaches of regulations by telecommunication providers has been postponed, they, too, will factually be only obliged to store data as of 1 January 2009. This approach takes account of the fact that the parties obliged will not be in a position to smoothly implement the data storage specifications on a short-term basis.

[55] On 11 March 2008, in the context of immediate legal protection proceedings (1 BvR 256/2008) contesting the storage of communication data, the Federal Constitutional Court ruled that telecommunication providers have to collect and store such data, but that they have to pass them on to the requesting law enforcement authorities (pursuant to section 100g subsection 1 German Code of Criminal Procedure), only if the request is based on investigative proceedings relating to an offence in the sense of section 100a of the Code of Criminal Procedure, that is a serious offence. If this is not the case, the transmission of data is suspended for the time being. Thus, the court held that a criminal offence of "substantial significance" pursuant to section 100g of the Code of Criminal Procedure would not meet the said requirements.

BKA shows that the passing on of communications data – for example, the IP address[56] allocated during data exchange via the Internet – is decisive for law enforcement authorities because communications data often yield the only investigative lead to follow. Prior to the new legislation, telecommunication providers and Internet services either did not store the data in question at all or were, in part, not allowed to do this (e.g., in the case of flat-rate contracts), or had deleted the data already before a judicial decision could be obtained.

Even though a general preventive effect is attributed to criminal law, by its nature criminal law is guided by individual cases. Therefore, it alone cannot guarantee security. The same applies with regard to special investigative powers for police authorities. Accordingly, our security architecture as well as repressive and preventive measures need to (also) be considered independent of the individual case and to be guided by strategic points of view. For strategy development to succeed, it should and must be guided by an active prevention concept for the whole of society. Essential prerequisites for this are extensive knowledge of the respective phenomenology and causes and thus a comprehensive understanding of the terrorist phenomenon. However, because of the complexity of this phenomenon, we do not yet understand it adequately. This is even truer of terrorism motivated by Islamist ideology. It cannot be explained adequately by the explanatory concepts used in the past, which are based on politically motivated terrorism.

At the present time, police prevention work in Germany is carried out at three different levels. In addition to specific measures to avert danger such as warning potential perpetrators, that is, classic police fields of action, advance clarification of emerging crime phenomena, and research on the causes of crime play a decisive role. The State is responsible for protecting its citizens from terrorist attacks. At the same time, it is not possible to provide protection for all potential targets, above all soft targets. Thus, uncovering attack planning at an early stage is decisive, and doing so requires timely and comprehensive information. In Germany, too, 11 September 2001 resulted in a re-orientation of the security architecture based on the assumption that networks on the side of the perpetrators must be countered by networks formed by security authorities in the sense of linked information exchange at both national and international level.

1.5.6 New Security Architecture

1.5.6.1 Gemeinsames Terrorismusabwehrzentrum

To achieve the necessary intensification of information collection, compilation, and exchange as central factors for successful aversion of danger, structural deficits in the practice of co-operation between the security authorities had to be remedied – both

[56] IP: Internet Protocol.

at the conceptional and analytical levels and also in the field of operations.[57] In view of this situation, in December 2004, the Gemeinsames Terrorismusabwehrzentrum (GTAZ)[58] was set up in Berlin, thereby satisfying a key prerequisite for a holistic approach to suppression. Setting up the GTAZ does not amount to creating a new agency. Rather, the interagency co-operation of the BKA, the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND), the criminal police offices and constitutional protection offices of the German states, the Military Counter-Intelligence Service (MAD), the Federal Police (BPOL), the Central Office of the German Customs Investigation service (ZKA), and other security authorities has been put on a different basis. Thus, the idea of setting up a "federal security office" where all counterterrorism powers would be consolidated, or even an agency analogous to the American "Department of Homeland Security," was rejected in favour of a co-operative approach. The inclusion of a prosecution authority (Office of the Federal Prosecutor General/GBA) in a counterterrorism centre, which has never been done before, serves the purpose of immediately orienting the work of the centre toward subsequent prosecution.

The most important objective of this co-operation is timely recognition of possible threat scenarios in the field of terrorism/extremism by incorporating all available sources of information with a view to coordinating preventive and repressive measures. Of particular importance is a speedy exchange of information, the expansion of previous co-operation – for example, to include the exchange of so-called operational information – and the strengthening and pooling of analytical competence.

In this respect, the GTAZ is something completely new in Germany because never before have so many authorities been brought together in a single place for daily situation briefings in order to exchange up-to-date police information and intelligence and to make joint assessments. In addition, threat and case assessments are carried out, operational information is exchanged, and structural analyses are prepared.[59] Despite the fact that the GTAZ is set up to promote an intensive exchange of information, it still complies with the so-called "ordinance of separation," which is intended to prevent the cumulation of intelligence functions with the executive powers of the police.[60]

---

[57] cf. Müller, 2004, p. 480 (485); Baumann, *DVBl* 2005, p. 798. Because of the Germany's federal structure, more than 30 different authorities are responsible for internal security issues, a situation that makes special demands with regard to ensuring an effective flow of information.

[58] Joint Counter-Terrorism Centre.

[59] For a detailed description of how the Joint Counter-Terrorism Centre functions, *see* Würz, *Kriminalistik* 2005, p. 10 ff.; Kerner/Stierle/Tiedtke, *Kriminalistik* 2006, p. 292 (304).

[60] Consequences of this "ordinance of separation" can be found in various laws. Accordingly, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service and the Military Counter-Intelligence Service may not be attached to a police authority (sec. 2 (1) sentence 3 BverfSchG [Protection of the constitution law], sec. 1 (1) sentence 2 BNDG [Federal intelligence service act] and sec. 1 (4) MADG [Military counter-intelligence service act]); according to section 8 (3) sentence 1 BVerfSchG, section 2 (3) BNDG, and section 4 (2) MADG, these institutions are not entitled to exercise police powers and do not have the authority to give directions. With regard to the history and the legal status of the ordinance of separation, *see* Nehm *NJW* 2004, p. 3289 ff.; Baumann, *DVBl* 2005, p. 798 (799 ff.).

To develop new investigative approaches in the battle against Islamist terrorism, together with the Federal Office for the Protection of the Constitution the BKA carried out individual operational projects directly applicable to this phenomenon. For example, the work on a project entitled "Arab mujahedin training camps" made it possible to gain a more complete picture of the structure and contents of the training and how it is conducted.[61] In the project "Indicators leading to suspicion of Islamist terrorism," the objective was to develop joint "terrorist profiles" and indicators of suspicion on the basis of available investigative results. Thus, by using a database with information about 60 accused persons, the BKA was able to reconstruct personal histories and to develop functional typologies (e.g., attackers, recruiters, financiers, and logisticians) including a differentiation between religiously motivated and profit-oriented individuals. These profiles were compared with the intelligence on hand at other security authorities, whereupon search measures were initiated with regard to potential perpetrators and so-called relevant persons.[62] Further structural analyses deal with the recruitment of individuals for international jihad and with the travel movements of presumed Islamists who travel from Germany to Iraq or vice versa. The analyses focus on characteristic features of the enlistment of new recruits and the logistical support of combat operations against the allied troops in Iraq as well as acts of violence in Germany itself.

1.5.6.2 Anti-Terror-Datei

The work of the Joint Anti-Terrorism Centre is supplemented by the Anti-Terror-Datei (ATD),[63] which was activated at the BKA on 30 March 2007. As this is already the case with the GTAZ, the ATD also has the objective of furthering a faster and more targeted information exchange between the approximately 40 federal and state security authorities involved all in all.[64] Information on about 15,000 persons from the field of international terrorism and extremism in support of international terrorism, previously stored in decentralized databases, has now been transferred into the ATD.[65] Apart from basic data for the identification of a person, such data are now also stored that allow an assessment with regard to the threat

[61] cf. Würz, *Kriminalistik* 2005, p. 10 (12); Ziercke, 2005, p. 15 (19).

[62] *See also* Ziercke, 2005, p. 15 (20 f.).

[63] Anti-Terror-Database.

[64] The legal basis is the Anti-Terror Database Act (ATDG) which came into force on 22 December 2006 [Federal Law Gazette (BGBl) 2006 I, p. 3409]. It contains detailed regulations with regard to the persons, premises, or objects to be stored and with regard to the prerequisites for data processing. In addition to data protection provisions, the objective of the Act is to ensure source protection and the necessary degree of secrecy which are decisive for the intelligence services, but also for the police authorities in their cooperation with foreign partner services.

[65] Because of the double entries, the data records are, however, not identical with the number of persons stored. It must also be mentioned that the number of persons who are living in Germany and are stored in this database amounts to less than a quarter of the total amount of persons stored.

involved. However, these so-called “expanded basic data” can only be retrieved in urgent cases or upon request at the authority where they are stored.

1.5.6.3 Gemeinsames Internetzentrum

In the light of the importance of the Internet as an information platform, but also for the planning and carrying out of criminal acts in the field of terrorism, the Gemeinsames Internetzentrum (GIZ)[66] took up its work in Berlin on 1 January 2007. Analogous to the GTAZ, it is staffed with members of the BfV, the BKA, the BND, the MAD, and the GBA, all of whom are carrying out Internet searches. Websites of individual persons or organizations, news groups, forums, and chat rooms are monitored, evaluated, and analyzed to be able to recognize terrorist, but also extremist activities in the Internet as early as possible. At the present time, such Internet sites are monitored in English, German, and Arabic. It is planned to extend this monitoring to Turkish, Kurd, Pashtun, and Urdu Internet sites. A main focus is on the analysis of statements of Islamist groups and the observation of various discussion forums that convey an idea of the attitude within the Islamist scene towards current political events (e.g., controversy about the Muhammad caricatures, speech of the Pope). The work of the GIZ currently concentrates on the fields of technology (analysis of, among other things, hacking, and encryption techniques), radicalization on the Internet (use of the Internet for recruitment and indoctrination), and logistics (analysis of, among other things, information on explosives and localization of potential crime scenes).

The idea of the GIZ was successfully promoted at the European level by Germany: The project “check the web” aims at furthering an intensive monitoring and analysis of open Internet sites by the members states, following the principle of division of tasks. The necessary information portal, through which the member states can exchange their information, was activated at Europol in early May 2007.

1.5.6.4 Gemeinsames Analyse- und Strategiezentrum Illegale Migration

The holistic combat approach of the GTAZ and the GIZ has also been adopted by the Gemeinsames Analyse- und Strategiezentrum illegale Migration (GASIM).[67] The aim of this centre, which was founded in Berlin in May 2006, is to take effective action to combat illegal migration and the offences associated with it or committed as a result of it. In addition to the security authorities of the Federation (BKA, Federal Police, Federal Intelligence Service, and Federal Office for the Protection of the Constitution), the Federal Office for Migration and Refugees

[66] Joint Internet Centre.

[67] Joint Analysis and Strategy Centre for Illegal Migration.

(BAMF), the Foreign Office (AA), and the Office of Financial Control – Illegal Labor (FKS) also co-operate in the GASIM. The prime objectives are the accelerated exchange and the joint assessment of information to initiate and support investigations, as well as to assume an early-warning function from the preventive point of view. One focus here is the analysis of connections between illegal migration and other crime fields such as terrorism and organized crime. The GASIM is not a new authority either. It is much rather another example of the approach of German security authorities to counter current crime phenomena with increased institutionalized interaction and supplementation of the existing and proven security architecture, instead of creating special new structures.

1.5.6.5 Dialogue with Muslims

Another component of the holistic approach in the field of international terrorism is the dialogue between the security authorities and the Muslim associations in Germany. Since September 2005, discussions have been held on a regular basis between high-level representatives of the federal and state security authorities under the leadership of the BKA and the BfV as well as representatives from the Central Council of Muslims in Germany (ZMD) and the Turkish-Islamic Union of the Institute for Religion (DITIB). Current events – for example, planned terrorist attacks detected in Germany – are the subject of such discussions. The long-term objective of this dialogue is to build up confidence between the dialogue partners by means of joint action and mutual contacts. Such confidence-building measures between the security authorities and the two Islamist associations specifically include the designation of fixed "partners to contact for the promotion of trust" and the staging of regional lectures and information events. The latter are intended to make it possible for interested Muslims and staff from the security authorities to enter into a direct dialogue about their respective concerns. In addition, mutual trust is to be achieved by providing and distributing information material in mosques that deals with the work of the security authorities as well as by intensifying the basic and advanced training of staff from the security authorities to promote intercultural competence. It should be pointed out that an agreement has already been reached according to which imams/prayer leaders and community chairmen from both organizations will continue to take a clear position against the use of violence and the destruction of life. Agreement has also been reached that DITIB and ZMD and the security authorities – in accordance with their statutory powers – should inform each other about calls for violence and rabble-rousing agitation in mosques and other institutions.

Besides this, the Federal Ministry of the Interior has initiated a dialogue with representatives of the Muslims living in Germany in the form of a German–Islam Conference that meets regularly. The conference, which first met in September 2006, comprises 15 government representatives from the Federation, the states, and the communities on the one hand and 15 representatives of Muslim communities on the other hand. The objective is to establish a network of multipliers in the

Muslim communities and to conclude a "social contract" that is centred around understanding and acceptance of the German Constitution. Here also, the core issue is "Security and Islamism," in addition to the issues "German social order and consensus on values," "Religious issues in the understanding of the German Constitution," and "Economy and media as bridges." A discussion group deals with questions of internal security, Islamist efforts directed against the free and democratic constitutional system in Germany and the prevention and detection of criminal acts with an Islamist background.

1.5.6.6 Federation-State Project Group

Another important approach to prevention is the recommendations given by the Federation-State Project Group on "Prevention of Islamist extremism/terrorism," established by the CID Working Group[68] in early 2006. It had the task of drafting a plan for the development and co-ordination of joint prevention approaches and projects. On the basis of its mission, this initiative views itself as a platform for co-ordination of efforts by society as a whole aimed at the prevention of Islamist terrorism and their practical implementation at the level of Federation-state co-operation. In addition, the project group considered ideas that are also important for the aforementioned dialogue between the security authorities and Muslim organizations. On the basis of an initial analysis of the terrorist phenomenon as seen from a scientific point of view and by the security authorities, according to the assessment of the project group, the following programme objectives should be emphasized in connection with the development and implementation of comprehensive approaches to prevention:

1. Elimination of the basis for justification of Islamist extremist/terrorist activities
2. Reinforcement of the value system of the German constitution
3. Integration of Muslims and encouragement of social participation
4. Recognition of and respect for migrants
5. Reduction of culturally accepted violence in the daily life of Muslims
6. Exertion of influence on structures that create opportunities for crime
7. Promotion of informal social controls within Muslim society

In summary, the following can be said about the projects referred to above: The common objective of all efforts is to deny nourishment to radicalization tendencies in mosques or other areas of Muslim life and also to agitators motivated by extremism, doing so by taking advantage of every opportunity to gain allies in the affected communities and by gaining trust and knowledge.

[68] The CID Working Group (AG Kripo) is composed of the BKA President and the heads of the 16 State Criminal Police Offices. Among other things, it is their task to co-ordinate criminal police co-operation between the Federation and the states and to prepare initiatives for decision-making at ministerial level.

1.5.6.7 Co-operation with the Business Sector

The efforts of the German security authorities to establish an information network have also led to closer co-operation with the business sector. This applies in particular to security partnerships with the so-called "global players." Large economic losses are one consequence of international terrorism. For example, after the attacks of 11 September 2001, there were increases in transaction costs for transport, tourism, and international trade in particular. The Organization for Economic Co-operation and Development estimates this increase at between 1%and 3% of the value of internationally traded goods.[69] In addition, attacks and abductions in crisis areas like the present-day Iraq lead to caution on the part of Western businesses, which then do not take advantage of opportunities for expansion in new markets.

Together with the Association for Security in Trade and Industry, which represents the security interests of German firms, the BKA has been organizing meetings with meanwhile 40 German "global players" at regular intervals since 2006. While the companies are interested in receiving early warnings about threats to their facilities and staff, information collected throughout the world by the security apparatus of these companies and also their security-related research work are important for the BKA. Reciprocal training visits and joint conferences help reach a further institutionalization and deepening of the co-operation between the BKA and these companies.

1.5.7 Early Detection

Besides immediate measures for warding off danger, prognostic instruments like future-oriented analyses and hypotheses as well as causal research on how crime phenomena will develop are increasingly gaining importance. The idea behind this is the question of what new and changing crime forms and modi operandi the police have to prepare for. The overall aim is the development of an early detection system[70] that is of particular urgency especially in the field of international terrorism due to the high risk involved.

On 1 January 2005, the International Coordination Division (IK) was set up at the BKA. The international tasks previously carried out by different divisions of the BKA are concentrated here, and additional time and effort are devoted to them. Division IK is composed of two major task areas – "strategy development/strategic advance clarification of crime phenomena" and "international support." The task of Division IK is to compile information from numerous sources all over the world and analyze it from the police point of view to determine if it indicates changes in

[69] For detailed comments, *see* Brück, 2005, p. 75 ff.

[70] As to the scientific positioning of causal research and early detection in connection with prevention cf. Kaiser, side note 4 ff.

the crime or security situation in Germany. The purpose of early detection and strategic analysis is to obtain information about possible developments in the field of crime, so that the BKA and the other security authorities will be able to react in a timely manner and take any necessary measures. For example, the section that deals with strategic advance clarification has prepared its first strategic regional analysis for the Gulf region. The focus was on preparing a substantiated assessment of the significance of the Gulf Region for the international security situation. This in turn serves as the basis for arriving at strategic conclusions, connections to Germany are of particular interest. An analysis for the Balkan region is currently being prepared. Another component of the early detection and strategy development process is the so-called Umfeldanalyse (UFA),[71] conducted at the BKA for the first time in 2007. The UFA monitors and assesses general trends in Germany and throughout the world with regard to the possible impact on the security situation in Germany. The UFA, which is to be updated continuously, is based on six subject areas according to the PESTEL principle: politics, economy, society, technology, ecology, and law.

1.5.8 Source Country Strategy

A further approach of the BKA to ward off global terrorist threats is what is referred to as the source country strategy, meaning the co-operation with countries of origin, transit, and/or destination with regard to certain forms of crime, among others international terrorism. This strategy, which was developed at the beginning of the 1980s to combat internationally organized drugs crime in particular, is based on the idea of combating crimes not just in our home country but already in the source and transit countries. There are four core elements – namely, material and training assistance for foreign police authorities, an almost worldwide network of liaison officers, and specific guidance and support for police forces in investigations on site.

The countries of the Arab/Islamic region are an important field of action because effective protection against danger and law enforcement must also begin in those very countries that are particularly affected by terrorist activities. To date, the BKA has dispatched liaison officers to nine Arab countries[72] – as well as to Afghanistan and Pakistan – and is providing reconstruction assistance for Afghanistan and Iraq. The reconstruction assistance comprises training, exchange, and co-operation programmes for foreign police officers, which are carried out in the form of scholarships, study visits, or training courses on site. Since 1982, a total of 348 foreign scholarship-holders from 77 nations have received training in Germany.

[71] Environmental scan.

[72] Tunisia, Morocco, Algeria, Egypt, Lebanon, Saudi Arabia, Yemen, United Arab Emirates, Jordan.

The European police mission EUPOL Afghanistan with its 110 staff members from 20 countries is currently supported by Germany with 26 German police officers from the Federation and federal states.[73] The support provided by the BKA includes, for example, taking care of the police academy in Kabul that has been set up by Germany, the establishment of another police academy in the north of the country (Mazar e Sharif), and the co-ordination of the reform of the Afghan police.

The training measures for Iraqi police officers, which are being carried out in co-operation with the United Arab Emirates (UAE), comprise, among other things, the fields of crime-scene work/evidence gathering, criminal investigations, and personal protection. To date, a total of 450 Iraqi police officers have been trained in the UAE. Since Germany continues to attach great importance to the training of Iraqi police officers, a training course for bomb disposal experts is currently planned to be carried out in Jordan. Should Jordan prove valuable as a training country, this "pilot project" is to be followed by additional courses, also with other thematic priorities. Moreover, Iraqi bomb disposal experts are trained in Germany. Germany also participates in the EU Rule of Law Mission EUJUST LEX where high-ranking officials from the police, the courts, and the prisons system receive advanced training in the EU member states. To date, Germany has provided advanced training to 147 Iraqis – inter alia on the subject areas "Management of Investigation" and "Senior Police Leadership."

The material assistance that the BKA offers to foreign police authorities includes, for example, the provision of computer equipment or the expansion of the motor vehicle fleets of local police forces and ranges all the way to the delivery of special equipment for carrying out forensic examinations (e.g., DNA analysis and gas chromatography). The training and material assistance is part of the support programmes of the Federal Government to improve the performance of foreign police forces in combating crime, securing borders, and furthering law and order and democracy.[74] However, because of the BKA's European orientation, the focus of the support provided is shifting more and more towards training assistance (keyword: capacity building).

In addition, the current total of 63 BKA liaison officers at 51 locations in 49 countries promote not only a bilateral exchange of information but also a comprehensive strategic and at the same time tactical observation of the crime situation in the respective region. The liaison officers of the BKA represent the interests of the German police in the host country and at the same time can perceive developments which may be of significance to the crime situation in the Federal Republic of Germany in good time, thus making a decisive contribution to the aforementioned goal of early detection. In 2006, further liaison officers were dispatched to Islamic regions (Kuwait and Saudi Arabia). Furthermore, they support the law-enforcement authorities of the host

[73] EUPOL was increased to 230 staff members by April 2008. Altogether, an increase in the number of persons to approximately 400 and an extension of the German contingent to 120 police officers is planned.

[74] *See also* Roell, 2003, p. 125 (138 f.).

country when investigations with links to Germany are concerned. The specific coaching of security services on site takes place with the aim of reinforcing the relations with foreign co-operation partners, to achieve a greater sense of obligation to agreements and increased sustainability of support measures, as well as to obtain additional information on issues of relevance to the security of Germany.

1.6 Research

1.6.1 Forschungsstelle Terrorismus/Extremismus

Prevention work in the field of international, Islamist-motivated terrorism is particularly difficult, because only little confirmed information on the phenomenon is available – not least due to its present significance and the low number of cases. The German criminal police are therefore not relying only on intelligence work, that is to say the systematic collection, analysis, and assessment of data, but are building up the Forschungsstelle Terrorismus/Extremismus (FTE)[75] within the Institute of Law Enforcement Studies and Training of the BKA. The FTE has set itself the goal of researching the fundamental aspects and developments in the field of terrorism/extremism. It works closely together with those operational units of the BKA dealing with counterterrorism and the police and non-police research institutes, and organizes the transfer of knowledge between the bodies involved. Since early detection and research into the causes have particularly proven to be central factors in counterterrorism, a monitoring system adequate to the phenomenon is to be introduced. The long-term aim is to forecast trends in the field of terrorism/extremism on the basis of known social conflicts and the analysis of the extremist and radical scene. The purpose is not to predict concrete offences or attacks but to monitor the threat and escalation potential. The information gained in this way is to enable the security authorities to react in a timely and coordinated manner. Apart from that, the FTE conducts both a qualitative study for the comparison and research of the biographies of violent extremists and secondary analyses for general research into terrorism and the potential number of fundamentalist people in Germany.

Up to now, there is hardly any firm knowledge about the motivation of Islamist terrorists and the processes of “radicalization” of originally peaceful Muslims to become (suicide) attackers. The central questions addressed by the FTE are given below:

1. Why does this offender act in this particular way at this place at this time?
2. Will we succeed in predicting threat scenarios on a scientifically founded basis?

In addition, the following more detailed questions on the radicalization of young Muslims appear to be in need of clarification:

[75] Terrorism/Extremism Research Unit.

1. Is Islamist radicalization spreading among apparently integrated Muslim youths, leading to a home-grown, not imported threat to the internal security in Europe?
2. What role does the ethnic-religious distribution of migrants in Europe and/or in Germany play? Could home-grown terrorist groups establish themselves in our country, too, and what role do "hate preachers" play in the radicalization process?
3. How can we improve our knowledge about the social and cultural background conditions that influence the Islamist radicalization processes in Germany?
4. To what extent can possible experiences of humiliation and marginalization, potential for aggression and identification deficits lead to the radicalization of young Muslims of the second and third generation of migrants in Germany?
5. How can one better understand the individual psychological experience of an "Islamist awakening" and the ensuing behavioural changes (ritualization of life in accordance with Islamic rules)?

"Understanding terrorism," however, means not only knowing about the offender but also comprehending what effect the respective terrorism has on the population and the – in part directly targeted – social institutions. Basically, it must be assumed that there are dynamic interactions between the terrorist protagonists, the instances of social control, the political/social decision-makers, the media, and the population as a whole. With regard to the development of an adequate security policy, the research activities of the FTE are therefore not only restricted to an isolated consideration of terrorist groups but also include surrounding social and cultural conditions as well as phenomenon-related protagonists. While a first expert colloquium in 2005 dealt with basic methodological problems, a second colloquium in 2006 addressed the initiation of concrete empirical test projects ("feasibility studies").[76]

At present, for example, the FTE is working on a research project where the biographies of extremists (left-/right-wing/Islamist) are analyzed (extremisms from the biographic perspective/EbiP). One of the aims is to establish the differences between religiously and politically motivated extremism and to analyze the process of radicalization. First results show that radicalization of extremists can be divided into the following four phases:

1. The phase of "ideological experimentation"

(Ideological commitment and behaviour patterns not yet consolidated; typical for this phase is experimentation with the ideas and symbols of the respective extremism with the purpose of provoking reactions in the person's own environment)

2. The radicalization phase

(Identification with the respective extremist ideology but not yet violent)

3. The recruitment phase

[76]The results of the first colloquium have been published in Kemmesies, 2006.

(Identification with the respective extremist ideology and propensity to violence but, so far, no concrete intentions to act)

4. The phase of terrorist activities

(Empathy with the respective extremist ideology, propensity to violence, and concrete preparatory acts – for example, training, information gathering, and preparations for an act)

The phases represent a kind of "career model." In general, both further radicalization and retrogression to an earlier stage are possible in every phase, which means that the radicalization process is not irreversible. The described stages of development are apparently furthered by the fact that the persons concerned have difficulties to cope with challenges normal for their age and critical life events.

Especially the "ideological experimentalists" (phase 1) are of particular importance with regard to crime-preventive aspects: At this stage, their personal environment as well as government authorities and institutions (family, school, police, justice, youth welfare services etc.) have the opportunity to counter extremist tendencies, which could become more and more set. The "stage of experimentation" appeals to all parties involved in the socialization process of adolescents not show indifferently vis-à-vis extremist statements. Lack of intervention is often (mis-) interpreted by the persons concerned as indifference and or even approval. The reactions from the environment are decisive as to whether and how mere experimentation leads to actual radicalization.

The evaluation of investigative results achieved so far shows that idols such as hatemongering clerics, who are known to be good rhetoricians, to possess charisma and to have a sound knowledge of religious issues, can play a decisive role in radicalization. Often Koran studies abroad also have a share in the radicalization process. Stays in a training camp are, on the one hand, meant to consolidate the ideological-religious attitude and to develop military capabilities – such as building bombs. On the other hand, future jihadists attending training camps receive instruction in the use of laptops as well as in undercover communication and data storage. Attendance at a training camp is, in most cases, the final stage of the radicalization process, the transformation from an Islamist to a violent jihadist.

Taking into account that Islamist circles use the Internet as a central means of communication for sharing information and disseminating Islamist propaganda, the Terrorism/Extremism Research Unit is running the project "Net Crawler." A software (Net Crawler), specifically developed by the BKA, automatically checks certain Internet sites for modifications on a daily basis. This approach is based on the assumption that the modification of extremist Internet sites is an early indicator of changes in the extremist community and of emanating offences with an extremist motivation. At this point, particular mention should be made of the activities pursued by the BKA's Central Unit for Random Internet Searches. The objective of the Central Unit for Random Internet Searches is to search the Internet and online

services for contents prohibited by law and thus enable early intervention ("cyber police patrols").[77]

In June 2007, while Germany was holding the Presidency of the European Council, the BKA invited about 80 experts from the police, intelligence services, and external research institutions of all EU member states to discuss perspectives and potentials of monitoring the phenomenon of terrorism/extremism as part of a long-term security strategy at European level. One result was the setting up of a European Expert Network on Terrorism Issues (EENeT), to facilitate a sustainable networking of the research sector and security agencies as well as the combining of resources. The network is designed to tackle terrorism issues in a multidisciplinary way and to promote international co-operation among the different players involved. It is planned to exchange new analysis approaches and research results through a public Internet platform operated by the BKA. In addition, further expert meetings are scheduled to be held on a regular basis to initiate concrete co-operation projects.

1.6.2 Research Programmes

1.6.2.1 European Level

Since 2004, major developments have also been observed in the rather technically oriented so-called security research. With particular regard to the phenomenon of international terrorism, research activities must not be allowed to remain limited to the national scientific environment. At European level, the European Union presented the European Security Research Program/ESRP in September 2004. Embedded in the seventh European Research Framework Program (term: 2007–2013; budget: 1.4 billion Euros), the ESRP serves the higher strategic goal of strengthening the competitiveness of European industry. The aim is to develop and implement research results and technological innovations directly for security-related projects within the framework of appropriate research programmes. The priorities are given below:

1. Protection against terrorism
2. Improvement of the awareness of the situation in security-related matters (prevention)
3. Optimization of security and protection of networked systems
4. Improvement of crisis management
5. Interoperability and integration of information and communications systems

[77] Incident-related searches differ from random searches because the latter are not conducted in response to external sources, that is, specific information or complaints or requests from other services, or in support of investigations but are rather the result of regular and systematic searches for evidence of all types of crime. cf. Kerner/Stierle/Tiedtke, *Kriminalistik* 2006, p. 292 (298).

The European Security Research Advisory Board (ESRAB), which is composed of 70 experts and currently has 5 German representatives, acts as an advisory body to the European Commission (COM) and assists the COM in the elaboration of a long-term vision, specific contents, and a strategic agenda. To draw up the strategic agenda for security research and innovation, which needs to be completed by the end of 2009, the ESRAB has developed a total of eleven thematic working groups: "Security of citizens" (inter alia against organized crime and terrorism), "Security of critical infrastructures," "Border security," "Crisis management," "Prognoses and scenarios," "CBRNE,"[78] "Situation monitoring," "Identity management concerning persons and objects," "Innovation and the European security market," "Control and co-ordination," and "Socio-economic and ethic questions." The selection of these topics satisfies the demand of the German police to not only pursue a technological research approach but also to deal with the causes and development of terrorism from a socio-scientific point of view, to forecast trends by new scenario and early detection methods, and to take a sociological research approach aimed at examining radicalization processes or public acceptance of tightened security measures. In December 2007, the working groups – each comprising up to 100 experts from the EU member states – assumed activities by precisely describing their goals and working methods.

1.6.2.2 National Level

In 2006, Germany, acting in accordance with examples given at European level, also adopted a security research programme ("Civilian Security Research") covering the period 2007–2010 and based on a budget amounting to 123 million Euros. The national programme is meant to encourage higher investments in civil security research and stronger scientific competition, to create a nationwide network of suppliers and users from the areas of research and industry as well as product appliers from the public and private sector for coordinating the identification of future threats and possible solutions, and to fix key objectives – also taking into account strategic aspects such as a research strategy orientated towards market and export opportunities. The main subjects of research are closely adapted to topics fostered by the European programme to create synergies and prepare Germany specifically for European research projects covering various issues. Similar to the European one, the German programme places emphasis on the necessity to carry out multidisciplinary security research that creates a link between technological and socio-scientific questions. Research work concerning the humanities and social sciences is expected to produce, above all, approaches to the following subjects:

1. Necessity and acceptance of security solutions, their effects, and consequences
2. Risks emerging from their freedom-limiting impact

[78] CBRNE stands for chemical, biological, radiological, nuclear, explosive substances.

3. Societal costs and benefits of security measures and strategies
4. Threat scenarios, especially in the fields of organized crime and terrorism/extremism, and the resulting demand for security solutions

1.7 Conclusions

Despite the relatively small number of cases compared, for example, to violent crime motivated by right-wing or left-wing extremism, international terrorism motivated by Islamist ideology is currently the greatest potential threat. As demonstrated by the events in New York, Madrid, and London, and the attempted attacks in Germany, a single "successful" attack (as viewed by the perpetrators) can already have devastating consequences.

The security authorities of the countries concerned are confronted with constantly changing new threats: differing modi operandi as well as perpetrator and offence profiles call for a continuous readjustment of the threat assessment. The security authorities must continue to anticipate attack scenarios that may differ from those committed in the past. Conceivable future scenarios could include, for example, attacks on maritime transport or the use of information technologies as a weapon against critical infrastructures such as nuclear power plants (so-called cyber terrorism).[79] Accordingly, established policies have to be adapted, new ones developed. To combat international terrorism motivated by Islamist ideology, Germany follows a comprehensive holistic approach: All responsible state authorities – as well as relevant non-governmental actors – are to link their initiatives and to exchange their information quickly and reliably; the law enforcement agencies are to reinforce prosecution efforts and to point out gaps in legislation as well as justify the need for amended and new legislation on investigative competences.

A comprehensive, holistic approach emphasizes especially the aspect of prevention. Effective prevention work requires systematic augmentation of information about organizations, structures, persons, and places associated with the Islamist scene as well as about planned acts of violence. If danger protection and law enforcement measures in the field of international terrorism are to be successful, above all a solid information base is necessary. The network of terror must be countered by a network of information. On the one hand, at national level, this requires a high degree of solidarity between the security authorities and other actors in the field of counterterrorism: Active and continuous collection of information is just as necessary as a regular, timely, and comprehensive exchange of information with other security authorities and offices at the police level of state security. However, in view of the fact that data and capital flows are networked at international level and also considering the mobility of terrorists and their supporters, a suppression strategy directed solely or primarily at the national level is inadequate. This is demonstrated by the developments in Iraq,

[79] cf. Falk/Schwartz, *Internationale Politik* 2005, p. 28 ff.

Afghanistan, Saudi Arabia, and Sudan as well as other parts of the world. Efforts are currently focused on enabling early detection of terrorist threats by collection and compilation of the information on hand at intelligence and police services as well as diplomatic missions and business institutions in Germany and abroad. The significance of the Joint Counter-Terrorism Centre, the Anti-Terror Database, the Joint Internet Surveillance Centre, and the Joint Analysis and Strategy Centre for Illegal Migration must be judged against this background.

To deprive terrorist groups of ideological nourishment, it is also necessary to communicate the values of a free democratic society in the context of a global political discussion. Here the BKA participates in the peacekeeping measures of the international community. Through its long-term commitment within the framework of missions abroad, the BKA contributes to the political stabilization and democratization – in the sense of participative elements – in the respective crisis areas. Inside Germany as well, valuable prevention work involves in particular imparting the values of the free and democratic constitutional system and preventing the development of parallel societies.

In this connection, extremist religious agitation aimed at destabilizing the constitutional democracy from within would be a cause for great concern.[80] This applies in particular to young persons, who are supposed to be kept from drifting into extremist circles. Here efforts to integrate migrants into German society are of special importance. Naturally the police also have to be sensitized to the specific problems of migrants, which can be accomplished in part by assigning officers who also have a migrant background. At the same time, Muslims need to be more fully integrated into German society by means of confidence-building measures – in particular, on the basis of an intercultural dialogue. This is certainly one of the conditions for effective implementation of a rational domestic security policy that is also accepted by Muslims.

Furthermore, a holistic approach to suppression also requires a comprehensive understanding of the phenomenon of international terrorism, a phenomenon we do not yet understand adequately in view of its largely foreign cultural and religious background. Thus far, almost no sociological information is available about the social structures from which the terrorists come. It is particularly difficult to obtain information due to the differing backgrounds and objectives of the perpetrators. In addition, because the case numbers are so small, it is almost impossible to arrive at generalizations. In view of this situation, the work done by the FTE at the BKA, which emphasizes phenomenological analyses, cause studies, and forecasting tools, is becoming increasingly important. The controversy about the so-called Muhammad caricatures at the beginning of 2006 provides impressive confirmation of this. Finding solutions to the potential conflicts of the twenty-first century also makes it necessary to take a close look at the significance of “culture” and “religion” as sources of terrorist violence.

[80] Krause, 2004, p. 75 (78 f.).

References

Alexiev, Alex: Wegschauen und verharmlosen. In Europa wird der islamistische Terror immer noch unterschätzt, Internationale Politik, September 2005, S. 92–98.

Backes, Uwe/Jesse, Eckhard: Islamismus – Djihadismus – Totalitarismus – Extremismus, in: Backes, Uwe/Jesse, Eckhard (Hrsg.): Extremismus & Demokratie, Baden-Baden 2002, S. 13–26.

Baumann, Karsten: Vernetzte Terrorismusbekämpfung oder Trennungsgebot? Möglichkeiten und Grenzen der Zusammenarbeit von Polizei und Nachrichtendiensten, DVBl, 2005, S. 789–805.

Brück, Tilmann: Die wirtschaftlichen Folgen des weltweiten Terrorismus, in: Netzwerke des Terrors – Netzwerke gegen den Terror. BKA-Herbsttagung 2004, München 2005, S. 75–84.

Buermeyer, Ulf: Die "Online-Durchsuchung." Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS, Heft 4, 2007, S. 154–166.

Bundesministerium des Innern (Hrsg.): Verfassungsschutzbericht 2007, Berlin 2008 (zitiert: Verfassungsschutzbericht 2007).

Di Fabio, Udo: Sicherheit in Freiheit. Vortrag an der Bundesakademie für Sicherheitspolitik (BAKS), 06.11.2007.

Eisenberg, Ulrich: Kriminologie, 6. Auflage, München 2005.

Elger, Ralf (Hrsg.): Kleines Islam-Lexikon, 3. Auflage, München 2001.

Falk, Ophir/Schwartz, Yaron: Piraten unter grüner Flagge. Islamisten haben das maritime Transportwesen im Visier, Internationale Politik, November 2005, S. 28–31.

Hauschild, Thomas: Auf den Spuren von Al-Qaida, Internationale Politik, November 2005, S. 32–49.

Hofmann, Manfred: Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ, Heft 3, 2007, S. 121–176.

Ignatieff, Michael: Freiheit und Armageddon. Wie können sich Demokratien gegen nuklearen Terror verteidigen? Internationale Politik, November 2005, S. 52–62.

Intelligence and Security Committee: Report into the London Terrorist Attacks on 7 July 2005, London 30.03.2006.

Jesse, Eckhard: Formen des politischen Extremismus, in: Bundesministerium des Innern (Hrsg.): Extremismus in Deutschland, Berlin 2004, S. 7–24.

Kaiser, Günther: "Kriminologie." 3. Auflage, Heidelberg 1996.

Kemmesies, Uwe E. (Hrg.): Terrorismus und Extremismus – der Zukunft auf der Spur. München 2006.

Kerner, Hans-Jürgen/Stierle, Claudia/Tiedtke, Ingo: Kriminalitätsbekämpfung durch Behörden des Bundes. Ein Überblick über nationale, europäische und internationale Elemente, Kriminalistik, Heft 5, 2006, S. 292–304.

Klink, Manfred: Konzepte zur Bekämpfung des islamistischen Terrorismus, Der Kriminalist, Heft 9, 2003, S. 341–346.

Klink, Manfred: Polizeiliche Bekämpfung des islamistischen Terrorismus, in: Bundesakademie für Sicherheitspolitik (Hrsg.): Sicherheitspolitik in neuen Dimensionen, Ergänzungsband I, Hamburg 2004, S. 89–106.

Körper, Rudolf: Ein neues Sicherheitskonzept: Das erste und zweite Anti-Terror-Paket im Überblick, dnp, Heft 1, 2002, S. 20–23.

Krause, Joachim: Eine neue Dimension – Europa braucht eine Strategie gegen islamistischen Terror, Internationale Politik, Heft 4, 2004, S. 75–83.

Meyer-Goßner, Lutz: Strafprozessordnung, 50. Auflage, München 2007.

Müller, Harald: Internationaler Terrorismus in: Knapp, Manfred/Krell, Gert (Hrsg.): Einführung in die Internationale Politik, München, Wien, Oldenburg 2004, S. 480–511.

Nehm, Kay: Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur, NJW, Heft 46, 2004, S. 3289–3368.

Neubacher, Frank: Politik und Verbrechen, MschrKrim, Heft 4, 2002, S. 290–300.

Pfahl-Traughber, Armin: Gewaltbereiter und gewalttätiger politischer Extremismus in Deutschland, Kriminalistik, Heft 4, 2003, S. 202–208.

Report of the Official Account of the Bombings in London on 7th July 2005, London 11.05.2006, 22.05.2006.

Raisch, Peter: Bekämpfung des internationalen Terrorismus, dnp, Heft 2, 2004, S. 30–33.

Roell, Peter: Deutschlands Beitrag zur internationalen Terrorismusbekämpfung, in: Hirschmann, Kai/Leggemann, Christian (Hrsg.): Der Kampf gegen den Terrorismus. Strategien und Handlungserfordernisse in Deutschland, Berlin 2003, S. 125–142.

Schrader, Tobias: Die Anti-Terror-Pakete ein Jahr nach ihrer Einführung, Kriminalistik, Heft 4, 2003, S. 209–212.

Singer, Jens Peter: Erfassung der politisch motivierten Kriminalität, Kriminalistik, Heft 1, 2004, S. 32–37.

Tibi, Bassam: Vom klassischen Djihad zum terroristischen Djihadismus – Der irreguläre Krieg der Islamisten und die neue Weltunordnung, in: Backes, Uwe/Jesse, Eckhard (Hrsg.): Extremismus & Demokratie, Baden-Baden 2002, S. 27–44.

Tröndle, Herbert/Fischer, Thomas, Strafgesetzbuch und Nebengesetze, 54. Auflage, München 2007.

Würz, Wolfgang: Die Zusammenarbeit der (Bundes-) Sicherheitsbehörden im Phänomenbereich islamistischer Terrorismus – Das Gemeinsame Terrorismusabwehrzentrum Berlin-Treptow, Kriminalistik, Heft 1, 2005, S. 10–13.

Ziercke, Jörg: Wissenschaft und Praxis im Kampf gegen den Terrorismus, in: BKA (Hrsg.): Netzwerke des Terrors – Netzwerke gegen den Terror. BKA-Herbsttagung 2004, München 2005, S. 15–30.

Chapter 2
Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet

Dr. Phillip W. Brunst

2.1 Introduction

Although it is known that terrorists already routinely use the Internet for purposes such as spreading propaganda or conducting internal communication, the threat that results from this use is heavily debated. Especially the question whether a cyber terrorist attack is imminent or if it is only a purely fictitious scenario is subject to many discussions. One reason for these differences in opinion is a lack of exact terminology. Already for the term "terrorism", more than 100 different definitions with more than 20 definitional elements have been identified (for further details, see Record 2003). The addition of "cyber" to this word already fraught with meanings does not help to clarify this issue. Consequently, current interpretations of "cyber-terrorism" range from very narrow to very broad. A more narrow view is often worded close to common terrorism definitions and might include only politically motivated attacks against information systems and only if they result in violence against noncombatant targets (Pollitt 1998). Broader approaches often include other forms of terrorist use of the Internet and therefore might define cyberterrorism as almost any use of information technology by terrorists (National Conference of State Legislatures 2002). To complicate matters even more, additional terminology is being introduced into the discussion, e.g. "digital Pearl Harbor", "electronic Waterloo", "Cyber war", or "electronic Chernobyl". These terms, however, focus mainly on the effects of possible future attacks by terrorists. Therefore, they rather cloud the discussion about a precise terminology on cyberterrorism or a terrorist use of the Internet.

This chapter is divided into three parts that depict the problematic areas that are currently under discussion. Part one will deal with what is usually considered as "real" cyberterrorism: attacks that are carried out via the Internet and that are aimed either at other IT systems or at real-world property and human lives. Part two will then cover issues that might not be considered as cyber terrorism in a narrow sense,

Dr. P.W. Brunst (✉)
Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: phillip@brunst.de

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_2,

but rather a use of the Internet for terrorist purposes. Finally, part three will cover uses of the Internet that might commonly be regarded as conventional or even harmless. A look in more detail will reveal, however, that even the everyday use of the Internet can offer some specific advantages for terrorists.

This chapter will not go into further details of the problems of defining cyberterrorism or a terrorist use of the Internet. Instead, it will give – as outlined above – an assessment of the risks and thus the threat of terrorists who can use the Internet for their purposes. The underlying term "terrorism" is for this reason understood in a broad sense to allow an expanded view of the risks and chances.

Furthermore, to allow a realistic risk analysis, it is not sufficient to look only at cases of terrorist involvement that have officially been confirmed. Often, the facts of such cases will be kept confidential, e.g. because they affect issues of national security. Therefore, this analysis is based on cybercrime and cyberterrorism literature as well as on specialized security reports, case studies, and news reports. Only such a broad approach allows the inclusion of occurrences of the past and also gives consideration to possible future threats.

2.2 Attacks via the Internet

Attacks that are launched over the Internet are commonly known as integral parts of what is commonly called "cyber crime". Formerly, perpetrators in this area were often young hackers, keen on experimenting with security-related issues and curious about technology. In the meantime, however, this situation has changed. Instead of experimenting youngsters, highly organized groups that use attacks as a source of income, businesses that conduct industrial espionage, and states engaging in electronic warfare can be observed. The only group of actors that seem to be missing are the terrorists who rarely admit to computer-related aggression. Nevertheless, this is no reason for an all-clear. The events in Estonia in 2007, for example, have shown that even whole countries can be put at risk without the use of a single conventional weapon.[1] This will not go unnoticed by terrorists. A more thorough look at the motivation of terrorists for attacks over the Internet is therefore of the essence (Sect. 2.2.1) before looking at the concrete possibilities for terrorist attacks (Sect. 2.2.2).

2.2.1 Motivation

Some authors claim that, to date, not a single instance of cyberterrorism has been recorded (Sieber 2004). According to informal sources, however, many attacks have

[1]See the section " Denial-of-Service Attacks" for further details on the Estonian case.

already taken place, but are kept confidential due to the security threat to important infrastructures that would evolve from details becoming publicly known. Whatever the case may be, it is undeniable that the threat of terrorist action over the Internet is realistic. Already this fact can (and is) abused by terrorists as a form of psychological warfare: cyber-fear is generated by the fact that what a computer attack *could* do is too often associated with what *will* actually happen (Weimann 2006).

2.2.1.1 General Motivation

Beyond the potential for psychological warfare, five main issues are relevant for a general motivation to commit crimes over the Internet:

Location Independence

Attacks in the Internet are not bound to a definite physical place. Although it is necessary to visit the locality of a conventional attack, e.g. to "case" the target or place the bomb, cyber terrorists do not have to be physically present at the place of their deed. This is a great advantage over conventional attacks where the danger of being suspected during the preparation phase or even detected immediately before the commitment of the crime is omnipresent. For any cyber crime, it is sufficient to be connected to the Internet from any place on earth. This can be a static connection, e.g. at home or at an internet café, or a mobile connection, e.g. over a cellular telephone.

Often, it is assumed that many countries that host terrorist groups are not well enough equipped with Internet connections to pose a real threat. However, this is true only with regard to the current status. The Internet penetration rates of North America, Australia, or Europe are still clearly above those of Africa, for example (Miniwatts Marketing Group 2007). The increase of Internet users within the last years, however, was extremely fast, in some countries, even close to 5,000% within the last 7 years (Miniwatts Marketing Group 2007). Especially the number of Internet cafés that can be used for rates affordable even to the poor has rapidly increased in most major cities during the last years. This allows large parts of the population (and the terrorists among them as well) to access the Internet without any further control.

Speed

Attackers are hardly dependent on their own connection speed for attacks that are launched over the Internet. Instead, they can use the bandwidth and speed of third parties, e.g. to launch distributed denial-of-service (DDoS) attacks.[2] The party's

[2]DDoS attacks are a way to hinder the accessibility of computer systems. For further details, see below.

own connection speed is needed only to distribute commands to the systems attached or to receive feedback about the successes. In both cases, even slow, low-bandwidth connections are sufficient.

The aspect of independency is true also for those attacks that act without human interaction, e.g. viruses or worms. These programs – once released by their creators – act on their own. The speed of their spreading is determined solely by the connection speed of the victims that help them to spread. This could be observed, for example, by the speed in which the Sapphire-, the Melissa-, or the I-Love-You-Worms spread during 1999 and 2003. None of them was dependent on the link-up of their creators.

Finally, the possibility to create and test malicious computer programs can be used to prepare action for future events. This makes it possible to react in a seemingly spontaneous manner to incidents, even though the preparation took place long before ("cyber revenge").

Anonymity

The anonymity of perpetrators is often alleged as a core feature of Internet-based communication. It is necessary to remember, however, that an IP address at least is transmitted with every step taken on the Internet. This can be used to get evidence of the person who initiated certain actions over the Internet. In many cybercrime cases, this can successfully be used to arrest the real perpetrator who thought that just by using the Internet he would remain anonymous.

Technologically knowledgeable people, however, have ways of hiding their identity and camouflaging their trail to an extent that makes a prosecution hard or – in some cases – impossible (Brunst 2009). The IP address of a user of an Internet café, for example, is transmitted as it is in any other case. If the owner of the establishment is not obliged or fails to register their users, however, the lead will end at the Internet Café without any further possibility to identify the culprit. Similar problems arise with wireless networks (WLAN) that – if not especially protected by the possessor – can be used to access the Internet by almost anybody within the range of the access point.

Apart from these purely organizational means, a number of additional – more technical ways – of hiding the identity on the Internet can be used. Perpetrators, for example, use proxy servers, anonymity networks, or they simply route their traffic over hacked computers of innocent users. In any of these cases, the trace cannot be followed to the computer of the perpetrator, who then cannot normally be identified either.

Internationality

The Internet connects countries regardless of their physical borders or diplomatic or political relations. Nation states, however, are still acting according to their national sovereignty, not as an operator or supervisor of a globally active network. This is

actively being taken advantage of by criminals. The aspect of internationality therefore has to be seen in close context with the anonymity and independency of place.

Examples of this technique are manifold. Especially in the area of controversial contents, it can be observed that perpetrators actively seek countries with more liberal free-speech laws to host their contents. Because content that is made available on the Internet, e.g. on the World Wide Web, is accessible from all over the world, the physical places of someone offering information and of a person accessing these data can easily differ. Other examples concern attacks that are routed through different computers to hide the traces. Often, the routing is deliberately chosen to pass through countries that do not cooperate either in criminal matters or at least in cybercrime matters. Alternatively, the routing can pass through countries where it is known that the technical capabilities of investigating cybercrime are not developed far enough to successfully gather evidence – a particular problem when considering internationally operating terrorists.

Cost-Benefit Ratio

When choosing targets and weapons, terrorists are often bound to a rigorous cost-benefit analysis of their own definition. Actions that bear a great risk of being detected too early or that will not achieve high visibility (and therefore fear in the population) have to be disregarded in favour of more "efficient" instruments (Giacomello 2004). Attacks committed over the Internet – at least in general – have an extremely positive cost-benefit ratio.

On the one hand, such attacks require only minimal initial investment. Computers are cheap and nowadays, in many areas of the world, are already part of daily life. Furthermore, an up-to-date computer model is not required. Because speed does not play an important role (as shown above) a computer of the last product line or even the generation before will be sufficient. Even some of the newer mobile phones can be used for simple Internet access. If these options are – for any reason – not available, Internet cafés that are found in any major city can also be used to cheaply access the Internet. The information that is needed to find relevant security holes and technical possibilities for exploitation is also available cost free.

On the other hand, even small attacks against targets lead to high costs for their owners. Constant updating, state-of-the-art equipment, and permanent monitoring is required to protect systems even against the so-called script kiddies.[3] Therefore, costs for personnel, machinery, and software constantly put pressure on the owners of publicly accessible computer services.[4] The Internet can therefore be seen as

[3]"Script Kiddies" is a term commonly used to describe people who do not possess the knowledge to build attacking software by themselves and who therefore have to rely on "ready-to-use" construction kits. Successful attacks by script kiddies are thus often only possible against very poorly protected targets.

[4]The White House, for example, has just allocated a sum of 6 billion US dollars for the strengthening of its systems against cyber attacks (Johnson 2008).

a form of "force multiplier". This military term means that the striking power potential of a unit is increased without increasing the personnel at the same time (White 1990). Especially for smaller terrorist groups this is true, because the Internet allows them to create harm much larger than possible with their conventional capabilities. Furthermore, the Internet can be used by them to create the illusion of greater size and power as well as having more followers than is truly the case. This, in turn, will lead their opponents to defensive measures that are far-reaching (and therefore, again, more costly) then objectively necessary.

Specific Terrorist Motivation

These five main areas of motivation are valid for terrorists as well as for ordinary cyber criminals. Differences can, however, be observed with regard to the underlying agenda (Brunst 2008). Terrorists aim primarily at the generation of fear, the creation of economic confusion, or a discrimination of the political opponent. Apart from these main motives, the generation of monetary income or the gathering of information (either for conventional or for electronic attacks) can also be objectives. To conduct actions over the Internet is only one way to achieve these goals.

The problematic issue relating to the terrorist intention behind action on the Internet is, however, that it is often undetectable. If, for example, a hacking attack with the aim of shutting down important systems at an airport is successful, terrorists will probably have an interest in making this publicly known to arouse fear in the population. In this case, it is easy to determine terrorists because the source of a cybercrime act and also the underlying agenda is clear. If, however, a hacking attack is committed in the hope of gaining information on the automobile route of an important person, this might be kept secret so as not to endanger future plans for a bomb assassination of that person (Brunst 2008). In this case, it is unknown that the act was committed by terrorists. Additionally, even if this fact would emerge, the specific intention of the perpetrators, i.e. *why* the hacking attack occurred (e.g. test of technical capabilities, preparation of conventional attack or allotted victim), would still be unknown. Therefore, from a purely objective perspective, in many cases the distinction between ordinary cybercrime and cyberterrorism is hard to make.

2.2.2 Attacks

Any attack with a computer – maybe with the unlikely exception of physical attacks with computer hardware – is aimed at another computer system. However, with respect to the terrorist intention and the outcome of cyber attacks, a distinction should be made between attacks that are actually aimed "only" at other computer systems and those that are intended to harm human lives.

2.2.2.1 Attacks Aimed at Other IT Systems

Attacks that are aimed at other IT systems can serve different intentions. Often, a first aim will be to get access to the computer system. This can be achieved either with technical means or with the help of deceiving users and administrators (see the following section on "Illegal Access"). If such an attack is successful, data that is stored or otherwise handled through this computer can be changed (see the section "Data Alteration") or secretly copied from the machine (see the section "Data Espionage"). In many cases, however, terrorists will not even try to gain access to the computer. Instead, it might be sufficient – as with a conventional attack – to hinder the system from functioning correctly. The use of either denial-of-service (DoS) attacks (see the section "Denial-of-Service Attacks") or even conventional attacks on computer infrastructure (see the section "Conventional Attacks on IT Infrastructure") can be a successful means to achieve these goals. Finally, a combination of classic conventional and new electronic attacks is regarded as a main threat by many experts (see the section "Hybrid Attacks").

Illegal Access ("Hacking")

Hacking, i.e. the illegal access to computer systems and data, is the scenario where problems, action, and results of terrorists and other cyber criminals probably differs the least. In general, a differentiation between illegal access by only technical means and access with human help can be made. An example of purely technical access would be the use of a computer program that uses software flaws that have been identified to gain access to a system (so-called exploit). Some exploits have already been available for a long time and will work only if a system administrator was not able to keep their computer up-to-date. Other exploits, however, are not known to the public or even the software manufacturers. These "zero-day exploits" or "less than zero-day exploits" can be acquired on the black market and will give access to systems, even if the administrator installed all possible security fixes that were available from the software company that developed the product (Wilson 2005).

The second category refers to access with human help. This can be achieved, for example, in the form of so-called social engineering, i.e. deceiving the user to give passwords or other protected information. Other ways to gain access with human help include the infiltration of dedicated personnel or the bribing of existing staff members. In general, the choice of the right technique (or a combination thereof) depends on the individual circumstances. Therefore, successful attacks against protected targets often require technical and social skills.

According to a study of the *Center for the Study of Terrorism and Irregular Warfare*, the capabilities that are needed for successful attacks can be divided into three groups (Nelson et al. 1999):

- "*Simple – unstructured*: The capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target analysis, command and control or learning capability.

- *Advanced – structured*: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organization possesses an elementary target analysis capability and command and control structure for sequential attacks from a single location. Some learning ability – can assimilate some new technologies and train personnel.
- *Complex – coordinated*: The capability for coordinated attacks capable of causing mass-disruption. Ability to analyse vulnerabilities, penetrate integrated, heterogeneous defences (including cryptography) and create attack tools. Strong ability to conduct target analysis and high confidence in results. Strong command and control structure capable of employing multiple, simultaneous attacks from different locations. Strong organizational learning capacity – can keep up with latest technology, train personnel, diffuse knowledge throughout the organization, make necessary doctrinal and organizational changes to enhance capabilities".

Already attacks of the lowest level, i.e. "simple – unstructured" can – under some circumstances – be sufficient to successfully gain access to a computer system. However, these forms of attack will only work if it is sufficient to attack *any* system. In this case, a computer system can be sought that is vulnerable to a certain form of attack, e.g. where a certain version of a software product is installed. If it is necessary to attack a *given* target, however, the efforts to successfully attack are incomparably higher. In this case, it might be necessary to acquire certain specialized tools, like the above-mentioned "zero-day exploits".

Attacks of the highest level, i.e. "complex – coordinated", will require a high degree of innovation and technical effort. In exchange, they allow access even to systems that are extraordinary well protected. An example for a successful combination of *social engineering* and an individually developed malicious program was shown in the year 2006 by a security company. To gain access to the systems of their client (who hired them to test their computer security), the company prepared USB sticks with a custom-designed, newly developed Trojan horse program that could not be detected by virus scanners. Twenty of these sticks were "lost" on the premises of the client. Of these, 15 sticks were found by employees – and promptly connected to the company network where the Trojan started to collect passwords and other valuable information and e-mailed this data back to the offenders (Weimann 2005). Of course, such an attack would be a powerful way for a terrorist organization to initiate counterespionage.

The assessment as to what extent hacking terrorists are realistic threats differs immensely. In many countries the information about actual incidents is classified and hard to verify. According to experts, however, terrorist groups had considered the integration of hacking into their repertoire already by the end of the 1990s (Borland 1998). Today, at least some terrorists are known to possess considerable hacking skills (Embar-Seddon 2002).

Apart from the actual skills, the time that is needed to educate a group on relevant hacking skills is also under debate. Members of the US *Naval Postgraduate*

School, for example, estimated in 1999 that it would take from 2 to 4 years to acquire the skills necessary to launch "advanced – structured" attacks. For "complex – coordinated" attacks a time-frame of 6–10 years is expected (Desouza & Hensgen 2003). Because access to the Internet and therefore the amount of freely available information has enormously increased since 1999, however, it has to be doubtful that those figures can still be regarded as realistic.

Furthermore, terrorists do not have to rely on their knowledge alone. Experts assume that it is a realistic option for professional hackers to be hired by terrorist groups – in some cases without knowing about the true expectations of their customer (Borland 1998). On the other hand, most terrorist organizations have worked in conspiratorial and close environments where weapons, attacks, and personnel were chosen and tested carefully and put to use only if no risk was to be expected. Therefore, a final assessment whether terrorists would use this form of "outsourcing" remains speculative.

Data Alteration

After a successful hacking attack, a perpetrator has many options on what to do with the system. A comprehensible first reaction would be to delete information or shut down the system. However, this technique would not be successful (at least not for any length of time), because administrators would immediately notice the failure and could reconstruct the system from backup files or switch to reserve systems. The amount of damage that would result from such an attack would therefore not be too high. However, in some areas, e.g. certain industrial production facilities or in medical environments, even short outages could have disastrous consequences.

Defacements

Alterations that are visible to a large audience are often considered to be better, because they can demonstrate the technical capabilities and create fear of what other systems could fall foul of future attacks. An example of an attack that is widely recognizable is a so-called defacement that often takes place after a hacker has gained access to a web server. In this case, a page on the web server, often the prominent entry page, is altered. Often insults (e.g. to the technical incapability of the system administrators) are put on the page together with hints as to the identity of the perpetrator (e.g. the name of a hacking group). By leaving this form of "digital business card", the perpetrator can keep record of their successful break-in and therefore of their technical capabilities. While other forms of cyber crime often remain in the dark, defacements are clearly meant to be seen by a large audience.

A large-scale series of defacements could be interesting for terrorists, especially if servers that belong to security agencies, the military, or other important services are concerned. This has already been observed. In the year 2001, for example, the group "Pentaguard" demonstrated its capabilities when it simultaneously defaced a

multitude of government and military websites in the UK, Australia, and the United States. This attack was later evaluated as one of the "largest, most systematic defacements of worldwide government servers on the Web" (Leyden 2001). In another case, pro-Palestinian hackers used a coordinated attack to break into 80 Israel-related sites and deface them (Conway 2002; Vatis 2001). Even al-Qaeda used the technique of defacement to demonstrate its technological as well as its conventional dangerousness when it deposited images of the hijacked (and later beheaded) Paul Marshall Johnson, Jr. on the hacked website of the Silicon Valley Landsurveying, Inc. (Musharbash 2004).

Other Forms of Data Alteration

Other forms of data alterations are discussed mainly as theoretical threats. Unlike the defacements that were discussed above, other alterations are usually not as obvious and therefore hard to recognize. This enables them to result in great damage.

Targets that are discussed in the literature as exceptionally disastrous are, for example, databases with social security numbers, data sets of banks and other financial institutions, or collections with military and classified information. Unnoticed attacks on any of these databases could have disastrous effects on the economy of a country and result in a continuing lack of trust of the people in their systems and institutions if changes were not to be detected (and repaired) within a short period of time (Berinato 2002).

Some authors claim that activities such as a manipulation of large and central databases would exceed the capabilities of terrorist groups that are often not composed of long-time experienced hackers. Planning games such as "Eligible Receiver"[5] and current information regarding recent attacks have shown, however, that even top-secret military computers and research laboratories that are handling nuclear materials are not immune against all possible forms of electronic attacks (Vatis 2001; Wilson 2005). For a realistic risk assessment, at least the possibility that terrorists are considering or evaluating such attacks has to be taken into account.

Data Espionage

For terrorist groups, the acquisition of information about their opponent is as important as for any other organization. If, for example, it becomes known that communication channels between members of the group are being monitored or that plans for a future operation have leaked to government agencies, appropriate action needs to be taken. Because most of today's communication structure is computer based, data espionage is on the rise throughout.

Commonly, the clandestine exploration and obtaining of protected digital information was originally particularly known between states that try to acquire security

[5]For more detailed information about the experiment "Eligible Receiver", see Sect. 2.2.3.

relevant information from other states to gain tactical advantages. However, in the meantime, industrial espionage has also become an important factor for many economies. With regard to electronic espionage that is directed against digital information, the boundaries between the activities of individual hackers, organized groups, and state-sponsored fractions become increasingly blurred.

In a case that took place in 1999 and that was later named "Moonlight Maze", for example, hackers allegedly were able to get access for a period of more than 1 year to computer networks at the US Energy Department nuclear weapons and research labs, at the National Aeronautics and Space Administration, and at numerous university research facilities and defence contractors. Although no classified computers were known to have been breached, even the unclassified networks are said to contain confidential and sensitive data that could potentially be valuable to any foreign government or terrorist group (Drogin 1999; Thornburgh 2005a). Experts therefore claimed that the value of the information that was gathered was "in the tens of millions – perhaps hundreds of millions – of dollars" (Testimony of James Adams, Chief Executive Officer, Infrastructure Defence, Inc. 2000).

Although evidence indicated in the beginning that the attacks of "Moonlight Maze" originated from Russian computers and that the attacks were state sponsored (Drogin 1999), this was later refuted by government officials (FCW Staff 1999). As in many cases, in the end, it remained unclear as to what extent which kind of information had been accessed. In addition, it could not be determined if the computer that was really used to attack was the computer of the actual attacker, if the attacker was acting on their own or on behalf of a government, or if the computer was only a hacked computer that was used to camouflage the traces to the real offender.

Almost the same is true for a series of attacks that started in 2003 and were named "Titan Rain" by the US government. Although evidence indicated, according to experts, that it would be "unlikely to come from any other source than the [Chinese] military" (AFP News Agency 2005), the exact source of the attack, the amount of data that was acquired, and the precise nature (i.e. state-sponsored, corporate espionage, or random hacker attacks) remain unclear (AFP News Agency 2005; Espiner 2005; Graham 2005; Thornburgh 2005b).

Apart from cases where data espionage is handled either by technical means as described above or by ways of social engineering, terrorist organizations can also try to get access to sensitive information by legal means. One example concerns the Japanese Metropolitan Police Department, which hired a company for the development of a software system for the tracking of their (also partly unmarked) cars. It later turned out that a part of the software was developed by members of the Aum Shinrikyo cult – the same group that was responsible for the gassing of the Tokyo subway in 1995. This was possible because the software developers were engaged as subcontractors, thus enabling personnel clearance to be circumvented. As it turned out later, members of the cult had developed not only this piece of software, but they were engaged in activities for at least 80 firms and 10 government agencies (Weimann 2005).

Another case concerned the company Ptech in Boston. The firm was, among others, working for the US Air Force, NATO, the US Congress, and it was developing

counterterrorism software for the FBI. Accordingly, the company had access to sensitive military and similar sensitive security relevant information. According to news reports, Yassin Al Qadi, a Saudi millionaire with alleged connections to Osama Bin Laden and al-Qaeda, had invested several millions of dollars into the company (Desouza & Hensgen 2003). Therefore, the US government feared that security-relevant information could have leaked to the terrorist organization, and they raided the company premises in 2002.

Denial-of-Service Attacks

Denial-of-service (DoS) attacks are targeted at the unavailability of a system or service and have a long tradition in computer crime. Modi operandi range from a crude cutting of power cables to complex exploitations of security weaknesses. Since the last couple of years, individual attacks have been replaced by DDoS attacks. So-called bot-nets, with hundreds or even thousands of Trojan horse-infected computers, are commanded by individuals to send massive requests to single targets. These computers are often not able to handle the enormous amount of traffic and are no longer able to send answers to either the computers of the bot-net or to other – legitimate – requests. Computers that are under the attack of a bot-net therefore seem to be unreachable (Brunst 2008; Janczewski & Colarik 2005; Wilson 2005).

An impressive example of the use of bot-nets was the "Estonian Cyberwar" that took place in 2007. During a longer period of time, Estonian government, news, and banking sites were under massive attacks by bot-nets. At the same time, coordinated hacking and defacement attacks took place (Davis 2007). According to Estonian Defence Minister Aaviksoo, more than one million computers worldwide were engaged in the attacks (Sliva & Ritter 2006). Because most of the attacks originated from Russia and some evidence indicated that the coordination of the attacks was of a quality unseen before, it was assumed that the Russian government was involved in the attack. Later, however, these charges had to be dropped, because it was not possible to determine whether the attacking computers were the origin of the attack or if they were only used to disguise the real perpetrators (Davis 2007; Rolski 2007; Sliva & Ritter 2006; Traynor 2007).

DDoS attacks do not necessarily have to be launched only with technical means. To call attention to the involvement of the German airline Lufthansa in the deportation of illegal alien residents, supporters of an online demonstration were asked to open the web page of the company at the same date and time. More than 13,000 people followed the call. In return, the Lufthansa server was unable to reply to the sudden peak of requests, and the web page became unavailable to customers during this time frame (OLG Frankfurt a.M. 2006). This technique is also known as "swarming", "virtual blockade", or "virtual sit-in" and it shows that even technically non-adept organizations can use the power of distributed attacks against targets on the Internet (Denning 2001; Weimann 2004a).

Instead of launching a DDoS attack by themselves or motivating followers to engage in such activities, terrorist organizations can also "outsource" activities.

Prices for attacks range from approximately 150–400 US dollars, depending on the target and the duration of the attack. Some bot-net operators even offer discounts for multiple orders (Brunst 2008; Sieber & Brunst 2008).

In the past, it could be observed that groups were actively using DDoS attacks to push their goals. For example, six different Hizbollah sites, the Hamas site, and other Palestinian information sites were brought down by a so-called FloodNet attack of pro-Israeli hackers. The service virtually "flooded" the respective servers with pings resulting in the unavailability of the servers for all other requests. Even after a relaunch with a slightly different spelling, the sites were still unreachable because the hackers immediately adjusted the attack to the new names (Conway 2002; Denning 2001).

Conventional Attacks on IT Infrastructure

Terrorists are free in the choice of their weapons and their targets. It is only the expected success, the necessary effort, and the possible consequences that guide terrorists. Because IT infrastructure and especially the use of the Internet have become essential parts of the everyday life of most individual and corporate users, conventional attacks might also be considered as an option by terrorists. Three examples show possible scenarios.

The domain name system (DNS), for example, is essential for many services that use the Internet. It is necessary to translate a human-readable domain name (e.g. www.mpicc.de) into the IP address (e.g. 194.94.219.193) that is needed by the computer to contact the appropriate server. If an attacker was able to disrupt DNS services, large parts of the Internet would be unusable. The attempt to hamper the functioning of the 13 root-DNS servers in 2002 was therefore evaluated by some authors as an attack against the "heart of the Internet" (Weimann 2004a). However, the consequences of these attacks were hardly noticeable due to built-in safeguards of the DNS systems: no slowdowns or even outages were caused. The same is true for a recent attack that took place in February 2007: even though the aggression lasted for almost 12 hours, the influence was hardly noticeable (ICANN 2007). If, however, terrorists were able to find a way to successfully disrupt the functioning of the DNS – even for a limited region – the consequences would be noticeable immediately by all of the affected users. This, on the one hand, could result in dramatic consequences for the economy that is largely dependent on the Internet as a main connector to their customers and other businesses. On the other hand, a destruction of Internet communication could also be used in connection with conventional attacks.[6] The incidents in Estonia, for example, have shown what happens if a whole population is no longer able to access independent information about recent incidents, because Internet connections are not available. Therefore, a terrorist organization could be interested in launching a conventional attack and blocking

[6]See the section "Hybrid Attacks" below for further information on the so-called "hybrid attacks".

all (apart from traditional media) access to independent information from the Internet, thereby raising the amount of panic and the feeling of helplessness within the population.

A second approach to attack IT infrastructure with conventional means could target the intercontinental connections. For example, many transcontinental data connections rely on transatlantic cable connections between Europe and the United States. Whereas European cable ends are widely spread between many different countries, they are often bundled on the American side and could therefore be an interesting target. The effects of such an attack could be observed when cables between the United States and China were damaged accidentally (Brunst 2008). According to a survey after this mishap, 97% of the Chinese users reported problems accessing foreign web pages; 57% claimed that their life and work was being affected by the damage (Persson 2006). If committed intentionally by terrorists, economic effects, in particular, could be the consequence. Furthermore, the psychological side within the population at large (terrorists being able to "shut down" the Internet) would be interesting.

Even though the structure of the Internet is spread widely and between many different systems, important connection points between different networks exist, so-called peeringpoints that could pose as possible targets for a third approach. The German peeringpoint DE-CIX in Frankfurt, for example, is said to handle 80% of the German and 35% of European Internet traffic (according to Force10 Networks 2007). The London Internet Exchange, LINX, is the world's largest Internet peeringpoint and was in the centre of a planned assault in the year 2006. However, Scotland Yard was able to arrest the suspects beforehand so that no damage was done. An MI5 website is reported to have said in this context that "without these services, the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large-scale loss of life" (Leppard 2007).

Hybrid Attacks

Although the attacks mentioned above are either pure electronic or pure conventional, many authors see a particular danger in hybrid attacks. Hybrid attacks are aggressions that use the advantages of both the virtual and the real world, e.g. to increase the number of casualties. This, for example, could be the case if perpetrators were able to manipulate the communication systems of police and ambulances to hinder an effective coordination of rescue teams in the event of a conventional bomb attack (Vatis 2001; Wilson 2005). Reality has already shown that such a scenario is not total science fiction. For example, a hacker from Toborg, Sweden was able to partially manipulate the "911" emergency call system in Florida, United States (Borland 1998; Cilluffo 2000). It is unknown, however, if this was the intention of the hacker or only a coincidence.

Apart from these attacks that are aimed at the lives of people, other hybrid attacks are being discussed that focus on severe economic consequences. These could occur if the perpetrators were able to launch a successful assault against

national financial networks (such as Fedwire or Fednet) or against transfer networks (such as SWIFT). It is estimated that such an attack could weak havoc on the entire global economy (Wilson 2005).

2.2.2.2 Attacks Against Human Lives

Even more dangerous than attacks that are targeted purely against other IT systems are those that target human lives. To understand the concept of such attacks, it is necessary to first describe the technical background for such attacks (see the following section "Technical Background"). Afterwards, a distinction is necessary between scenarios that target immediate death or bodily harm of the victims (see the section "Attacks with an Immediate Outcome") and those that try to achieve a long-term success (see the section "Attacks with a Long-Term Effect").

Technical Background

Often, attacks against computer systems are considered less dangerous than conventional attacks with bombs, because damages to computers are said to "only" lead to economic losses. At first glance, it seems almost impossible that human lives could be endangered by mere electronic attacks. However, the convergence between a "real", i.e. physical, and a "virtual", purely electronic, world is constantly rising. Therefore, computers are no longer exclusively used to "crunch numbers" and store huge amounts of data. Instead, a new type of computing services has quietly evolved without which production facilities for food, pharmaceutical products, electricity, traffic management systems (especially for trains and airplanes), and many other military and civil establishments would be unthinkable today. So-called supervisory control and data acquisition (SCADA) systems are used to measure and control other systems.

Often, SCADA systems are either directly connected to the Internet or they are connected to internal networks that are themselves connected to the Internet. According to informal sources, 17% of SCADA malfunctions are caused by a direct Internet access to the SCADA system (Sieber & Brunst 2008). The reason for this is often the wish that systems should be ubiquitously accessible so that data and systems can be controlled remotely (Collin 1997). In the long run, owners hope to save costs if they are able to reduce personnel on site and consolidate at a central location. As a result, many connection lines that carry sensitive data exist on the ground, in the air, or in the water. All of these could pose as targets for terrorist attacks. Furthermore, a successful attack against only one site can reveal access and possibilities for manipulations at many different localities. Because many of the control systems are based on standard Windows and UNIX operating systems (Bachfeld 2003), some hackers claim that it would take them only about a week to get into most of the existing control systems (Lenzner & Vardi 2004).

The effect that SCADA systems that are connected to the Internet can have on a population could be observed in 2003 when 21 power plants were brought down, and other critically important institutions in the United States (including Edwards Air Force Base, the test centre for B-2 and B-1 bombers) were also affected. Following the incident it was discussed whether these breakdowns were the result of the W32. Lovsan worm that was using the same port to exploit a weakness on individual personal computers being used by the plants to communicate with each other (Bachfeld 2003). The collision resulted in a large power-down in the United States and Eastern Canada. It is therefore an important task to determine which parts of a national infrastructure have to be regarded as "critical", i.e. a successful attack would have a serious impact on a nation. By the mid-1990s, the US *President's Commission on Critical Infrastructure Protection* determined eight areas of critical infrastructure that were considered as vulnerable and potential targets for attacks (Embar-Seddon 2002).

Attacks with an Immediate Outcome

Most of the attacks that are aimed at critical infrastructure have an effect that is immediately noticeable. Additionally, none of the scenarios that are described below have – as far as it is known to the public – taken place yet. Nevertheless, many authors see them as realistic possibilities that could be taken into consideration by terrorists, because their outcome is more direct and visible than most of the pure attacks on IT infrastructure described above. Furthermore, they almost guarantee what is important to generate fear within a population: extensive news coverage with impressive picture material. As such, mainly three scenarios are discussed in the literature: attacks on hydroelectric dams; tampering with control systems, especially for railways or air traffic; and taking over control of power plants.

Attacks on Hydroelectric Dams

Probably the most discussed scenario of cyberterrorism with an immediate danger for human lives is an attack on a hydroelectric dam. A perpetrator could gain access to a control system and remotely open the floodgates, thereby endangering the areas and inhabitants behind the gates. The consequences of (accidentally) damaged dams could be observed in the past, e.g. when, in 1975, the Banqiao and Shimantan dams on tributaries of Hang He (Yellow) river in China failed. Dozens of lower dams were damaged and at least 85,000 people died (Gleick 2006). Today, security measures at most dams probably would prevent such extreme results. However, if terrorists were able to control a dam, e.g. by hacking into the SCADA system controlling it, a deliberate opening of the floodgates could put hundreds or even thousands of people at risk.

The danger of dams connected to SCADA systems could be observed especially in two scenarios. In the first scenario, an individual was able to break into the computer system that runs Arizona's Roosevelt Dam. Although some details of the attack are being disputed (for details, see Brunst 2008), the fact alone that the

Roosevelt dam was compromised is sufficient to show the danger of a terrorist attack. The second case concerns a case that took place in the year 2000 in Queensland, Australia. There, the culprit was able to manipulate the control system of the sewage treatment facilities over a period of 2 months, letting hundreds of thousands of gallons of putrid sludge ooze into parks and rivers. According to an employee of the Australian Environmental Protection Agency "marine life died, the creek water turned black and the stench was unbearable for residents". In the concrete case, the motive of the perpetrator was not to generate fear in the public. The damage was caused "only" to bargain for a consulting contract to fix the problems he had caused (Gellman 2002; Giacomello 2004). However, the case also shows the potential a terrorist would have for bio-related terrorism, i.e. causing illness or death not only in people, but also in animals or plants (for further details on the threat of bioterrorism see Centers for Disease Control and Prevention 2007; Committee on Water Systems Security Research 2007; Leitenberg 2005).

Attacks on Traffic Control Systems

In the attacks of 9/11, the hijackers impressively and horrifically showed the amount of damage that they could do with airplanes under their control. It is easy to imagine the possibilities and the fear that would be created if terrorists were able to gain control over airplanes or airport control systems without actually being on board.

In 1997, for example, a juvenile was able to access the communication systems of Worcester, MA airport. The action disrupted the telephone service to the Federal Aviation Administration Tower at the airport, the Airport Fire Department, and other related services such as airport security, the weather service, and various private airfreight companies. Furthermore, the main radio transmitter and the circuit that enables aircraft to send an electronic signal to activate the runway lights on approach were disabled (Berinato 2002; Cilluffo 2000; Testimony of FBI Deputy Assistant Director Keith Lourdeau on "Virtual Threat, Real Terror: Cyberterrorism in the 21st Century" 2004). Fortunately, no accidents were caused by the attack.

The incident, however, shows the vulnerability of modern transportation systems. Therefore, not only airports and airplanes (which are usually quite well protected), but also train systems are the focus of the discussion. In a worst-case scenario, colliding trains or airplanes could possibly cost hundreds of lives (Giacomello 2004; Weimann 2005).

Attacks on Power Plants

The scenario that probably causes the most fear is a manipulation of power plants, especially of nuclear power plants. A similar danger is expected from intrusions into military missile control centres. Although these premises should count as areas with the highest protection and control density, authors still see a possibility for terrorist attempts (Foltz 2004). Furthermore, the massive breakdown of nuclear power plants in 2003 that was described above (see the section "Technical Background") clearly shows that even these systems are vulnerable to cyber attacks.

Attacks with a Long-Term Effect

Some scenarios that are discussed in the literature do not result in a one-time catastrophe. Instead, they aim at a long-lasting panic, fear within the population, and a continuing distrust in local economies. As such, they pose tempting targets for terrorist groups.

One of the cases that are being discussed as a theoretical threat is the manipulation of the production line for breakfast cereals or for baby food. If, for example, a terrorist was able to manipulate the production process and change to proportion of ingredients, this could prove dangerous for the customers, e.g. if the portion of iron in baby food was increased to a hazardous amount (Collin 1997). The same effect could be induced if terrorists changed the doses or composition of pharmaceutical products and medicine (Collin 1997).

Other areas that are being discussed concern the manipulation of weapons production processes, where a manipulation could lead to useless ammunition or attacks on the economical stability of a country by way of secret manipulations on bank, currency, and transfer systems (for further details, see Brunst 2008; Sieber & Brunst 2008).

2.2.3 Risk Assessment

The scenarios that are discussed last, i.e. attacks with a long-term effect are probably the ones that have to be feared the least. The production chain of a food company, for example, is usually constantly monitored. A manipulation would therefore often be detected already at an early stage. In addition, a sudden increase in the use of different ingredients would likely draw attention. Finally, a manipulation of the composition of certain food products will most likely alter the taste of the product so that again either quality control or customers will detect the change. Other areas that were mentioned (e.g. weapons or medication production sites) are often high-risk areas, where security measures are high, and production computers are seldom linked to public networks.

The same seems – at first glance – to be true for many of the attacks that would lead to an immediate outcome. Often, the sites affected by attacks – especially military ones – are "air-gapped", meaning that they are completely physically, electrically, and electromagnetically isolated (Brunst 2008). In these cases, a remote launch of, for example, a military missile would simply be impossible (Foltz 2004; Green 2002). Furthermore, many of the situations described rely on a failure of all accompanying security measures at the same time. Especially air traffic controllers and pilots are trained regarding "situational awareness", however, and use computers only as an aid. For a successful attack, it would therefore be necessary to manipulate not only the control system, but also pilots and/or controllers (Pollitt 1998).

There are, however, no grounds for a complete all-clear:

- One reason is that it is not reasonable or sufficient to distinguish exclusively between "computer-only" and "human-only" scenarios. Many organizations will, for example, have the funds to buy or otherwise introduce an insider. This can happen either in the form of active participation or in the form of gathering otherwise protected information. With such help, many security measures can be dangerously compromised. The cases of the Japanese Metropolitan Police Department or the company Ptech that were described above (see the section "Data Espionage") show that even vettings can be successfully circumvented.
- Another problematic area is the increasing use of connectivity and remote controlling even in high-risk areas. For example, new weapons are being developed by the military that rely on remote control, e.g. semi-autonomous military robots (see Brunst 2008 for further details). Many of these products rely on civilian technology and established operating systems, thereby opening additional loopholes for security risks.
- Finally, terrorists can use the fact that often, due to a lack of technical knowledge, members of the press or even politicians will draw wrong conclusions from facts that have become known to the public. For example, it is widely known that computers are used within missile launching premises. Computers have security weaknesses that can be exploited. Therefore, the deduction that missile centres are vulnerable to cyber attacks suggests itself. However, this conclusion might be wrong, if systems are in fact air-gapped as described above. This is, in turn, used by terrorists who do not necessarily rely on attacks being successful. An important aspect of terrorist attacks on the Internet is rather the creation of fear and uncertainty and the expectation that terrorists *could* at any time strike at any target they chose.

In this context, attacks against IT infrastructure can be of great help. The pure number of vulnerabilities that have become known and the number of targets that can be chosen offer a wide range of possible actions for cyber criminals as well as for terrorists. Any successful attack against "prominent" targets, e.g. government or intelligence websites, can be used to increase the level of anxiousness regarding more serious attacks.

The real danger that evolves from cybercrime attacks could be seen already in 1999, when the United States conducted an exercise named "Eligible Receiver". Hackers of the NSA acted as a so-called red team and attacked computer systems of the CIA, FBI, Defense Intelligence Agency, National Reconnaissance Office, Defense Information Systems Agency, Department of State, Department of Justice, and civilian establishments of relevant infrastructures during a 5-day period. Although many details of the exercise remained secret, it has become known that the red team relied solely on techniques and software that was freely available over the Internet. The group was able to enter protected networks, render systems inaccessible with the help of DoS and DDoS attacks, forge e-mails and gain root

level access to 36 government networks. Even the take-over of resources of the US Pacific Fleet, control of electric power systems, and the emergency number "911" in nine larger American cities was allegedly possible (Pike 2005; Weimann 2005).

Often, those who claim that cyberterrorism is not a real threat state also that terrorists lack the necessary skills for an electronic attack. The current generation of young terrorists, however, has – at least partly – grown up in a digital world. Computers seized from al-Qaeda, for example, show that they are becoming increasingly familiar with hacker tools that are freely available over the Internet (Wilson 2005). Furthermore, know-how, personnel, and outsourced services can be acquired on the free market, making it possible even for incapable groups to enter the new world of cyber attacks. The Islamic fundamentalist group "Harkat-ul-Ansar", for example, attempted to buy cyber attack software from hackers as early as late 1998 (Wilson 2005).

Finally, many nation states have started to invest into cyber forces to increase their powers also in this relatively new sector. This, in turn, opens new possibilities for state-sponsored terrorism (see Brunst 2008 for further details). The threat of future terrorist attacks that involve specific use of the Internet therefore has to be taken very seriously.

2.3 Dissemination of Terrorist Contents

With the establishment of the WWW, the Internet has created the possibility for everyone to disseminate information without costs – and largely without any control regarding the content. Terrorists are using the Internet therefore not only to launch attacks, but also to fight a "war of ideas" (Giacomello 2004).

2.3.1 Terrorist Websites

For a terrorist organization, it is extremely important to communicate their views, aims, and ambitions. Although in former times this was extremely difficult, the Internet now offers possibilities to easily communicate and possibly influence the media and the public at large (Brunst 2008). Therefore, it is no wonder that today almost every underground organization has its own website (Weimann 2004b, 2006) and the number is still steadily rising. In 1999, only a few of the 30, according to the US Department of State, deemed foreign terrorist organizations were able to operate a website (Conway 2002; Desouza & Hensgen 2003). By 2005, this number had increased to more than 4,500 terrorist-related websites (Coll & Glassner 2005; Conway 2002). The number of Internet-related items that carry terrorist contents (i.e. including forums, blogs, etc.) is even higher. According to some sources, in 2007, there were approximately 50,000 sites with extremist and terrorist content (Chen & Larson 2007).

Terrorist websites can be used for a number of purposes. For example, it is possible to target special audiences, e.g. the media, followers, or – with cartoon-style design and children stories – even young kids (Tsfati & Weimann 2002; Weimann 2004b, 2006). Contents can be presented as mere text-written viewpoints or – often with the help of fresh graphics, sound, or video files – as a glorification of recent acts or as an incitement to future acts (Brunst 2008). Although it is difficult to assess how many people are paying attention to these websites, it is said that the most popular terrorist sites are able to attract tens of thousands of visitors every month (Conway 2002). The difficulty of judging an organization only by its website (often as its only "official" organ) can also be abused. For example, a terrorist organization with an impressive website can easily claim to be bigger and to have more followers than it actually has (Embar-Seddon 2002).

Another issue of popular terrorist websites is that governments will often try to shut them down when they becomes too popular. However, the censorship resistance of the Internet in many cases prohibits these efforts. For this reason, many websites are not stored in the country of their organization. Instead, they are hosted on servers in countries that have a more liberal freedom-of-speech approach. Several websites of al-Qaeda, for example, were physically stored in the United States and Canada (Brunst 2008). The same is true also for other organizations that chose to be hosted outside of their country (Desouza & Hensgen 2003).

2.3.2 Threats and Propaganda

As already mentioned above, terrorist websites are not restricted to presenting only their own viewpoints. Instead, they can also be used to threaten the enemy or to spread propaganda. Especially if threats are presented with the help of multimedia technology, this gets the attention of the press and the public. For this reason, computer games have been developed, e.g. one named "Quest for Bush" that lets followers kill US President Bush (Vargas 2006). Other multimedia threats can literally burn images into the memories of the viewing audience. The assassination of Daniel Pearl, for example, showed the impact of psychological warfare that was conducted by these new means. Since then, the use of multimedia has rapidly increased. Whereas the al-Qaeda media arm As-Sahab issued only six audio or video web messages in 2002, this number increased to an impressive 97 multimedia messages in 2007 (Sedarat 2008).

To improve the presentation of their viewpoints, threats, propaganda, or incitements to terrorism, terrorists have even begun to record their attacks. For the best results, they are often filmed simultaneously from different angles so that the material can be better used for the distribution to the media, websites, and the production of DVDs (Kristof 2005). This kind of material is often used to (directly or indirectly) influence public opinion.

In the past, only a few well-established organizations were able to produce newspapers, magazines, or TV shows. The Internet makes it now possible for virtually

anyone to launch their own periodicals. Al-Qaeda therefore was able, for example, to start its own TV program "voice of the caliphate", which is available on the Internet. In the program, a hooded newsreader with a gun and a copy of the Koran on his desk, reads the latest headlines from the world of the Islamist jihad (La Guardia 2005; Musharbash 2005). Additional multimedia items were often sent out by the "Global Islamic Media Front" (GIMF). This kind of information can normally be easily recognized as terrorist material. Other information, however, might be disguised as seemingly neutral material in the hope that less critical members of the press take up the news and report about them. Because the Internet has become a major source for stories, background information, and also for photographic and similar material, this hope cannot be dismissed. By attractively presenting viewpoints and opinions, terrorist organizations can at least increase their chances of introducing these opinions into mass media products.

2.3.3 Financing

Online advertising and similar ways of gaining monetary income with Internet services has become a profitable business model for many. For terrorists and terrorists groups, this is not as easy, especially if explicit terrorist content is contained on a website. Nevertheless, some organizations have started to use their site not only to disseminate information, but also to use their site as a source of income for financing and fundraising.[7] Some websites, for example, are used – apart from their original purpose – to sell CDs, DVDs, T-shirts, badges, flags, or books (Conway 2002; Weimann 2004b).

Another way to finance terrorist activities is to give instructions on how to donate money. This can be done, for example, by giving necessary information (e.g. bank account details for transfers) or by implementing possibilities to enter credit card information for automatic withdrawals (Weimann 2004b).

Since the websites terrorist organizations are often at the center of surveillance by security agencies, hundreds of support websites commonly appear and disappear. Each website provides links to other supporter websites so that a visitor who once has found an entry point into the terrorist web can easily find other and similar sites. In some cases, even specialized web rings are founded. Yahoo!, for example, hosted dozens of sites in the "Jihad Web Ring", a coalition of 55 Jihad-related sites (Buettner 2001; Conway 2002; Reuters 2001).

If, at any point, users give personal information, terrorists are also able to gather user demographics. This can happen, for example, if a user fills out online questionnaires, order forms, or enters relevant e-mail lists. Users that are identified as potential sympathizers can then be e-mailed and asked to make donations over other (e.g. more secret) channels (Weimann 2006). Because this

[7]For other aspects of terrorist financing, see Chap. 16.

first contact is made electronically and over a distance, users might engage more easily into this "clean" form of terrorist support, which also can function as a gateway into closer ties between terrorist organizations and their future supporters.

2.4 Conventional Use of the Internet

A commonly underestimated threat is the conventional use of the Internet. While the access to "dangerous" sources, e.g. terrorist websites or relevant message boards, could – at least potentially – be constantly monitored and taken as an initial point for action, this is not possible with everyday services such as search engines, common websites, or e-mail traffic. However, a closer look reveals that even seemingly harmless sites offer information that is, on the one hand, valuable and important for terrorists and, on the other hand, uncontrollable. By way of example, the use of individual communication between terrorists and the planning and supporting of conventional attacks will be highlighted below.

2.4.1 Individual Communication

Although conventional methods for individual communication are still widely available, e.g. telephone or letters, they have individual disadvantages over the possibilities that the Internet offers. A telephone conversation, for example, requires both parties to be present simultaneously at their point of communication. Additionally, contents are transmitted unencrypted so that government agencies can listen if the parties are already under surveillance (or if they are affected by strategic large-scale surveillance measures). A letter, on the other hand, offers the possibility for asynchronous communication and easy encryption, but it takes longer to transmit. Additionally, like the telephone, it requires both parties to be present at certain points, e.g. at a mailbox for the sender or at the destination address for the recipient.

The Internet, however, allows both parties to communicate asynchronously, e.g. by e-mail. This service does not require much bandwidth, making it possible to send and retrieve information even over older mobile phones or in areas where Internet connections are limited. Additionally, messages can be stored and retrieved at any given point in time; terrorists neither have to be online all the time, nor do they have to entrust third parties with the task of accepting personal messages for them. Therefore, e-mail allows terrorists to communicate independently of a specific and pre-determined place. Furthermore, many companies offer e-mail services free of charge so that several different e-mail accounts can be used simultaneously. The organizers of the 9/11 attacks, for example, had operated in such a way and opened multiple accounts on largely anonymous e-mail services, such as "Hotmail" (Conway 2002).

If, for any reason, a synchronous communication is preferred, the Internet offers many different opportunities as well. Internet Relay Chat (IRC), for example, allows for a conversation between two or more persons who are online at the same time. The service is text-based, fast – and largely unsupervised. Even voice-based systems, like Skype, can be used (Weimann 2004b; Wilson 2005).

The biggest advantage of Internet-based communication, however, is that all messages are digital right from the start. Therefore, many publicly available encryption programs can be used (see Brunst 2008; 2009 for further details). These are accessible as open source so that terrorists can check themselves for hidden backdoors or other unwanted "features". Nevertheless, terrorist groups have started to compile their own software products for encrypted communication. The software "Secrets of the Mujahideen" – currently available as version 2.0 – is advertised as "the first Islamic program for secure communications through networks with the highest technical level of encoding" (Sedarat 2008). The use of such specialized and often easy-to-use applications drastically increases the protection of terrorist's messages between each other. This, in turn, makes it hard or – if used correctly – impossible for government agencies to successfully monitor communication, resulting in a lack of information.

2.4.2 Planning and Supporting

It seems surprising that most of the information needed for a conventional attack is not protected, but freely available. This can, for example, be a picture of an important manager that is available on a company's website or the favourite nightclub of his teenage daughter that can be taken from her profile on facebook.com. According to a terrorist manual, public sources can therefore provide up to 80% of all required information on an opponent (Weimann 2004b).

An example that is often cited is the satellite maps that are provided, for example by Google, Microsoft, or NASA. In former times, images of that quality were available only to experts, now they are a common good and accessible to anybody. It is therefore of no surprise that terrorists have started to use these services for their own purposes. According to UK army intelligence sources, for example, during a raid in 2007, printouts from Google Earth were found. They showed buildings inside the British bases in Basra in detail and vulnerable areas "such as tented accommodation, lavatory blocks and where lightly armoured Land Rovers are parked" (Harding 2007). Due to some additional evidence, officials believed that this information was used to prepare attacks on the premises.

According to some authors, terrorist organizations have even started to use databases to gather, sort, and evaluate the details of potential targets in the United States (Weimann 2004b). Actual findings on terrorists' computers have shown that publicly available information of all kinds are indeed being downloaded and used for planning purposes (Harding 2007; Weimann 2004b). It can therefore be assumed

that information that is freely available on the Internet is indeed significantly strengthening the operational capabilities of terrorist groups.

Terrorists, however, are not only taking information from the Internet. They use the net also to store information and make it available for others. Some authors therefore claim that the Web has become "an open university for jihad" (Coll & Glassner 2005). This "university" offers information such as the "Mujahadeens Poisons Handbook" that contains various "recipes" for homemade poisons and poisonous gases (Weimann 2004b, 2006). Similar information is compiled in other collections, such as the "Terrorist's Handbook", the "Anarchist Cookbook", the "Encyclopedia of Jihad", the "Sabotage Handbook", and the famous "How to Make Bombs". Today, many collections are amended by extra information, e.g. on hostage taking, guerrilla tactics, or special kinds of bombs (Brunst 2008).

2.5 Conclusions

In this chapter, different risks of terrorists using the Internet have been assessed. Although a large cyber attack that was verifiably committed by terrorists has – up until now – not taken place, this is no reason to underestimate the risks and potential of future scenarios. Already the brief outline of the conventional use of the Internet by terrorists has shown that terrorists are not unfamiliar with the Internet. On the contrary, it is known that the Internet is constantly used for their purposes already today, e.g. to prepare conventional attacks, to communicate, or to disseminate their respective contents.

The general characteristics of the Internet indicate furthermore that digital attacks are a likely scenario. Chances are high that such incidents will be directed against other IT systems, especially if connected to real-world machinery, and result in an immediate outcome rather than long-term effects. The attacks and aggressions that have been launched in the past by common cyber criminals, state-sponsored, or (presumably) governmental groups have partly demonstrated the potential of such assaults. Especially the two last-mentioned groups have to be considered as extremely dangerous, because they have the ability to use monetary and technical resources to which common criminals seldom have access.

The actions that have been taken on a political and legal level to counter cyberterrorism have, for a long time, been rather reluctant.[8] In the end, it was probably the attacks on Estonia in 2007 that showed governments around the world and the public at large what knowledgeable aggressors can do to a whole nation solely by digital means. International organizations such as NATO therefore now take cyber attacks "as seriously as the risk of a missile strike" and see cyberterrorism as a chief threat (Johnson 2008). Especially if a nation with offensive cyber capabilities is

[8]For legal responses that have been taken to conquer cyberterrorism see Sieber, this volume.

willing to support perpetrators, the risks and potential damages will additionally increase. The convergence of terrorism and the cyber world therefore creates a new threat that has to be taken very seriously.

References

AFP News Agency. (2005). Hacker Attacks in US Linked to Chinese Military [Electronic Version]. *Breitbart.com*, *12.12.2005*. Retrieved April 2008 from http://www.breitbart.com/article.php?id=051212224756.jwmkvntb&show_article=1.

Bachfeld, D. (2003). War der Wurm drin? *c't, 2003*(18), 34.

Berinato, S. (2002). Cybersecurity – The Truth About Cyberterrorism [Electronic Version]. *CIO Magazine*. Retrieved April 2008 from http://www.cio.com/article/30933/CYBERSECURITY_The_Truth_About_Cyberterrorism.

Borland, J. (1998). Analyzing the Threat of Cyberterrorism [Electronic Version]. *Techweb.* From http://www.techweb.com/showArticle.jhtml?articleID=29102707.

Brunst, P. W. (2008). Use of the Internet by Terrorists – A Threat Analysis. In Centre of Excellence – Defence Against Terrorism (Ed.), *Responses to Cyber Terrorism* (pp. 34–60). Amsterdam: IOS Press.

Brunst, P. W. (2009). Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen. Berlin: Duncker & Humblot.

Buettner, R. (2001). Web of Terror Thrivin on Net. Retrieved April 2008 from http://www.nydailynews.com/archives/news/2001/09/18/2001–09–18_web_of_terror_thriving_on_net.html

Centers for Disease Control and Prevention. (2007). Bioterrorism Overview. From http://www.bt.cdc.gov/bioterrorism/overview.asp

Chen, H., & Larson, C. (2007). Dark Web Terrorism Research. Retrieved April 2008 from http://www.ai.arizona.edu/research/terror/index.htm

Cilluffo, F. J. (2000). Cyber Attack: The National Protection Plan and Its Privacy Implications. Testimony of Frank J. Cilluffo Before the Subcommittee on Technology, Terrorism, and Government Information Committee on the Judiciary on 1 February 2000 [Electronic Version]. From http://www.csis.org/media/csis/congress/ts000201cilluffo.pdf.

Coll, S., & Glassner, S. (2005, 7 August). Terrorists Turn to the Web as Base of Operations. *The Washington Post*, p. A01.

Collin, B. C. (1997). The Future of Cyberterrorism. *Crime and Justice International*, 13(2), 15–18.

Committee on Water Systems Security Research. (2007). *Improving the Nation's Water Security*. Washington, DC: The National Academies Press.

Conway, M. (2002). Reality Bites: Cyberterrorism and Terrorist 'Use' of the Internet (Publication. Retrieved 01.12.2005): http://www.firstmonday.org/Issues/issue7_11/conway/index.html

Davis, J. (2007). Hackers Take Down the Most Wired Country in Europe [Electronic Version]. *Wired Magazine*. Retrieved April 2008 from http://www.wired.com/politics/security/magazine/15–09/ff_estonia.

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Arquilla, J. & Ronfeldt, D. (Eds.), Networks and Netwars (pp. 239–288). Santa Monica, CA: Rand Corp.

Desouza, K. C., & Hensgen, T. (2003). Semiotic Emergent Framework to Address the Reality of Cyberterrorism. *Technological Forecasting & Social Change*, *70*, 385–396.

Drogin, B. (1999). Russians seem to be Hacking into Pentagon [Electronic Version]. *San Francisco Chronicle Online*, *07.10.1999*. Retrieved April 2008 from http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/10/07/MN58558.DTL.

Embar-Seddon, A. (2002). Cyberterrorism – Are We Under Siege? *American Behavioral Scientist*, *45*(6), 1033–1043.

Espiner, T. (2005). Security Experts Lift Lid on Chinese Hack Attacks [Electronic Version]. *ZDNet News*, *23.11.2005*. Retrieved April 2008 from http://news.zdnet.com/2100–1009_22–5969516.html.

FCW Staff. (1999). Russia Hacking Stories Refuted [Electronic Version]. *Federal Computer Week*, *27.09.1999*. Retrieved April 2008 from http://www.fcw.com/print/5_188/news/68553–1.html.

Foltz, B. (2004). Cyberterrorism, Computer Crime, and Reality. *Information Management & Computer Security, 12*(2), 270–295.

Force10 Networks. (2007). Customer Profile: DE-CIX. Retrieved April 2008 from https://www.force10networks.com/company/customer_profiles/profiles-de-cix.asp

Gellman, B. (2002, 27 June). Cyber-Attacks by Al Qaeda Feared. *The Washington Post*, p. A01.

Giacomello, G. (2004). Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism. *Studies in Conflict & Terrorism*, *27*(5), 387–408.

Gleick, P. H. (2006). Water and Terrorism. *Water Policy*, *8*, 481–503.

Graham, B. (2005). Hackers Attack Via Chinese Web Sites [Electronic Version]. *The Washington Post Online*, *25.08.2005*, A01. Retrieved April 2008 from http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

Green, J. (2002). The Myth of Cyberterrorism [Electronic Version]. *Washington Monthly*. Retrieved April 2008 from http://www.washingtonmonthly.com/features/2001/0211.green.html.

Harding, T. (2007). Terrorists 'Use Google Maps to Hit UK Troops' [Electronic Version]. *The Telegraph Online*. From http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/13/wgoogle13.xml.

ICANN. (2007). Factsheet: Root Server Attack on 6 February 2007. Retrieved April 2008 from http://icann.org/announcements/factsheet-dns-attack-08mar07.pdf

Janczewski, L. J., & Colarik, A. M. (2005). *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. Hershey, PA: Idea Group Publishing.

Johnson, B. (2008). Nato Says Cyber Warfare Poses as Great a Threat as a Missile Attack [Electronic Version]. *The Guardian Online*. Retrieved April 2008 from http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity.

Kristof, N. D. (2005, 20 December 2005). Terrorists in Cyberspace. *The New York Times*, p. 31.

La Guardia, A. (2005). Al-Qa'eda Launches Voice of the Caliphate Internet News Bulletins [Electronic Version]. *The Telegraph Online*. Retrieved April 2008 from http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/09/28/wirq128.xml&sSheet=/news/2005/09/28/ixnewstop.html.

Leitenberg, M. (2005). *Assessing the biological weapons and bioterrorism threat*. Strategic Studies Institute of the U.S. Army War College.

Lenzner, R., & Vardi, N. (2004). The Next Threat [Electronic Version]. *Forbes Magazine*. From http://www.forbes.com/forbes/2004/0920/070_print.html.

Leppard, D. (2007). Al-Qaeda Plot to Bring Down UK Internet [Electronic Version]. *The Times Online*. From http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece.

Leyden, J. (2001). Mass Hack Takes Out Govt Sites [Electronic Version]. *The Register*. Retrieved April 2008 from http://www.theregister.co.uk/2001/01/22/mass_hack_takes_out_govt/.

Miniwatts Marketing Group. (2007). Internet Usage Statistics. Retrieved April 2008 from http://www.internetworldstats.com/

Musharbash, Y. (2004). US-Firmen-Website für Qaida-Botschaft gehackt. *Spiegel Online*, *17.06.2004*.

Musharbash, Y. (2005). Al-Qaida Launches a Weekly News Show [Electronic Version]. *Spiegel Online*. Retrieved April 2008 from http://www.spiegel.de/international/0,1518,378633,00.html.

National Conference of State Legislatures. (2002). Cyberterrorism. Retrieved April 2008 from http://www.ncsl.org/programs/lis/cip/cyberterrorism.htm.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). *Cyberterror: Prospects and Implications*. From http://www.nps.edu/Academics/Centers/CTIW/files/Cyberterror%20Prospects%20and%20Implications.pdf.

OLG Frankfurt a.M. (2006). Lufthansa Online Demonstration. *Multimedia und Recht* 2006, 547–552.

Persson, C. (2006). "Rückfall ins Telefonzeitalter" nach Erdbeben. Retrieved April 2008 from http://www.heise.de/newsticker/Rueckfall-ins-Telefonzeitalter-nach-Erdbeben--/meldung/83007

Pike, J. (2005, 27.04.2005). Eligible Receiver. Retrieved April 2008 from http://www.globalsecurity.org/military/ops/eligible-receiver.htm

Pollitt, M. M. (1998). Cyberterrorism – Fact or Fancy? *Computer Fraud & Security* (February 1998), 8–10.

Record, J. (2003). *Bounding the Global War on Terrorism*. University Press of the Pacific.

Reuters. (2001). This Jihad WEb Site Brought to You by… Visa? Retrieved April 2008 from http://www.usatoday.com/tech/news/2001/09/19/jihad-sites.htm

Rolski, T. (2007). Estonia: Ground Zero for World's First Cyber War? [Electronic Version]. *ABC News*. From http://abcnews.go.com/International/Technology/Story?id=3184122&page=1.

Sedarat, F. (2008). Jihadi Software Promises Secure Web Contacts [Electronic Version]. *Reuters Online*, *2008*. From http://www.reuters.com/article/internetNews/idUSL1885793320080118.

Sieber, U. (2004). The Threat of Cybercrime. In Council of Europe (Ed.), *Organized Crime in Europe: The Threat of Cybercrime* (pp. 81–217). Strasbourg: Council of Europe.

Sieber, U., & Brunst, P. W. (2008). Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions. In Council of Europe (Ed.), *Cyberterrorism – The Use of the Internet for Terrorist Purposes* (pp. 9–105). Strasbourg: Council of Europe Publishing.

Sliva, J., & Ritter, K. (2006). Estonia's Defense Minister Says Kremlin Involvement Possible in Cyberattacks [Electronic Version]. *The Sydney Morning Herald Online*. Retrieved April 2008 from http://www.smh.com.au/news/Technology/Estonia39s-defense-minister-says-Kremlin-involvement-possible-in-cyberattacks/2007/05/18/1178995335698.html.

Testimony of FBI Deputy Assistant Director Keith Lourdeau on "Virtual Threat, Real Terror: Cyberterrorism in the 21st Century", Subcommittee on terrorism, technology and homeland security of the committee on the judiciary United States Senate, 24 February Sess. (2004).

Testimony of James Adams, Chief Executive Officer, Infrastructure Defense, Inc., United States Senate, Committee on Governmental Affairs (2000).

Thornburgh, N. (2005a). Inside the Chinese Hack Attack [Electronic Version]. *Time Online*, *25.08.2005*. Retrieved April 2008 from http://www.time.com/time/nation/article/0,8599,1098371,00.html.

Thornburgh, N. (2005b). The Invasion of the Chinese Cyberspies [Electronic Version]. *Time Online*, *29.08.2005* from http://www.time.com/time/magazine/article/0,9171,1098961–1,00.html.

Traynor, I. (2007). Russia Accused of Unleashing Cyberwar to Disable Estonia [Electronic Version]. *The Guardian Online*, *17.05.2007* from http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Tsfati, Y., & Weimann, G. (2002). www.terrorism.com: Terror on the Internet. *Studies in Conflict & Terrorism*, *2002*(25), 317–332.

Vargas, J. A. (2006). Way Radical, Dude [Electronic Version]. *The Washington Post Online.* From http://www.washingtonpost.com/wp-dyn/content/article/2006/10/08/AR2006100800931.html.

Vatis, M. A. (2001). *Cyber Attacks During the War On Terrorism: A Predictive Analysis*. Retrieved April 2008 from http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

Weimann, G. (2004a). Cyberterrorism: How Real is the Threat? [Electronic Version]. *Special Report (United States Institute of Peace)*, *119*.

Weimann, G. (2004b). www.terror.net. How Modern Terrorism Uses the Internet [Electronic Version]. *Special Report (United States Institute of Peace)*, *116*.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*, *28*, 129–149.

Weimann, G. (2006). *Terror on the Internet*. Washington, DC.

White, J. R. (1990). *Terrorism – an Introduction*. Pacific Grove, CA: Brooks/Cole Publishing Co.

Wilson, C. (2005). *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Vol. RL32114). Washington, DC

Part II
The International Front

Chapter 3
The Role of the United Nations in the Prevention and Repression of International Terrorism

Paul J. Rabbat

3.1 Introduction

In the last two decades, the emergence of highly organized, well-trained, and well-financed international terrorist networks has exposed significant gaps in the United Nations (UN)'s pre-existing anti-terrorism framework which, although commonly acknowledged as an important foundation, was clearly the product of another era. This recognition by the UN's Member States coupled with their acknowledgement of the sheer magnitude of the threat posed by the "new terrorism" has acted as an important catalyst for the reform of the global legal framework against terrorism, and has galvanized Member States to adopt sweeping changes, many of which have often been highly controversial.

The end of the Cold War as well as aftermath of the tragic attacks on the USA in 2001 have borne witness to the overhaul of the Organization's anti-terrorism strategy, the adoption of far-reaching resolutions, the creation of important new institutions, as well as the imposition of an onerous set of mandatory obligations on Member States. The UN's broad membership and well-developed institutional framework has contributed to the Organization's emergence and continued development as the most suitable and effective global forum for the coordination of the international community's anti-terrorist initiatives.[1] Moreover, the UN's broad mandate and the existence of its specialized agencies have allowed the Organization to pursue a comprehensive and multi-faceted response to terrorism. However, this development has not been without its problems.

In order to understand the intricacies of the current UN framework against terrorism, it is first imperative to examine the origins of this construct as well as historical and

P. Rabbat (✉)
Formerly Head of International Criminal Law Section, MPI for Foreign and International Criminal Law, Freiburg
e-mail: p.rabbat@mpicc.de

[1] As the Security Council itself acknowledged in S/RES/1269 (1999).

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_3,

political developments having informed its development. As such, the first part of this chapter will be devoted to a brief outline of these factors. Part II will examine subsequent developments having occurred in the periods following the end of the Cold War and in response to widespread acts of international terrorism including those of September 2001.

Because of the complex nature of the UN framework against terrorism as well as the limited scope of the present chapter, the issues addressed do not purport to be fully comprehensive. Rather, they represent the most salient, and in many cases, the most controversial features of the Organization's effort to combat terrorism.

3.2 Early International Action against Terrorism

3.2.1 The League of Nations Conventions

The first attempt at concerted action against terrorism under the aegis of an international organization occurred in response to the assassination of King Alexander of Yugoslavia during a State visit to Marseille in 1934.[2] In response to the assassination, the League of Nations, in many ways the UN's institutional predecessor, passed a resolution declaring that "*the rules on international law concerning the repression of terrorist activity are not at present sufficiently precise to guarantee efficiently international cooperation.*"[3] The Council of the League of Nations mandated a special commission of experts with the task of elaborating two distinction conventions: the first for the *Prevention and Punishment of Terrorism* and the second for the *Creation of an International Criminal Court* intended to bring accused terrorists to justice. Given the fact that the first of these Conventions was ratified by India alone and the second failed to receive even a single ratification, both instruments failed to enter into force and remained dead letter.[4] In spite of this, several elements of the first Convention merit closer attention. The Convention provided, for example, that High Contracting Parties would undertake to prevent the preparation of terrorist attacks on their territory,[5] and that international terrorist acts would, in limited circumstances, be subject to extradition despite their apparent political character.[6]

---

[2] Kovacs, P. (2002). Le grand précédent: la Société des Nations et son action après l'attentat contre Alexandre, roi de Yougoslavie. *European Integration Studies, vol. 1/2002*, 30–40.

[3] League of Nations, Committee for the International Repression of Terrorism (CIRT), Geneva, 10 April 1935, League of Nations Doc. CRT1., cited in: Saul, B. (2006). The Legal Response of the League of Nations to Terrorism. *4 Journal of International Criminal Justice (2006)*, 78–102, at p. 80.

[4] Gross, L. (1973). International Terrorism and International Criminal Jurisdiction. *American Journal of International Law, Vol.67, No. 3, July 1973*, 508–511, at p. 508.

[5] Article 1(1).

[6] Article 8(1).

The scope of the material acts covered by the Convention included attacks against "protected persons" such as Heads of State, their spouses, as well as individuals "*charged with public functions when the act is directed against them in their public capacity*,"[7] the destruction of public property,[8] as well as the commission of acts likely to endanger human lives[9] and extended beyond that to cover attempts as well as to preparatory acts.[10] Pursuant to the Convention, these material acts would be incorporated into the domestic criminal legislation of the High Contracting Parties that would also be enjoined to apply the principle of *aut dedere aut judicare* in addition to providing each other with a high degree of mutual legal assistance.[11]

Despite the fact that the *Convention for the Prevention and Punishment of Terrorism*, never entered into force due to an insufficient number of ratifications as well as the subsequent demise of the League of Nations, the elaboration of this Convention can be seen as having sown the seeds of later developments.

In particular, the League of Nations' understanding of the concept of "terrorism" as acts committed by individuals or groups against the State or representatives thereof differed significantly from that which traditionally characterized this notion at international humanitarian law. According to international humanitarian law, the concept of "terrorism" could be likened to "collective punishment" in that it was typically perpetrated by States (or at least state-sponsored) against civilian populations in the context of armed conflict.[12]

To a great extent, the debates having occurred within the League of Nations also foreshadowed many of the contentious issues later to face the UN such as the challenge of defining terrorism, the questions of self-determination and "freedom fighters" and of "State terrorism."[13] On a broader level, attempts by the League of Nations to elaborate concrete measures to prevent and repress international terrorism also entrenched the idea that high-level concerted action by the international community was the most effective means of addressing this threat and that this action could best be undertaken within an established and representative global institutional framework.[14]

---

[7] Article 2(1).

[8] Article 2(2).

[9] Article 2(3).

[10] Article 2(4).

[11] Kovacs, p. 9.

[12] This interpretation of terrorism is notably retained in Article 4 of the Statute of the International Criminal Tribunal for Rwanda. On the evolution of these different concepts, *see* generally: Weigend, T. (2006). The Universal Terrorist: The International Community Grappling with a Definition. *4 Journal of International Criminal Justice (2006)*, 912–932.

[13] Saul, p. 79.

[14] Supra, Condorelli, p. 833.

3.2.2 Early UN Initiative Against Terrorism

Action against terrorism at the international level gained momentum within the UN framework during the early 1960s, in which terrorism was predominantly viewed as an internal and/or national law enforcement issue and continued to develop in the 1970s and 1980. This was also a historical period marked by wars of decolonization and activities of national liberation movements to which a large number of States were sympathetic, and in which many politically motivated acts of violence were considered by various members of the international community to be legitimate.[15] In addition, there was a great amount of discord as to how to define the concept of terrorism. The combination of these factors, which were exacerbated by Cold War political tensions, had a profound impact on the manner in which the international legal framework governing terrorism was fated to evolve.[16]

Indeed, the Member States of the UN were forced to reconcile their desire to act in a concerted manner to prevent and repress acts of terrorism with their inability to define the very phenomenon they sought to prohibit. This was especially problematic in light of the *nullum crimen sine lege* principle, one of the most fundamental tenants of criminal law,[17] according to which behaviours which are elevated to the status of "crime" and which are therefore subject to prosecution and punishment must be clearly defined in order to guarantee the foreseeability of the law as well as the transparency of the criminal law.[18]

Despite the failure to agree on a comprehensive definition of terrorism, UN Member States nonetheless saw the need to act against certain instances of politically motivated violent acts against civil aviation, maritime navigation, as well as internationally protected persons that were deemed to be unacceptable and were susceptible of having a trans-national component.[19] As such, the legal regime against terrorism was characterised by a "piecemeal" approach, evidenced by the adoption of so-called "sectoral treaties,"[20] predicated on the criminalisation at the national level, of a variety of terrorist acts representing the lowest common denominator of States participating in the process.[21] Another limitation to the UN Conventions is that no implementation measures were provided for to ensure the compliance of State Parties.[22]

---

[15] Weigend, p. 918.

[16] Nuotio, K. (2006). Terrorism as a Catalyst for the Emergence, Harmonization and Reform of Criminal Law. *4 Journal of International Criminal Justice (2006)*, 998–1016, at p. 1003.

[17] *See* International Covenant on Civil and Political Rights, Article 15.

[18] Kolb, R. (2004). The Exercise of Criminal Jurisdiction over International Terrorists. In A. Bianchi (Ed.), *Enforcing International Law Norms against Terrorism* (pp. 227–282). Oxford, Portland: Hart Publishing, at p. 227.

[19] A list of UN instruments against terrorism can be found in Annex I.

[20] Bianchi, A. (2004). Enforcing International Law Norms against Terrorism: Achievements and Prospects. In A. Bianchi (Ed.), *Enforcing International Law Norms against Terrorism* (pp. 491–534). Oxford, Portland: Hart Publishing, at p. 494.

[21] Laborde, p. 64.

[22] Laborde, p. 64.

From 1963 until 1988, nine international conventions against terrorism were adopted within the UN framework targeting these specific acts of terrorism and leaving open the possibility of adopting further measures if necessary and if and when circumstances permitted.

The UN legal instruments adopted during the period from the 1960s until the early 1990s established a common structure made up of the same four elements which would also characterise future conventions.[23]

The first of these is that the Conventions establish the scope of the conduct to be prohibited by defining the substantive "terrorist" offence which is to constitute the Convention's *rationae materiae* provision (e.g., attacks against civil aviation and maritime navigation, attacks against internationally protected persons, the taking of hostages, and terrorist bombings).

After having defined the proscribed conduct, the Conventions enjoin State Parties to penalise the acts in question in their domestic legal orders. However, while this obligation is a *sine qua non* for the respect of the Conventions' obligations, it is nonetheless interesting to note that the Conventions do not in any way, impose a corresponding obligation for State Parties to specifically qualify these acts as "terrorist offences."

The third common feature shared by the Conventions is that each instrument identifies certain bases on which State Parties are required to establish their jurisdiction over the crimes defined therein. Depending on the specific conduct covered, these may include territoriality, nationality, and State of registration of a vessel or aircraft.

Finally, the anti-terrorism Conventions establish the principle of *aut dedere aut judicare* according to which States are requited either to prosecute individuals in their custody for acts covered by the Conventions over which they have jurisdiction or to extradite the suspect to another jurisdiction willing to do so. These instruments also provide that the offences listed therein are automatically incorporated into any existing extradition treaty and cannot be considered as falling within the "political offence exception," or in the absence of an extradition treaty, that the anti-terrorism treaty may itself serve as the legal basis for extradition.

Notwithstanding its limited scope, the early UN framework against terrorism was actually quite inventive and resourceful given the political divisions which dominated at the time. Where properly implemented, these instruments also had the capacity to have a tangible impact on the establishment of individual criminal responsibility for the acts they sought to proscribe.[24] Moreover, the adoption of the early treaties served as proof that action against terrorism is possible, even in the absence of a universally accepted definition of this concept, through a targeted criminalization of the gravest and most common terrorist acts as well as through a bolstering of extradition and mutual legal assistance frameworks.

---

[23] *See* "United Nations Counter-Terrorism Conventions," at www.unodc.org/en/terrorism/conventions.html

[24] Bianchi (2004) p. 495.

3.3 More Recent Developments

3.3.1 Post-Cold War Consensus

The increase in momentum of UN action against terrorism that characterised the late 1980s continued into the 1990s, a decade in which a further three instruments were elaborated.[25]

Although action against terrorism in the post-Cold War period prior to the 11 September 2001 terrorist attacks continued to be marred by some of the same problems as in the decades previous, several significant developments owing to evolving political realities occurred during this period. These developments were essentially due to the end of the gridlock associated with the Cold War as well as to the decrease in importance of the decolonisation movement, given the fact that most former colonial States had achieved their independence. This evolution enabled the organization to confront the continuing threat of terrorism with a theretofore unprecedented degree of unity and resolve which would prove to have important repercussions for future UN action against terrorism.[26]

Thus, it is during this period that the Security Council first qualified acts of international terrorism as "threats to international peace and security" in response to the bombing of Pan Am flight 103 in 1992 ("Lockerbie").[27] In the interim period from 1992 until the 11 September 2001 terrorist attacks, the Council made use of this qualification in response to three additional instances of terrorism to which it was confronted.[28] In accordance with the UN Charter, the legal effect of labelling terrorism, a "threat to international peace and security" was to empower the Council to enact measures to combat it under Chapter VII (and therefore binding on all Member States).

A further development was the emergence of a consensus to the effect that ideologically motivated acts of violence directed against civilians could not be justified under any circumstances.[29] Thus, in 1994, the UN General Assembly issued its *Declaration on Measures to Eliminate International Terrorism*[30] in which it declared:

> 1. The States Members of the United Nations solemnly reaffirm their unequivocal condemnation *of all acts, methods and practices of terrorism, as criminal and unjustifiable, wherever and by whomever committed*, including those which jeopardize the friendly relations among States and peoples and threaten the territorial integrity and security of States; […]

---

[25] Cf. Annex I.

[26] Nuotio, p. 1003.

[27] S/RES/731 (1992).

[28] S/RES/1054 (1996); S/RES/1189 (1996); S/RES/1267 (1999); *See also*: Bianchi, A. (2006). Security Council's Anti-terror Resolutions and their Implementation by Member States: An Overview. *4 Journal of International Criminal Justice (2006)*, 1044–1073, at p. 1045.

[29] Nuotio, p. 1003.

[30] "Declaration on Measures to Eliminate International Terrorism," annexed to GA/RES/49/60 (1994), "Measures to Eliminate International Terrorism," 9 December 1994.

> 3. Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them; [*emphasis added*]

In addition to the categorical language adopted in the preceding quote, the Declaration is also noteworthy in that it further departs from previous practice in consciously omitting any reference to the right of oppressed peoples to undertake a "legitimate struggle for freedom and independence."[31]

Pursuant to the Declaration, the General Assembly also created an *Ad Hoc Committee*[32] in 1996 that went on to draft the *International Convention for the Suppression of Terrorist Bombings*,[33] the *International Convention for the Suppression of the Financing of Terrorism*,[34] and in 2005, the *International Convention for the Suppression of Acts of Nuclear Terrorism*.[35] The Committee was also subsequently given the mandate of elaborating a Comprehensive Convention on International Terrorism. As will be discussed below, the Financing Convention is particularly worthy of note in that it contains the first general definition of terrorism adopted within an international instrument.

The General Assembly's unequivocal stance against all forms of terrorism was shared by the Security Council Resolution as evidenced in Resolution 1269 (1999) which acknowledged the GA resolution and adopted an equally unequivocal condemnation of all acts of terrorism regardless of the motives for which they are committed.[36]

Resolution 1269 also called upon States to take appropriate steps to "*prevent and suppress in their territories through all lawful means the preparation and financing of any acts of terrorism*."[37] This stipulation is indicative of a renewed broadening of the UN framework against terrorism to include not only the perpetration of terrorist acts but also contribution to these acts, heralding the revisiting of an approach also focussed on prevention.[38] This shift approach was arguably the result of two factors.

---

[31] Weigend, p. 920.

[32] GA/RES/51/210 (1996), 17 December 1996.

[33] International Convention for the Suppression of Terrorist Bombings, GA/RES/52/164, adopted 15 December 1997.

[34] International Convention for the Suppression of the Financing of Terrorism, GA/RES/54/109, adopted 9 December 1999.

[35] International Convention for the Suppression of Acts of Nuclear Terrorism, GA/RES/59/290, adopted 13 April 2005.

[36] S/RES/1269 (1999), "On International Cooperation in the Fight against Terrorism," 19 October 1999.

[37] Ibid. para. 4.

[38] Originally used in the 1980 Convention on the Physical Protection of Nuclear Materials and evidenced in both the International Convention on the making of Plastic Explosives for the purpose of Detection (1991) *see*: Laborde, J.-P., & DeFeo, M. (2006). Problems and Prospects of Implementing UN Action against Terrorism. *4 Journal of International Criminal Justice (2006)*, 1087–1103, at p. 1091.

The first of these is the fact that the exclusive focus on perpetration ignored realities associated with the commission of large-scale terrorist attacks having dramatically increased in scope and sophistication and involving multiple actors at all stages of preparation prior to execution. Thus, the fact that these acts were not the typically the result of one person acting alone but of multinational groups acting through a complex division of labour was left relatively unaddressed. In addition, the quasi-exclusive focus on legal deterrence had known limited success given the fact that many perpetrators of terrorist attacks were prepared to sacrifice their lives in carrying out their attacks, rendering the prospect of punishment irrelevant.[39]

Another development which demonstrates the increased importance of "prevention" within the UN framework against terrorism was the adoption of the *International Convention for the Suppression of the Financing of Terrorism* of 1999 that deviates from previous instruments in not only criminalizing violent acts or their attempted commission but rather the non-violent provision or collection of funds "*with the intention that they should be used or in the knowledge that they will be used*" to carry out a terrorist attack.[40] Thus, the criminal conduct in question is subject to prosecution whether or not the terrorist attacks using the funds have occurred or have been attempted.

3.3.2 Resolution 1267, the Al Qaida and Taliban Sanctions Committee and the Consolidated List

In 1999, the Security Council acting under Chapter VII of the UN Charter adopted Resolution 1267 aimed at the Taliban regime.[41] Although Resolution 1267 highlights various egregious policies pursued by the Taliban such as the disregard for international humanitarian law, human rights, the rights of women, and the large-scale production of opium,[42] the Resolution's main focus is clearly the Taliban's support of terrorism. Indeed the initial paragraphs of Resolution 1267 are a clear indictment of the Taliban regime for the "sheltering and training of terrorists and planning of terrorist acts"[43] as well as for continuing to "*provide safe haven to Usama bin Laden and to allow him and other associated with him to operate a network of terrorist training camps… and to use Afghanistan as a base from which to sponsor international terrorist operations*."[44]

In particular, Resolution 1267 is a response to the refusal of the Taliban to extradite Usama bin Laden to face trial for the bombing of the US Embassies in Kenya and

[39] Laborde & DeFeo, p. 1087.

[40] Financing Convention, Art. 2.

[41] S/RES/1267 (1999), 15 October 1999.

[42] Para. 3.

[43] Para. 5.

[44] Para. 6.

Tanzania having occurred in 1998 in violation of Security Council Resolution 1214 requiring it to do so.[45] As such, the Council imposes a series of measures on Member States meant to induce the Taliban regime to act in accordance with the obligations ascribed to it by the Council. The first of these measures consists in the imposition of travel restriction on the Taliban through the denial of landing or take-off rights of aircraft "owned, leased, or operated by or on behalf of the Taliban."[46] The second and by far most important measure is the obligation on Member States to freeze all assets owned or controlled whether directly or indirectly by the Taliban.[47]

Another salient feature of Resolution 1267 is that it also provides for the creation of a Committee to monitor the implementation of the obligations it imposes (the so-called 1267 Committee).[48] The Committee, which is composed of representatives from all 15 Members of the Security Council,[49] is mandated with the further collection of information from States as well as the preparation of reports to be submitted to the Council for consideration. To facilitate the Committee's work, Resolution 1267 imposes an obligation on Member States to fully comply with requests for information emanating from the Committee and to further assist it in the carrying out of its mandate.[50] In addition, the Resolution requires that Member States report to the Committee the steps they have taken to implement the Resolution within 30 days of its adoption.[51]

The framework established by Resolution 1267 has since been modified and strengthened through the adoption of subsequent Resolutions, modifying the Committee's functions.[52] As significant broadening of the 1267 sanctions, regime was operated by Security Resolution 1390 that extended the measures against the Taliban to Al Qaida and Usama bin Laden.[53] However, arguably the most important (and controversial) Resolution with respect to the Committee's mandate is Security Council Resolution 1333 (2000) that provides for the creation and updating of a list of the "*individuals and entities designated as being associated with Usama bin Laden including those in the al-Qaida organisation*,"[54] and has named the 1267 Committee the responsible monitoring body.[55]

---

[45] S/RES/1214 (1998), para. 13.

[46] S/RES/1267, operative para. 4 (a).

[47] S/RES/1267, operative para. 4 (b).

[48] S/RES/1267, operative para. 6.

[49] Guidelines of the Committee for the Conduct of its work (adopted on 7 November 2002, as amended on 10 April 2003, revised on 21 December 2005 and amended on 29 November 2006), para. 2 (a) (hereinafter "Guidelines").

[50] S/RES/1267, operative para. 9.

[51] S/RES/1267, operative para. 10.

[52] S/RES/1390 (2002), S/RES/1526 (2004), S/RES/1617 (2005), S/RES/1730 (2006), S/RES/1735 (2006).

[53] S/RES/1390 (2002), operative para. 2.

[54] The consolidated list is available at www.un.org/sc/committees/1267/consolist.shtml

[55] S/RES/1333 (2000), operative paras. 8 (c), 16 (b).

The "listing" of individuals and entities on the "terror list" is undertaken by the 15 Members of the Committee on recommendation from a Member State for inclusion on the list. Although the "nominating State" must provide justification for each listing request, the fact that the Committee's deliberations as a rule take place meeting behind closed doors[56] and is typically convened within two days notice[57] has led to pointed critique as to the process' fairness and transparency. The Committee's decisions are to be taken by consensus, or in cases, where consensus is impossible the matter is to be referred back to the Security Council.[58]

The Sanctions regime established by Resolution 1267 and further developed by its subsequent resolutions applies a broadly defined concept of association to Al-Qaida, Usama bin Laden, and the Taliban which is set out in Security Council Resolution 1617 (2005). However, for an individual to be put forward for inclusion on the list, it is not necessary that the person in question have been found guilty before a court of law, nor is it required that the he have ever been the subject of criminal accusations of any kind. This fact is explained by the Committee by the fact that the freezing of assets is intended to pursue a "preventive" rather than a repressive objective.[59] However, as shall be discussed below, this assertion may seem highly disingenuous when the extremely prejudicial effects of inclusion on the list are considered.

Furthermore, individuals and entities considered for listing are not given the opportunity to defend themselves or even gain access to the documents supporting their nomination to the list but rather are merely informed of the fact that they are being considered for listing as well as being made aware of their right to request their names to be removed from the list. According to the Committee's procedural rules, an individual or entity may petition his State of nationality or residence, to submit a request for his name to be removed from the list[60]; however, the State having put forth the listed person's name for inclusion must be consulted.[61] Furthermore, it has also been pointed out that pursuant to international public law, it is unclear whether a right to claim diplomatic protection from their State of origin against the UN exists.[62]

In addition to the severe stigma it entails, the practical consequences of inclusion on the 1267 Committee's for an individual or entity is a freezing of all assets, and

[56] Guidelines, para. 3 (b).

[57] Guidelines, para. 3 (a).

[58] Guidelines, 8 (e).

[59] Guidelines, para. 6 (c).

[60] Guidelines, para. 8 (a).

[61] Guidelines, para. 8 (b) and 8 (d). It is to be noted that although not mandatory, consultations between the "nominating State" and the State of the nominated person's nationality and/or residence are encouraged in the pre-submission phase (where the nomination States deems such consultations to be "appropriate").

[62] Al-Jumaili, D. (2008). Stationen im Kampf gegen die Terrorismusfinanzierung – New York-Brüssel-Berlin. *Neue Juristische Online Zeitschrift 2008 issue 4*, 188–211, at p. 192.

specifically for individuals, a ban on international travel.[63] Recognizing the fact that the freezing of assets may have grave consequences on the capacity of listed individuals to ensure their livelihoods, the Security Council enacted Resolution 1452 in 2002 through which it provides for the possibility for States to provide listed individual limited access to their frozen assets "necessary for basic expenses."[64]

Although the exclusive recourse for listed individuals and entities was to seek the submission of a request for de-listing on their behalf by their State of nationality/residence, this changed in 2006 with the adoption of Security Council Resolution 1730.[65] Through Resolution 1730, the Security Council sought to appease its critics and strengthen the de-listing framework by providing for the creation by the Secretary General of a so-called "focal point for delisting."[66] According to this modified structure, individuals and entities named on the 1267 Committee's Consolidated list may continue to address their requests for "de-listing" to the Committee through the intermediary of their State of nationality and/or residence, or may chose to forward the request directly to the Delisting focal point.[67] In response to the creation of this new "institution," some States have opted to decline the presentation of requests for delisting on behalf of their nationals/residents to the Committee and have instead adopted a uniform practice of referral of individuals seeking delisting directly to the focal point.[68] This approach may be criticized as an abdication of any potential influence these States may have had in assisting in the de-listing of their nationals/residents whose inclusion on the list may have been erroneous.

In Security Council Resolution 1735 (2006) adopted pursuant to Chapter VII, the Council attempted inter alia to provide general guidance to the Committee in the continued elaboration of a set of factors to be taken into consideration in the evaluation of de-listing requests. Thus, according to the Resolution, the Committee "*may consider among other things*" whether (1) the individual was placed on the list due to a mistake of identity, (2) whether the individual no longer meets the criteria for inclusion on the list [as set out in Resolution 1617 (2005)], and (3) whether the individual is deceased, or whether it has been demonstrated that the individual or entity has severed all association with Al-Qaida, Usama bin Laden, the Taliban, and their supporters including other individuals on the list.[69]

---

[63] Other serious consequences may also derive from inclusion on the list, given the fact that the daily updated list is available on-line for anyone with access to internet to consult.

[64] S/RES/1452 (2002), operative para. 1. Although the determination of the nature of the expenses is explicitly conferred upon States and subject to their entire discretion, para. 1 (a) is indicative of the sort of expenses to be authorized including food, rent, mortgages, medical treatment, taxes, insurance premiums and the reimbursement of expenses associated with the provision of legal services.

[65] S/RES/1730 (2006), para. 3.

[66] S/RES/1730 (2006), para. 3 outlining the focal point's duties.

[67] S/RES/1730 (2006), para. 3.

[68] This is notably the case of France since April 2007; cf. Al-Jumaili, p. 193.

[69] S/RES/1765 (2006), operative para. 14.

The listing process has without a doubt been the most controversial practice adopted pursuant to the UN's efforts to combat international terrorism given the opacity of the procedure, the severe limitation on a listed person's right, as well as the egregious consequences likely to result from inclusion on the list not to mention the difficulty of the delisting process. Indeed, as has been mentioned above, the Al Qaida and Taliban Sanctions Committee operates in closed sessions as a general rule and follows a procedure that denies any form of representation for the individual or entity being considered for listing and often basing its decisions on suspicions of varying degrees of credibility. Moreover, while the implications of inclusion on the 1267 Committee's list has grave prejudicial effects on individuals and entities, it is widely agreed that, although positive developments have occurred, insufficient safeguards exist to ensure transparency and the respect for due process rights.[70] Furthermore, even despite efforts to remedy this problem, the delisting process remains onerous and similarly devoid of transparency. The current framework also fails to provide for any form of compensation for individuals having suffered prejudicial effects resulting from their erroneous inclusion on the list.[71]

Given the considerations exposed above, it may come as no surprise that the listing framework has been a lightning rod for criticism emanating not only from institutional and academic circles but from civil society and the mainstream media,[72] and has been the object of several legal challenges.[73]

In a 2007 the Council of Europe report,[74] Special Rapporteur Dick Marty gives a damning appraisal of the UN listing procedure which he qualifies as Kafkaesque: "*It is frankly shocking to see that an international organization whose purpose it is to affirm the principles of peace, tolerance and justice uses itself means that do not respect the fundamental principles at the base of any restriction of individual freedom in any civilized country: the right to be heard, the right to appeal to an independent tribunal, that to a fair trial, the principle of proportionality.*

---

[70] This was notably also the position held by the Court of Justice of the European Communities in its recent decision in Kadi and Al Barakaat v. Council and Commission, Joint Judgment of Court of Justice of the European Communities, n° C-402/05 P, of 3 September 2008. Although the Court noted that attempts have been made to establish additional safeguards in the listing procedure, it noted that the failure of the process to afford individuals nominated for listing the opportunity to be heard was highly prejudicial to their rights.

[71] "UN Security Council Black Lists: Introductory Memorandum," (Rapporteur: Dick Marty), Committee on Legal Affairs and Human Rights, Council of Europe, AS/Jur (2007) 14, 19 March 2007 (hereinafter "Council of Europe Report").

[72] *See*, for example: Crawford, D. (2006). The Black hole of a UN Blacklist. *Wall Street Journal*, 2 October 2006.

[73] *See*, for example: Bosphorus Hava Yollari Turizm v. Ireland, application No. 45036/98, Grand Chamber, 30 June 2005; Kadi v. Council and Commission, judgment of 21 September 2005, ECR II-3649.; Ahmed Ali Yusuf and Al Barakaat International Foundation v. Council and Commission, judgment of 21 September 2005, ECR I-3533; Ayadi v. Council, judgment of 12 July 2006, T-253/02; Hassan v. Council and Commission, judgment of 12 July 2006, T-49/04.

[74] Council of Europe Report.

The Parliamentary Assembly of the Council of Europe can certainly not remain indifferent in the face of such abuses."[75]

3.3.3 Resolution 1373 and the Counter-Terrorism Committee

3.3.3.1 The Aftermath of the Attacks of 11 September 2001

On the day following the 11 September 2001 terrorist attacks on the USA, the Security Council convened an emergency session in which it elaborated Resolution 1368, which inter alia condemns the terrorist acts on New York, Washington DC, and Pennsylvania, and qualifies them as threats to international peace and security. Resolution 1368 also calls upon the international community to bolster its efforts to prevent and suppress terrorist acts including through increased cooperation, and "full implementation of the relevant international anti-terrorism conventions and Security Council resolutions, in particular resolution 1269."[76]

While Resolution 1368 was highly declaratory in nature, the substantive reaction of the UN Security Council to terrorist attacks on the USA would be contained within Security Council Resolution 1373.[77]

3.3.3.2 Resolution 1373: General and Contextual Aspects

Security Council 1373 was adopted on 28 September 2001 in the immediate aftermath of the terrorist attacks on the USA. Because the resolution was adopted pursuant to Chapter VII of the UN Charter (Threats to International Peace and Security), it is legally binding on all UN Member States. Failure to comply with Chapter VII resolutions may lead to punitive measures taken against recalcitrant States such as sanctions and embargos.

Despite its far-reaching scope and the broad and substantial obligations it imposes on Member States, the fact that Resolution 1373 was adopted unanimously and without being vetoed by one of the five Permanent Members of the Security Council testifies to both the importance ascribed to measures to combat terrorism as well as the universal condemnation of terrorist acts. That being said, it is commonly acknowledged that a binding Resolution as sweeping as Resolution 1373 would never have garnered unanimous approval by the Security Council and been adopted so quickly absent the backdrop of the 11 September terrorist attacks that brought with them a perceived urgency and need for decisive action.[78] As has been noted, the

[75] Council of Europe Report, p. 2.

[76] S/RES/1368 (2001), 12 September 2001.

[77] S/RES/1373 (2001), 28 September 2001.

[78] Condorelli, p. 834.

substantive content of the obligations contained within Resolution 1373 is, to a certain extent, a restatement of those found in previous instruments (in particular, the Convention for the Suppression of the Financing of Terrorism).[79] However, the primary innovative character of Resolution 1373 is attributable to the fact that these obligations are now enshrined in an instrument with binding force. Nonetheless, such is the importance of Resolution 1373 in the Global Legal Framework against Terrorism that it has been qualified as a "pillar" of this framework comparable to the universal legal instruments themselves.[80] In fact, several authors have expressed the opinion that the obligations incumbent on UN Member States pursuant to Resolution 1373 are comparable with those that would typically result from an international instrument.[81] When seen in this light, it is clear that the imposition of these obligations through a binding Security Council resolution as opposed to a multilateral treaty presents several practical advantages: bypassing the need for complicated negotiations, lengthy ratification periods required for the entry into force of the said instrument as well as avoiding weak or non-existent enforcement provisions.[82]

The corollary of this debate has been strong criticism directed at the Security Council to the effect that the imposition on Member States of the measures contained within Resolution 1373 constitutes a legislative act through which the Council has adopted a legislative role and has thus acted *ultra vires* the mandate conferred on it in the UN Charter.[83]

This debate has been further complicated by the fact that Resolution 1373 marks the first time that the Security Council has adopted a Chapter VII resolution, which is not aimed at a specific set of events having occurred but rather at "acts of terrorism" as such.[84] Also in contrast to previous resolutions, the validity of 1373 is not

---

[79] Betti, S. (2006). The Duty to Bring Terrorists to Justice and Discretionary Prosecution. *4 Journal of International Criminal Justice (2006)*, 1104–1116, at p. 1105; Fassbender, B. (2004). The Security Council and International Terrorism. In A. Bianchi (Ed.), *Enforcing International Law Norms against Terrorism* (pp. 83–102). Oxford, Portland: Hart Publishing, at p. 89.

[80] Gehr, W. (2003). Le Comite contre le terrorisme et la résolution 1373 (2001) du Conseil de sécurité. *Actualité et droit international, January 2003*, available at www.ridi.org/adi (consulted 15 August 2008), at p. 1; *see* also Condorelli, p. 834.

[81] Condorelli, p. 834 et seqq.; REF

[82] Codorelli, p. 834.

[83] Although a comprehensive exploration of this debate is beyond the limited scope of this chapter, a more detail account of the main arguments can be found in the following: Olivier, C. (2004). Human Rights Law and the International Fight against Terrorism: How do Security Council Resolutions Impact on State's Obligations Under International Human Rights Law (Revisiting Security Council Resolution 1373)? *73 Nordic Journal of International Law, 2004*, 399–419; Szasz, P.C. (2002). The Security Council Starts Legislating. *96 American Journal of International Law (2002)*, 901–905; Hinojosa Martinez, L.M. (2008). The Legislative Role of the Security Council in its Fight against Terrorism: Legal, Political and Practical Limits. *57 International Criminal Law Quarterly (2008)*, 333–359.

[84] Bianchi (2004), p. 498; Laborde, p. 67.

limited by geographic or temporal boundaries, conferring on it an open-ended character.[85] This fact has led the Policy Working Group on the UN and Terrorism to qualify Resolution 1373 as "*one of the most expansive resolutions in the history of the Council*."[86]

3.3.3.3 Resolution 1373: Substantive Aspects

In seeking to enjoin States to take concrete steps to combat different acts of terrorism or contribution thereto, Resolution 1373 imposes on States several obligations that have a direct and substantial bearing as well as wide-reaching implications on their national criminal law. The Resolution also espouses a multi-faceted approach to terrorism by addressing many of its constituent acts.

The wording of the two first paragraphs of Security Council Resolution 1373 leaves little doubt as to the biding nature of the obligations contained therein ("decides that all States shall…").[87]

Paragraph 1 of the Resolution takes aim at the financing of terrorism, recognizing that the stemming the flow of resources to would be terrorists is an effective method of limiting their ability to carry out terrorist attacks. As such, paragraph 1 provides for measures to prevent and suppress the financing of terrorism including the wilful provision or collection of funds "with the intention…or with the knowledge" that they are intended for use in the perpetration of acts of terrorism [para. 1(b)]. This paragraph also obligates Members States to freeze the funds and other assets of persons who commit (or attempt) acts of terrorism. It also creates an obligation on States to establish mechanism for the reporting of suspicious transactions to authorities.[88]

The criminalisation of terrorist acts is provided in the second paragraph of Resolution 1373, which also emphasizes their preparation and support. Further, paragraph 2 enjoins States to take all appropriate measures to bring terrorist to justice both within their national boundaries as well as to facilitate international cooperation in bringing terrorists to justice by "affording each other the greatest measure of assistance." Paragraph 2 further calls upon States to take all measures as to ensure that they refuse the right of asylum to terrorists as well as to establish effective border controls. In addition, States are called upon to strictly control the issuance of identity papers and travel documents.[89]

The wording of paragraph 3 of the Resolution ("calls upon States") would seem to indicate that this provision lacks the binding character of the ones before it.

---

[85] Betti, p. 1106.

[86] Report of the Policy Working Group, para. 32.

[87] Laborde, p. 67.

[88] SC/RES 1373 (2001), para. 1.

[89] SC/RES 1373 (2001), para. 2.

Paragraph 3 enjoins States to intensify the exchange of operational information and to increase their cooperation through the conclusion of bilateral and multilateral agreement and to fully ratify and implement the Universal Instruments against Terrorism. Despite the fact that that this provision is technically devoid of peremptory character, the broad emphasis placed by all agencies within the UN Secretariat on the measures it sets out is to be underscored. This is particularly the case for the call to ratify the Universal Instruments to which States have significantly responded in the post-11th September 2001 period.[90]

Paragraphs 4 and 5 of Resolution 1373 have a clear declaratory function. Indeed, while paragraph 4 notes the "close connection" between international terrorism and other forms of large-scale international criminality,[91] paragraph 5 declares that the "acts, methods, and practices of terrorism are contrary to the purposes and principles of the UN" and that "knowingly financing, planning, and inciting terrorist acts are also contrary to the purposes and principles of the UN."[92]

3.3.3.4 Counter-Terrorism Committee

Another fundamental feature of Resolution 1373 is that like Resolution 1267, it provides for the creation of a Security Council Committee intended to monitor the resolution's enforcement: the Counter-Terrorism Committee (CTC).[93] However, as will be seen below, the CTC's functions and mandate differ significantly from the Sanctions Committee created by Resolution 1267.[94] Although it is strictly speaking an organ of the Security Council, the functions undertaken by the CTC are primarily of a legal rather than a political nature, resting heavily of the legal analysis of national legislation.[95] As such, the committee, which is made up of all 15 Members of the UN Security Council, relies primarily on the work of independent legal experts in order to carry out its functions that consist essentially in holding States to account, following up on their obligation to report concrete measures they have adopted, as well as assisting them in meeting the obligations imposed on them.[96]

In order to support the CTC in its efforts, the Security Council adopted Resolution 1535 in 2004 through which it created the Counter-Terrorism Committee

---

[90] SC/RES 1373 (2001) para. 3.

[91] SC/RES 1373 (2001), para. 4: "transnational organized crime, illicit drugs, money-laundering, illegal drugs trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials."

[92] SC/RES 1373 (2001), para. 5.

[93] SC/RES 1373 (2001) para. 6.

[94] Gehr, p. 3.

[95] Gehr, p. 1, Laborde, p. 68.

[96] For the latest CTC report on the status of implementation of Resolution 1373, *see*: "Survey of the Implementation of Security Council Resolution 1373 (2001): Report of the Counter-Terrorism Committee," S/2008/379.

Executive Directorate (CTED). The CTED's stated mandate is to facilitate the provision of technical assistance to Member States as well as to facilitate cooperation with international, regional, and sub-regional organizations.[97]

Resolution 1373 "*calls upon*" States to report to the committee (initially within 90 days of the Resolution's adoption) in order to inform the Committee of the concrete measures (legislative, administrative, etc.) taken to implement the obligations contained within it.[98]

On receiving the initial reports from Member States, each report is thoroughly examined by one of the CTC's three sub-committees followed by the entire committee sitting in plenary session. The CTC's deliberations are further informed by advisory information received by the CTED. After having identified aspects of the Member State's report which require further clarification, the CTC contacts the Member State in question in order to request additional information related specifically to these aspects.[99] States are expected to respond to the CTC's request within a 3-month period. Within the first year of its operation alone, the Committee received and responded to over 280 reports. Since then, the number of reports has increased dramatically.[100] The thoroughness and professionalism with which the CTC has pursued its mandate has not only earned it the praise of the Secretary General but has also contributed to validating its creation and demonstrating its enormous potential.[101] Reflecting its success, the CTC saw its mandate further extended through Security Council 1624 (2005) that calls upon States to take measures against the "incitement to commit terrorist acts" in that this resolution also imposes a reporting obligation for which the CTC has been designated the competent body.

In the exercise of its mandate, the CTC is not endowed with any concrete enforcement powers. The Committee may nonetheless report voluntary inaction on the part of Member States in the implementation of the Resolution to the Security Council that may adopt measures pursuant to Chapters VI or VII as it sees fit. Since beginning its mandate, however, the CTC has adopted an approach based more on capacity building than coercion,[102] notably in recognition of the fact that Member States do not all dispose of the same resources and that the vast majority thereof are plagued by what it has called "competing developmental priorities."[103] In choosing an approach that emphasizes legal assistance rather than reprimand and in working together with Member States in identifying areas in which technical assistance activities are required, the CTC has acted as an essential component of efforts aimed

[97] S/RES/1535 (2004); *See also* "Proposal for the Revitalization of the Counter-Terrorism Committee," annexed to Security Council Document S/2004/124.

[98] Ibid.

[99] Laborde, p. 68.

[100] For more detailed information on the CTC and country reports *see*: www.un.org/sc/ctc/

[101] Quoted in Gehr, p.2.

[102] Gehr, p. 3.

[103] CTC 2008 REPORT, REF.

at the adherence of UN Member States to the Global Legal Framework against Terrorism and has acted as a force for law reform.[104] It has been pointed out that this may be one of the reasons for which States seem more willing to collaborate with the CTC than with the Al Qaida and Taliban Sanctions Committee discussed earlier.[105]

In keeping with its strong focus on capacity building, and in order to optimize available resources, the CTC has also created a Technical Assistance Coordination Team, which is inter alia, responsible for the maintenance of a technical assistance matrix which seeks to comprehensively list technical assistance activities undertaken by international, regional, and sub-regional organizations with the goal of avoiding overlap.[106]

3.3.4 The UN's Office on Drugs and Crime and the Terrorism Prevention Branch

In addition to the CTC's work in assisting States to comply with their obligations against terrorism, another pivotal institutional actor in the provision of technical assistance is the United Nations Office on Drugs and Crime (UNODC), acting through its Terrorism Prevention Branch (TPB). Although States are legally obliged to report to deal with the CTC, the recourse to the provision of technical assistance administered by the TPB is entirely voluntary in nature as it is subject to the receipt of an official request submitted by States requiring it.[107]

The Branch was established in 1998 following the re-organization of the UN Secretariat. Although initially responsible for pursuing research on various aspects of terrorism, TPB has since its mandate considerably evolved, and is now one of the primary bodies responsible for the delivery of technical assistance against terrorism.[108] This is primarily accomplished by encouraging States to ratify the UN instruments against terrorism; helping them to incorporate the obligations contained therein into their national law through the drafting of anti-terrorism legislation, and through the training of government actors and senior criminal justice officials. The Branch also assists States in fulfilling their reporting obligations to the Security Council Committees established pursuant to Resolutions 1267 and 1373.

---

[104] Nuotio, p. 1006.

[105] Foot, R. (2007). The United Nations, Counter-Terrorism, and Human Rights: Institutional Adaptation and Embedded Ideas. *29 Human Rights Quarterly (2007)*, 489–514, at p. 496.

[106] Laborde, p. 69.

[107] For more information on the Terrorism Prevention Branch's mandate and activities, *see*: "Delivering Counter-Terrorism Assistance," Terrorism Prevention Branch, United Nations Office on Drugs and Crime, April 2005.

[108] The original mandate to provide technical assistance to Member States was given by GA/RES/56/123, 19 December 2001 but has since been reiterated by the General Assembly (GA/RES/59/153) and by the Economic and Social Council.

In addition to its work with the CTC/CTED, the TPB also benefits from its placement within the UNODC and works closely with other UNODC bodies in the terrorism-related areas of anti-money laundering, organized crime, and corruption.

Although a seldom discussed actor in academic literature, the role played by the TPB is central to the implementation of the obligations stemming from the legal framework against terrorism. In particular, the voluntary nature of its provision of its expertise, its transparency and its focus on capacity-building, have made the Branch an attractive partner for States requiring its support. Thus, since it was given the mandate of providing technical assistance, the Branch has completed several hundred technical assistance activities and has participated in the training of thousands of senior criminal justice officials.[109]

3.3.5 The Global Counter-Terrorism Strategy

In 2002, the Policy Working Group on the UN and Terrorism issued a report in which it advocated the adoption of a three-pronged approach to fighting terrorism consisting of: dissuading disaffected groups from embracing terrorism, denying groups or individuals the means to carry out acts of terrorism, and sustaining broad-based international cooperation in the struggle against terrorism.[110]

In a speech in Madrid in 2005, one year after the terrorist attacks there, then UN Secretary General Kofi Annan laid out his vision for a comprehensive global framework which he suggested should be founded on five pillars which in large part reflected the findings of the working group:

- Dissuading groups from resorting to terrorism,
- Denying terrorists the means to carry out and attack,
- Deterring States from supporting terrorist groups,
- Developing State capacity to defeat terrorism, and
- Defending human rights in the context of terrorism and counter-terrorism.[111]

In order to assist in coordinating action against terrorism within the Organization, the Secretary General established the *Counter-Terrorism Implementation Task Force* in 2005, which is composed of representatives from nearly 19 departments

[109] *See* www.unodc.org/unodc/en/terrorism/unodcs-taas.html according to which between 2002 and 2006, assistance was provided to 125 States and over 4,600 national officials have participated in technical assistance activities.

[110] "Report of the Policy Working Group on the United Nations and Terrorism," UN Document A/57/273 or S/2002/875.

[111] Address of the Secretary General on the occasion of the one year anniversary of the terrorist attacks on Madrid, Madrid, Spain, 10 March 2005.

and UN agencies, and is responsible for the overall coordination of at least two dozen bodies within the UN system.[112]

The Secretary General's proposal was further refined and set out in a report submitted to the Plenary of the General Assembly in 2006, in which the Secretary General detailed the Organization's existing activities and put forward suggestions to improve its work.[113] The General Assembly, basing itself on the Secretary General's report adopted the UN Global Counter-Terrorism Strategy in September 2006.[114]

Reflecting the recommendation set out above, UN action against terrorism has not been limited to the Security Council and General Assembly, but has also involved several other UN agencies and bodies as well as other stakeholders such as international, regional, and sub-regional organizations as well as national governments. Although a degree of de facto coordination of these interactions had evolved, it soon became apparent that an overarching strategic framework against terrorism was needed in order to streamline international efforts against terrorism and to increase the Organization's effectiveness in contributing to this pursuit. The idea of a comprehensive global counter-terrorism strategy was first officially advanced by the *High-Level Panel on Threats, Challenges, and Change* in its 2004 report. In its report, the Panel advocated the adoption of a global comprehensive strategy against terrorism which would address factors that facilitate terrorism, strengthens the capacity of States and the rule of law and which would also promote respect for fundamental human rights.

3.3.6 The Comprehensive Convention and the Elusive Definition of Terrorism

As has been eluded to throughout this chapter, the failure of Member States to agree on a comprehensive definition of "terrorism" has been a defining characteristic of the evolution of the UN legal framework since its very inception and has had profound repercussions on the development of this framework. Indeed, the international community's inability to agree on this point can be seen as having severely hampered early efforts to adopt a comprehensive set of measures aimed at fighting terrorism, and continues to constitute a severe impediment to the adoption of a Comprehensive Convention against Terrorism.

However, it is to be noted that although the definition remains an elusive one, substantial progress has been made, since the first Convention was adopted in 1963.

---

[112] *See* "Implementing the Global Counter-Terrorism Strategy: Fact Sheet," Peace and Security Section, Department of Public Information, DPI/2439B/Rev.1, May 2007.

[113] "Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy: Report of the Secretary General," A/60/825, 27 April 2006.

[114] The United Nations Global Counter-Terrorism Strategy, 6 September 2006, A/60/L.62.

One of the important first steps forwards in delineating the concept of "terrorism" was the consensus mentioned above, reached in the 1990s and first expressed in the 1994, the UN General Assembly *declaration on measures to eliminate international terrorism* to the effect that politically motivated acts of violence directed against civilians could not be justified under any circumstances whatsoever and which was echoed by Security Council Resolution 1269 (1999).[115]

Another important step forward in the search for a comprehensive definition was taken with the preparation of the *International Convention for the Suppression of the Financing of Terrorism* by the Ad Hoc Committee as well as its adoption by the General Assembly, ratification by Member States and subsequent entry into force. In drafting the Financing Convention, the Committee was faced with the daunting task of having to elaborate a legal text that would proscribe the financing of a form of criminality, which theretofore had not been explicitly defined. As the finalized text of the Convention demonstrates, the Committee was able to arrive at a skilful definition "acts of terrorism" for the purpose of the Convention's application which blended a reference to pre-existing instruments with an intent-based and conceptual approach. Thus, Article 2 of the Financing Convention defining the offence of terrorist financing reads as follows:

> Article 2
> 1. Any person commits an offence within the meaning of this Convention if that person by any means, directly of indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
> (a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
> (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such an act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.
> […]

Despite the seemingly comprehensive character of the definition given in the Financing Convention, it is widely agreed that it was exclusively intended to enable the application of the Convention per se. As the UN global legal framework against terrorism gains momentum and the measures it espouses grow in scope and complexity, the Organization has had to adopt purpose oriented "working definitions" to avoid paralysis in the implementations of these measures. A further example of this approach can be found in Security Council 1566 adopted in October 2004 which contains descriptions of acts of terrorism aimed at protecting civilians:

> 3. "Recalls that criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable

[115] Cf operative para. 1.

> by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented to ensure that such acts are punished by penalties consistent with their grave nature;"

Thus, the wording of the working definition given in Resolution 1566 refers to the offences "as defined in international protocols relating to terrorism."[116]

Reflecting the fact that the issue of comprehensive definition has not been settled by the adoption of "working definitions," the General Assembly adopted Resolution 59/46 in December 2004, in which it reiterated the mandate previously conferred on the Ad Hoc Committee for the continued elaboration of the Comprehensive Convention on International Terrorism which is on-going.[117]

Although great strides have been made in the Convention's elaboration and the issues of agreements outweigh those of contention, two central issues in addition to the question of definition continue to stand in the way of agreement. The first of these issues is the relationship between terrorism and anti-colonial and national liberation movements the substantive details of which has yet to be comprehensively agreed upon. The second remaining issue of contention is the controversial application of the Convention to the activities of States' armed forces in the context of armed conflict and in the carrying out of their official duties.[118]

In addition, a practical issue remains as to what the exact legal relationship of a Comprehensive Convention would be with the existing legal instruments against terrorism.[119]

3.3.7 Human Rights

Since the terrorist attacks on the USA in 2001, there can be no doubt that measures intended to combat terrorism at the national, regional and international levels have increased exponentially. As has been commonly acknowledged, a negative by-product of this development has been that the expansion of anti-terrorism measures has occurred at the detriment of respect for civil liberties and human rights. This is principally due to the fact that the rigid adherence to human rights guarantees has commonly been perceived as hindering the effective prosecution of measures aimed at combating terrorism. The negative repercussion of the adoption of anti-terrorism

---

[116] Id.

[117] *See* website of the "Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996" at www.untreaty.un.org/cod/terrorism/index.html

[118] Hmoud, M. (2006). Negotiating the Draft Comprehensive Convention on International Terrorism: Major Bones of Contention. *4 Journal of International Criminal Justice (2006)*, 1031–1043, at p. 1034; for a summary of the developments having occurred in the course of the negotiations, *see*: The Draft Comprehensive Convention on International Terrorism, Centre for Nonproliferation Studies, 8 November 2006.

[119] *See* www.unodc.org/unodc/terrorism/conventions.html

measures has acknowledged in various echelons of the UN structure not least of which being that of the Secretary General himself.[120]

While various UN actors have advocated the need for a strict adherence to human rights in the elaboration of measures against terrorism,[121] the realities of the implementation of many of the obligations incumbent on States by virtue of UN instruments have in many instances been problematic. Compounding this problem is the fact that while many States have unwillingly infringed on human rights in their haste to adopt measures against terrorism, others have availed themselves of the fight against terrorism as a pretext allowing them to curtail the rights of their populations.[122] As has been pointed out, seen against this backdrop, the adoption of draconian measures against terrorism which violate human rights may in fact be paradoxical in that terrorism has been proven to actually flourish in the absence of strong human rights frameworks.[123] This is particularly striking in light of the UN's purported commitment to address the so-called "roots causes" of terrorism. It is therefore noteworthy that within the UN context, the two structures against terrorism posing the greatest potential threat to human rights, namely the frameworks established by Resolutions 1267 and 1373, are also among those which seem to afford them the least importance.[124]

However, as has been seen earlier, the Organization and its membership have recognized these shortcomings and have sought to adopt measures aimed at correcting this imbalance, leading some to contend that the initial hard-line approach may have to some extent yielded to one that is more sensitive to human rights concerns.[125] Although the pendulum appears to be swinging the way of a renewed emphasis on human rights, additional measures that would contribute to firmly anchoring human rights within the UN's anti-terrorism framework are clearly needed.

As the choice means for the implementation of international obligations stemming from UN instruments is left to States, the actions of bodies such as the Office of the UN High Commissioner for Human Rights in assisting States to understand and respect their human rights obligation in the context of the fight against terrorism are to be underscored. Moreover, the incorporation of further human rights consideration in the technical assistance provided by the CTC and UNODC may also prove to be an effective and desirable outcome.

---

[120] In a 2005 speech, Kofi Annan noted the negative impact that the adoption of counter-terrorism measures has had on human rights, Press release, "Secretary General Offers Global Strategy for Fighting Terrorism," UN Doc. SG/SM/9757 (10 March 2005), available at www.un.org/News/Press/docs/2005/sgsm9757.doc.htm

[121] E.g. S/RES/1456 (2003); *see also* Laborde & DeFeo, in which Laborde, the Chief of the Terrorism Prevention branch argues against an interpretation of anti-terrorist measures as being antagonistic to human rights and advocates a "synergy" between the two concepts.

[122] Foot, p. 490.

[123] *See* Krueger, A. B., & Maleckova, J. (2003). Education, Poverty and Terrorism: is there a Causal Connection? *17 Journal of Economic Perspectives (2003)*, 119–144.

[124] Foot, p. 491.

[125] Foot, p 491.

3.4 Conclusion

As the saying goes if the UN framework against terrorism did not exist, we would need to invent it. Indeed, although it is far from perfect, the UN framework is the by far the most viable and comprehensive global structure against terrorism which exists today. The evolution of this framework has been confronted with significant difficulties from its very inception owing to political tensions as well as the evolving nature of terrorism itself. However, the repeated perpetration of large-scale acts of international terrorism, including but not limited to those of 11 September 2001, has emphasized the need for Member States to take action; a call to which they have largely responded.

While there is no doubt that this concerted action has yielded impressive results, the speed with which these developments have occurred has inevitably led to "growing pains," specifically in the organization's shift from a reactive approach towards terrorism to its new focus on prevention. In seeking to adopt the most effective measures for the prevention of terrorism and terrorist financing, the UN has been confronted by many of the same difficulties as that of its constituent Members, namely that of balancing the interests of security with respect for human rights and due process guarantees.

In this light, it is questionable whether the perceived gains realized through the adoption of certain draconian measures adopted by the UN and its Member States to prevent terrorism will not be outweighed by their unintended effects on the protection and promotion of human rights. Therefore, the measures adopted by the UN in an attempt to remedy this imbalance are to be welcomed.

The role of the UN in the Prevention and Repression of Terrorism which has progressively developed over the past decades has been significantly accelerated since the terrorist attacks of 11 September 2001. While having identified terrorism early on as an issue needing to be addressed, the development and widespread adoption of concrete measures aimed at combating this phenomenon within the UN framework have historically been severely hindered by geopolitical realities as well as marked differences in the strategies espoused by the organization's Member States. As a result of these difficulties, the historical approach taken by the UN in addressing the issue of terrorism has been the development of a pragmatic piecemeal legal framework aimed at criminalizing certain "terrorist acts" subject to widespread agreement. With the passing of the decolonization period and the end of the Cold War, some of the substantive legal and political issues of contention surrounding terrorism have subsided heralding the advent of an environment more conducive to agreement.

The principle catalyst for change has, however, been the events of 11 September 2001 that have illustrated both the scale of the global threat posed by terrorism as well as the need for a comprehensive strategy to combat it. The UN has been at the vanguard of the push to develop this new strategy and has established a multi-faceted anti-terrorism framework. Despite the fact that the best known and most controversial UN initiatives against terrorism are primarily those of a coercive nature stemming from the adoption of binding Security Council resolutions, UN action against terrorism is by no means limited to these measures.

This chapter aims to shed light of the various institutions and mechanisms within the UN structure that contribute to the combating of terrorism and to provide a summary appraisal of their effectiveness.

3.5 Annex II

Relevant Security Council Resolutions

1. Threats to international peace and security caused by terrorist acts:	
S/RES/1269 (1999)	On international cooperation in the fight against terrorism
S/RES/1373 (2001)[a]	On international cooperation to combat threats to international peace and security caused by terrorist acts
S/RES/1535 (2004)	Creation of the Counter-Terrorism Executive Directorate (CTED)
S/RES/1566 (2004)[a]	Descriptions of acts of terrorism aimed at protecting civilians; establishment of a working group for the identification of terrorist entities and groups not associated with the Taliban; creation of an international fund to compensate victims of terrorist acts
2. On measures against Al-Qaida, Usama Bin Laden, and the Taliban:	
S/RES/1267 (1999)[a]	On measures against the Taliban
S/RES/1333 (2000)[a]	On measures against the Taliban
S/RES/1363 (2001)[a]	On the establishment of a mechanism to monitor the implementation of measures imposed by resolutions 1267 (1999) and 1333 (2000)
S/RES/1390 (2002)[a]	On the extension of measures against the Taliban to Al Qaida and Usama Bin Laden
S/RES/1452 (2002)[a]	On implementation of measures imposed by paragraph 4 (b) of Resolution 1267 (1999) and paragraph 1 and 2 (a) of Resolution 1390 (2002)
S/RES/1455 (2003)[a]	On improving implementation of measures imposed by paragraph 4 (b) of Resolution 1267 (1999), paragraph 8 (c) of Resolution 1333 (2000), and paragraphs 1 and 2 of Resolution 1390 (2002) on measures against the Taliban and Al-Qaida
S/RES/1526 (2004)[a]	Creation of the monitoring team
S/RES/1617 (2005)[a]	1267 Committee checklist
S/RES/1699 (2006)	General issues relating to sanctions (cooperation between INTERPOL and the 1267 Committee)
S/RES/1730 (2006)	General issues relating to sanctions (de-listing procedure)
S/RES/1735 (2006)[a]	Establishment of a focal point for the listing and de-listing procedure
3. On international human rights, refugee, and humanitarian law:	
S/RES/1456 (2003)	Declaration on the issue of combating terrorism
4. Non-acquisition of weapons of mass destruction for terrorist purposes:	
S/RES/1540 (2004)	Non-acquisition of weapons of mass destruction; their means of delivery and related materials by non-state actors for terrorist purposes
5. On incitement to commit terrorist acts:	
S/RES/1624 (2005)	On incitement to commit terrorist acts

[a]Legally binding on Member States as adopted pursuant to Chapter VII of the UN Charter (Threats to International Peace and Security)

References

Al-Jumaili, D. (2008). Stationen im Kampf Gegen Die Terrorismusfinazierung – New York-Brüssel-Berlin. *Neue Juristische Online Zeitschrift 2008 issue 4*, 188–211.

Betti, S. (2006). The Duty to Bring Terrorists to Justice and Discretionary Prosecution. Journal of International Criminal Justice 4, 1104–1116.

Bianchi, A. (2004). Enforcing International Law Norms Against Terrorism: Achievements and Prospects. In A. Bianchi (Ed.), *Enforcing International Law Norms against Terrorism* (pp. 491–534). Oxford, Portland: Hart Publishing.

Bianchi, A. (2006). Security Council's Anti-Terror Resolutions and Their Implementation by Member States: An Overview. Journal of International Criminal Justice 4, 1044–1073.

Condorelli.

Crawford, D. (2006). The Black Hole of a UN Blacklist. *The Wall Street Journal*.

Fassbender, B. (2004). The Security Council and International Terrorism. In A. Bianchi (Ed.), *Enforcing International Law Norms against Terrorism* (pp. 83–102). Oxford, Portland: Hart Publishing.

Foot, R. (2007). The United Nations, Counter-Terrorism, and Human Rights: Institutional Adaptation and Embedded Ideas. *Human Rights Quarterly 29*, 489–514.

Gehr, W. (2003). Le Comite contre le terrorisme et la résolution 1373 (2001) du Conseil de sécurité. *Actualité et droit international, January 2003, available at* www.ridi.org/adi (consulted August 15, 2008).

Gross, L. (1973). International Terrorism and International Criminal Jurisdiction. American Journal of International Law, 67(3), 508–511.

Hinojosa Martinez, L.M. (2008). The Legislative Role of the Security Council in its Fight against Terrorism: Legal, Political and Practical Limits. *International Criminal Law Quarterly 57*, 333–359.

Hmoud, M. (2006). Negotiating the Draft Comprehensive Convention on International Terrorism: Major Bones of Contention. *Journal of International Criminal Justice 4*, 1031–1043.

Kolb, R. (2004). The Exercise of Criminal Jurisdiction over International Terrorists. In A. Bianchi (Ed.), *Enforcing International Law Norms against Terrorism* (pp. 227–282). Oxford, Portland: Hart Publishing.

Kovacs, P. (2002). Le grand précédent: la Société des Nations et son action après l'attentat contre Alexandre, roi de Yougoslavie. *European Integration Studies, 1*, 30–40.

Krueger, A. B., & Maleckova, J. (2003). Education, Poverty and Terrorism: is there a Causal Connection? *Journal of Economic Perspectives 17*, 119–144.

Laborde, J.P.

Laborde, J.-P., & DeFeo, M. (2006). Problems and Prospects of Implementing UN Action against Terrorism. *Journal of International Criminal Justice 4*, 1087–1103.

Nuotio, K. (2006). Terrorism as a Catalyst for the Emergence, Harmonization and Reform of Criminal Law. *Journal of International Criminal Justice 4*, 998–1016.

Olivier, C. (2004). Human Rights Law and the International Fight against Terrorism: How Do Security Council Resolutions Impact on State's Obligations Under International Human Rights Law (Revisiting Security Council Resolution 1373)? *Nordic Journal of International Law, 73*, 399–419.

Saul, B. (2006). The Legal Response of the League of Nations to Terrorism. *Journal of International Criminal Justice 4*, 78–102.

Szasz, P.C. (2002). The Security Council Starts Legislating. *American Journal of International Law 96*, 901–905.

Weigend, T. (2006). The Universal Terrorist: The International Community Grappling with a Definition. *Journal of International Criminal Justice 4*, 912–932.

Chapter 4
The European Union as an Actor in the Fight Against Terrorism

Thomas Wahl

4.1 Introduction

The thwarted plot to attack the Christmas market in Strasbourg in 2000; the horrible bombings in Madrid in March 2004 and London in July 2005, which slaughtered a number of civilians; the assassination of Theo Van Gogh, a Dutch film director and critic of Islam, in Amsterdam in November 2004; the failed suitcase bombings on regional trains in Germany on 31 July 2006; menaces of the al-Qaeda network to eye France as one of its next targets in September 2006; and eventually the fact that important wirepullers of the dreadful attacks in New York on 11 September 2001 resided in Germany and Spain reminded European governments anew that Europe is not immune from contemporary forms of terrorism, i.e. international and Islamic terrorism. It also again raised awareness that preventing terrorist attacks and prosecuting terrorist offenders cannot be solved by the nation state alone but by – the indispensable – international cooperation, because terrorist groupings operate and cooperate across borders and terrorism is a threat common to all democratic societies, which requests concerted actions.

This understanding was clear for European governments already in the early forms of terrorism on the European territory after the Second World War, such as terrorist acts by the IRA in Northern Ireland and the British mainland, ETA in Spain, the RAF in Germany, the Red Brigades in Italy, or the Algerian FIS in France. As a result, European States, which already worked successfully within the European Economic Community (EEC, which comprised nine Member States since 1973) pooled their experience in the TREVI working group formally established in 1976.[1]

T. Wahl (✉)
European Criminal Law Section, Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: t.wahl@mpicc.de

[1] TREVI expresses the acronym for Terrorism, Radicalism, Extremism, and International Violence and is in memory of the famous fountain in Rome, where the meeting of justice and home affairs ministers deciding on the establishing of TREVI took place in 1975.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_4,

Practical cooperation to fight terrorism among the EEC Member States was preferred because the States could already build on common values and homogeneity – two prerequisites for the necessary mutual confidence into the legal systems of each other and matters that the second main European Organisation, the Council of Europe, could and can not provide for.[2] However, law enforcement cooperation via TREVI took place outside the EEC framework! TREVI was designed to be an intergovernmental forum (meetings of ministers responsible for internal security, civil servants, and representatives of police and security services) to coordinate an effective response to international terrorism.[3]

The main objectives of TREVI were cooperation in the fight against terrorism and exchange of information about the organisation, equipment, and training of police organisations, especially tactics employed against terrorism. The concrete measures adopted by the TREVI working groups included the exchange of information on terrorist activities, techniques to face up to terrorist acts, control of arms trafficking, exchange of police personnel, and the protection of the safety of civil aviation.[4]

From the outset, activities and meetings of the TREVI working groups were kept secret, public information on the results of their work was only given sporadically.[5] Parliamentary scrutiny did not take place, at least not effectively. This structure triggered criticism by the European Parliament and civil rights organisations blaming TREVI for its lack of transparency and of external democratic control.[6] However, from a political and practical perspective, the TREVI cooperation is considered a success.[7] From a legal perspective, the most promising attempts to fight terrorism by a common approach of European States in the 1970s and 1980s took place within the framework of the Council of Europe.[8]

---

[2] Vennemann (2003a), p. 222.

[3] Anderson et al. (1995), p. 53. For the development of the different TREVI working groups, see Gueydan (1997), p. 105.

[4] Vennemann (2003a), p. 220

[5] Messelken (2003), p. 9.

[6] Anderson et al. (1995), p. 56.

[7] Eventually, the TREVI working groups were a pathfinder for several well-established institutions today, such as Europol, which were formally adopted after the entry into force of the Maastricht Treaty in 1993 (see below). By that time, the TREVI structures were integrated into the European Union.

[8] After the Second World War, the Council of Europe especially fostered judicial cooperation in the criminal law field by a series of conventions. A particular convention in the field of terrorism is the European Convention for the Suppression of Terrorism, on which the European States agreed within the Council of Europe in 1977 (ETS No. 90, entry into force on 4 August 1978). The main element of the Convention is the principal abolishment of the political offence exception for extradition for specific enumerated offences. In 2005, the Convention on the Prevention of Terrorism was adopted (ETS No. 196, entry into force on 1 June 2007). The Convention provides for ways of Member States on how to prevent terrorism: First, criminal offences for certain acts that may lead to the commission of terrorist offences (namely: public provocation, recruitment, and training) are established. Second, co-operation on prevention both internally and internationally is reinforced.

Counter-terrorism policies in Europe were established in a climate of domestic terrorism. However, terrorism that the world predominantly faces today by al-Qaeda and its network has changed in comparison with the terrorism of ETA or IRA.[9] Whereas the latter is traditionally active in the territory of a certain State, the first is international and/or imported. Meanwhile, also the European (Economic) Community has changed, in particular when it merged into the European Union (EU) by the beginning of the 1990s with a view to political integration in the area of justice and police cooperation. This evolution gives cooperation of Member States a new shape and new forms of acting.

This chapter mainly looks into the question of whether the EU can be considered a strong actor in the worldwide fight against terrorism. Related to this are questions such as what the peculiarities of the EU and its "added value" in comparison with other international organisations, such as the United Nations, are; how did it come that there is panoply of measures to counter terrorism emanating from the EU; and to which extent the organisation's contributions were significant and effective to counter the changing forms and types of modern terrorism? In order to understand how the EU's role is perceived in the "War on Terrorism", it is crucial to have first an inherent understanding of what the EU actually is. Therefore, the following section, first, outlines the nature and structure of the EU (Sect. 4.2). The next section provides an overview of the relevant legal framework the EU has at its disposal to adapt counter-terrorism measures (Sect. 4.3). In Sect. 4.4, the EU's arsenal of counter-terrorism measures since 2001 is explored in more detail before assessing the main existing deficiencies of the EU as an actor in the fight against terrorism and possible future directions in the concluding remarks (Sect. 4.5).

4.2 Structure of the European Union

It is no easy task to describe the structure and nature of the European Union. Jacques Delors, Former President of the European Commission, called the EU an "unidentified political object".[10] In contrast to other European Organisations, such as the Council of Europe or the OSCE, the EU goes beyond an international organisation in the classic sense of international public law. The EU's current shape was modelled by the Treaty of Maastricht of 1992, which must be considered the most incisive reform of European integration. It was further developed by the Treaty of Amsterdam of 1997 and the Treaty of Nice of 2001. The next stage of closer integration will be achieved by the Treaty of Lisbon of 2007, which will enter into force after all 27 EU Member States have ratified it. The objectives of the

[9] EU TE-SAT report 2002, p. 20 and 21; Javier Solana, EU High Representative of the Common Foreign and Security Policy, European Council Thessaloniki of 20 June 2003, p. 5 (http://ue.eu.int/ueDocs/cms_Data/docs/pressdata/en/reports/76255.pdf, last visited: July 2009); Wilkinson (2005).

[10] Drake (2000), p. 5.

treaty reforms were to enable the EU to meet new challenges, in particular, the enlargement of the EU (from 12 Member States in 1992 to 27 Member States since 2007), but also the increase of international crime, including terrorism.

The latter aspect is closely connected with the birth of the EU since the pre-existing European (Economic) Community set a new goal, i.e. to establish an area without internal borders and the free movement of persons by the end of 1992.[11] This area was in fact achieved in 1995 by a group of Member States signing the Schengen Agreement.[12] It was feared that the abolishment of internal borders would also benefit criminals, so that Member States of the European Community (EC) had to think about compensatory measures to meet the loss of border controls within the formal structures of the EC. Another reason for the creation of the EU was that, at an external level, the collapse of communism in Eastern Europe and the outlook of German reunification led to a commitment to reinforce the Community's international position. As a result of these internal and external events, the Maastricht Treaty formalised and institutionalised the political cooperation of Member States of the European Community in the fields of foreign policy and policy of justice and home affairs – cooperation that had hitherto been informal and not structured outside the EC, e.g. as it was the case with the mentioned TREVI cooperation.[13] Thus, the Maastricht Treaty adds the two components entitled Common Foreign and Security Policy (CFSP) and cooperation in the field of Justice and Home Affairs (JHA) to the existing framework, which is focused on economic integration, i.e. the founding treaties of 1952 and 1957 establishing the European Coal and Steel Community, the European Atomic Energy Community, and the European Economic Community (the European Communities).

However, because these two new components are very sensitive issues in terms of national sovereignty, the legal structure widely maintains the intergovernmental cooperation and does not merge them into the structures of the European Communities. This led to the rather complicated architectural object, which is often referred to as the "pillar structure", in which the European Communities form the first pillar, retaining their own legal status (i.e. legal personality), own institutional framework, own decision-making processes, etc. designed to implement their economic goals.[14] Alongside this, the CFSP and the JHA form the second and third

[11] Single European Act of 1987, OJ (Official Journal) L 169 of 29 June 1987.

[12] On 26 March 1995, the 1990 Convention Implementing the Schengen Agreement of 1985 came into force. The Schengen area is not identical with the EU area because some EU Member States, such as the UK and Ireland, are not parties, but apply only certain provisions. In addition, non-EU Member States, such as Norway, Ireland, and Switzerland, are part of the Schengen area. With the Amsterdam Treaty, the Schengen acquis was integrated into the EU's legal and institutional framework.

[13] For the cooperation concerning the foreign and security policy, see Eaton (1994), pp. 215ff.; for cooperation in justice and home affairs issues, see Peers (2006), p. 6.

[14] The most important one is the European Community (EC), based on the Treaty establishing the European Community (TEC). Reference is made in the following to the EC only. Since 2002, the EC picked up the European Coal and Steel Community.

pillars, with own sets of rules to achieve their objectives (Title V and VI Treaty on European Union [TEU]).[15] The European Community follows the supranational approach or "Community method", which is characterised by the following elements:

- Establishment of a common market as the common goal of the European Community is achieved by a conferral of powers for certain policies from the Member States to the Community.
- Sophisticated system of decision making, where, in principal, the Council (made up of representatives of the governments of the Member States) is acting equally together with the European Parliament (representing the people of the Community) in the co-decision procedure (Art. 251 TEC).
- For most policy areas of the Community, decisions in the Council can be taken by qualified majority vote (Art. 205 TEC), i.e. against the will of individual Member States.
- The Commission, as the EU's executive body independent of governments, upholds the collective European interest and ensures that EC policies are properly implemented, e.g. by bringing Member States to the European Court of Justice if they infringe or refuse implementation of Community law.
- Decisions of Community institutions can be taken with binding direct effect on the Member States and/or its citizens; in particular, the EC can act through Regulations that entail simultaneous, automatic, and uniform binding effect in all the national legal systems without the need of further incorporation into national law (Art. 249 TEC).

The main facts of the intergovernmental approach taken by the second and third pillars are as follows:

- Decision making by Member States is orientated on consensus; as a rule, decisions are taken by the Member States in the Council by unanimity.
- Very limited role of the other institutions, i.e. the European Parliament (EP) is only consulted in the policy areas of CFSP and JHA (cf. Art. 21, 39 TEU), the Commission has no powers to enforce non-implementation or false implementation of measures taken, the European Court of Justice has no or very few control powers.
- No instrument with direct applicability, so that every act must be transposed by Member States into national law.[16]

As a result, the pillars reflect three separate approaches to integration; the EU does not form a unified European legal order. The EU only cramps these three pillars by common provisions (commonly referred to as the roof), which, inter alia,

[15] For consolidated versions of the treaties, see OJ L 325 of 24 December 2002.

[16] For a detailed analysis of the Community method vs. intergovernmental method, see for example Demaret (1994), pp. 3ff.; Oppermann, § 6 mn. 6ff.

address the objectives of the Union, the rule of consistency and continuity relating to individual measures adopted in the three pillars, the distinct powers of the EU's institutions depending on the pillar, and provisions on the human rights protection, and the national identity of Member States.

It is not a surprise that this structure triggered different final legal assessments by scholars. The view is very much dependent on whether one allocates to the EU legal personality with the consequence of being a subject of international law. Preferable is the view that the EU is a "compound of states and international organisations (the communities)" operating through a hybrid system of intergovernmentalism and supranationalism without having a legal personality and own competences. The European Union is only a forum for the States to form their will and make decisions. Decisions that are taken in the framework of the second and third pillars can not be attributed to the Union but only to the Member States.[17]

4.3 Foundations for the EU's Counter-Terrorism Response

4.3.1 Fighting Terrorism as a Cross-Pillar Task

Analysts agree that the Maastricht Treaty and the later revision by the Amsterdam Treaty in 1997 established the basis for a swift and common reaction of the European Union's Member States to the attacks of 9/11 as well as let the European Union appear as a visible actor in the fight against terrorism.[18] The Treaty on European Union as well as the Treaty establishing the European Community provides for an arsenal on which the EC Member States could not rely when working together against terrorist threats in the 1970s and 1980s. The multifaceted nature of international terrorism, as it emerged in the 1990s and shown quite plainly by the attacks of 9/11, revealed that not only internal security issues are at stake but foreign policy is also affected and even military implications had to be considered. Therefore, condemning the threat of terrorism is conceived as a challenge affecting all three pillars. The European Union and its Member States indeed have made use of the whole broad spectrum that is offered by the pillars (see the following). In addition, responses to counter-terrorism revealed that the boundaries between the pillars have been blurred because a lot of individual reactions, such as combating terrorist financing, crises management, or the external dimension of counter-terrorism must be addressed across the pillars (*cross-pillarisation*, see below, Sect. 4.3.2).

The *Common Foreign and Security Policy* (CFSP, second pillar) covers all areas of foreign and security policy. It is related to the maintenance of external security

[17] Pechstein and Koenig (2000), mn. 92; Schweitzer and Hummer (1996) mn. 66.

[18] Cf., among others, Den Boer (2003a), p. 188; Messelken (2003); Verbruggen (2004), p. 303; Monar (2004), p. 140; Dittrich (2005); Keohane (2005).

of the "Union" whereas cooperation in Justice and Home Affairs (JHA, third pillar) is tangential to internal security. The CFSP enables a permanent exchange of issues relating to international policy, and leads to alignments of national positions including the establishment of common concepts and their implementation into concrete actions. The establishment of permanent bodies responsible for CFSP in Brussels since 2000 as well as the work of the High Representative for the common foreign and security policy, Mr. Javier Solana (since 1999), were essential factors for sharpening the "anti-terror profile" of the EU and better visibility of European foreign policy after the attacks of 9/11. An important provision is Art. 11 TEU, second indent, which defines the "strengthening of the security of the Union in all ways" as one of the objectives of the CFSP. The broad notion of security includes threats through international terrorism.[19] As a result, Member States can use the means of Art. 12 TEU for the purposes of counter-terrorism, notably common strategies, joint actions, and common positions.[20] Worth mentioning for overcoming crises caused by terrorism is also the definition of a European security and defence policy (ESDP) in Art. 17 TEU. It enables the EU to establish its own capacities to act militarily. The possible radius of action within the ESDP refer to humanitarian and rescue tasks, peacekeeping tasks, and tasks of combat forces in crises management, including peacekeeping.

In the area of *Justice and Home Affairs* (third pillar), an essential step forward was taken by the Amsterdam Treaty. It integrates the maintenance and development of the Union as an *area of freedom, security, and justice* as a new general objective of the Union in Art. 2 TEU. This new setting is probably the most important goal for integration after the establishment of an internal market and the introduction of an economic and monetary Union. The notion of an area of freedom, security, and justice indicates that the EU provides an area where citizens (including affiliated third country nationals) enjoy free movement while the possibility of free movement does not result in a deficit of internal security. Thus, the area of freedom, security, and justice adumbrates a common – not necessarily unified – zone of internal security where the EU itself may be perceived as an actor for providing security.[21] This deduction is supported by the conclusions of the summit of the heads of state and government, who convened in the framework of the European Council[22] in 1999 in Tampere, Finland and who gave the major impetus for the implementation of the area of freedom security and justice as introduced by the Amsterdam Treaty. The summit takes up terms like "our territory"

[19] Monar (2004), p. 141.

[20] Joint actions and common positions may be adopted in isolation or as a means of implementing a common strategy. A joint action addresses a specific situation where operational action by the EU is deemed necessary, while common positions define the approach of the Union to a particular matter.

[21] Monar (2005b), pp. 29ff.; Jour-Schröder and Wasmeier (2003/2004), mn. 57.

[22] The European Council convenes the Heads of State or Government of the Member States and the President of the Commission. Its role is to provide the EU with political impetus on key issues (cf. Art. 4 TEU).

or "genuine European area of Justice", which lead to the impression that the Union forms a common legal area.[23]

Art. 29 TEU and 61(e) TEC even mandate the EU to provide "a high level of safety/security" within the area of freedom, security, and justice. Art. 29 TEU also mentions terrorism explicitly as one of the crimes that should be prevented and combated in order to achieve the defined objective, and it further defines several possible actions with relevance for the fight against terrorism, including closer police cooperation; further development of the European police office (Europol); better judicial cooperation in criminal matters; involvement of the European Judicial Cooperation Unit (Eurojust) in the judicial cooperation; and adoption of minimum rules relating to the constituent elements of criminal acts and to penalties in the fields of serious crimes, which encompass terrorism (Art. 31(1e) TEU).

Art. 29 and 31 (1e) TEU are the only provisions that - to date - explicitly mention terrorism in the primary legal framework of the EU. Although terrorism remains within intergovernmental cooperation and does not give the EU exclusive competences, the possible actions and instruments of Title VI TEU (third pillar) open intensive cooperation among Member States' law enforcement authorities in the field of combating terrorism.[24] We will shortly see that the bulk of the EU's anti-terrorism actions after the attacks of 9/11 is focused on the field of "police and judicial cooperation in criminal matters" (PJCC).

In comparison with the Maastricht Treaty, the Amsterdam Treaty brought about a further essential change as to the legal instruments on which the Member States can act in the third pillar. Beside common positions[25] and conventions,[26] Art. 34(2b) TEU introduces *framework decisions* as a possible form of action. Framework decisions can be used for the purpose of approximation of the laws and regulations of the Member States. The framers of the Amsterdam Treaty wanted to establish a more binding instrument for the Member States because the success of joint actions and conventions as provided by the Maastricht Treaty were disappointing because of insufficient transposition. The effect of framework decisions is aligned to directives, which are the usually used instrument in the first pillar to harmonise Member

[23] Council Doc. SI (1999) 800. The conclusions can be retrieved at the following website: http://presidency.finland.fi/doc/liite/treconen.rtf (last visited July 2009).

[24] Monar (2004), p. 140.

[25] Art. 34 (2a) TEU. Common positions define the approach of the Union to a particular JHA matter. It is highly disputed whether common positions have only political significance or whether they are legally binding in terms of international public law. They are akin to common positions adopted in the CFSP (Art. 12, 15 TEU), however, it is questionable whether one common position can regulate both CFSP and JHA matters because structure and objectives of the second and third pillar and procedures are different. Nevertheless, the Council based two common positions relating to combating terrorism both on Art. 15 and 34 (Common Positions 2001/930/CFSP and Common Position 2001/931/CFSP, OJ L 344 of 28 December 2001, p. 90/93). This shows again the "cross-pillar" nature of terrorism.

[26] Art. 34(2d)TEU. The main issue is that conventions have only binding effect after their ratifications by the Member States.

States' national laws: Framework decisions shall be binding on the Member States as to the result to be achieved but shall leave to the national authorities the choice of form and methods. Framework decisions contain deadlines that oblige Member States to transpose the provisions into national law. The intergovernmental character of framework decisions is maintained because (1) they have no direct effect;[27] and (2) no judicial enforcement is possible in case of not timely or false implementation by Member States (see above).

Framework decisions became one of the most important legal tools of the EU for actions in the fight against terrorism. They replaced actions through conventions since the entering into force of the Amsterdam Treaty in 1999. Lengthy proceedings of signature and ratification could be avoided, and a proper follow-up mechanism could be established (regular reviews of implementation by Commission, although these non-binding reviews entail more or less the effect of "naming and shaming"). Framework decisions have provided for specific legal regimes, in particular, in respect of the definition of criminal acts, type and level of criminal penalties, and compulsory rules on jurisdiction as well as of defining new approaches in the field of mutual legal assistance between police and judicial authorities.

Moreover, the Amsterdam Treaty newly offers action through *decisions* (Art. 34(2c) TEU).[28] They can be applied for any other purpose consistent with the objectives of Title VI EU Treaty, excluding the approximation of the laws and regulations of the Member States. In comparison with framework decisions, they are fully binding on the Member States (and not only binding as to the result). Direct effect is explicitly excluded. In addition, decisions in the sense of Art. 34 TEU became an important instrument to the EU's reactions to terrorism. They mainly allow the establishment of central capacity building of the EU as far as police and judicial cooperation is concerned.

Additionally, the *communitarised policies (first pillar)* that are designed to realize the objective of economic integration of the European Union provide for legal bases to help stem security threats and to help peace building.

Rules concerning the entry and movement of persons (as provided for in Title IV TEC)[29] are important, in particular, standards and procedures for carrying out checks on persons at the external borders of EU Member States; rules on visas and conditions of entry and residence; and measures on illegal immigration and illegal residence.

Other areas affected in the first pillar are those relating to transport (e.g. air and sea security), the promotion of research and technological development, health protection (e.g. alert system in the event of outbreaks caused by bio-terrorism) and civil protection, financial programmes, and external economic trade.

---

[27] The main consequence is that an individual can not rely on provisions of a framework decision if a Member State fails to transpose it. Nevertheless, the ECJ conferred indirect effects to framework decisions. In the "Pupino judgment" (Case C-105/03), the ECJ ruled that national law must be interpreted in conformity with the provisions of framework decisions.

[28] They must be distinguished from decisions as provided for in the first pillar, Art. 249 TEC.

[29] The Amsterdam Treaty transferred these areas from Title VI TEU to the EC Treaty, but maintains intergovernmental elements for a transitional period. Cf. Art. 67 TEC. Details at Peers (2006), 2.2.2.

4.3.2 The Example of "Cross-Pillarisation": EU Blacklisting and Freezing Assets of Terrorists

As mentioned introductorily, the EU Member States had to dovetail instruments and measures of the European Union that are spread across the pillars in order to achieve a certain aim, regularly a foreign policy aim. The prime example of this "cross-pillarisation" is the EU's approach to cut the sources that fund terrorism. Here, the EU implements relevant UN Resolutions by instruments of the second pillar and Community law (first pillar). Under the code "smart sanctions", the United Nations Security Council established two regimes that allow freezing of funds and other financial assets or economic resources of individuals or private organisations. The first one specifically requires the freezing of funds of Osama bin Laden, the al-Qaeda network and the Taliban,[30] the second imposes a general obligation on States to freeze funds related to persons or entities who commit terrorist acts.[31] The main difference between these two UN regimes is that, for the first one, the UN established its own procedure for listing the individuals or entities whose funds are to be frozen (blacklisting by its own sanctions committee), whereas the second, more general regime, leaves the final destination of appropriate subjects to the resolution's addressees.

Although the European Community is not itself bound by the Security Council Resolution from an international law perspective (Art. 48 (2) UN Charter), the European Council decided on a concerted action with instruments of Community law in order to ensure an uniform application of the UN requirements in the EU territory.[32] To this end, the Council adopted Common Positions in the framework of the CFSP, which provide for the consensus and the basis for a coordinated implementation by Community law.[33] Regarding the freezing of assets, the Common Positions contain two obligations expressively addressed to the European Community: The European Community shall order the freezing of the funds, financial assets, or economic resources of the individuals and entities listed, and it must ensure that these financial means are not made available, directly or indirectly, for the benefit of mentioned subjects.

This is a reference to Art. 301 and 60 TEC, i.e. the first pillar, which contain the exclusive competences of the European Community to implement trade embargoes

[30] Resolution 1390(2002), which adjusts the scope of sanctions concerning the freezing of funds, visa ban, etc. imposed by Resolutions 1267(1999) and 1333(2000).

[31] Resolution 1373(2001).

[32] Meyer (2007), p. 7; Jimeno-Bulnes (2004), p. 246f.

[33] For the first UN regime, this was Common Position 2002/402/CFSP of 27 May 2002 concerning restrictive measures against Usama bin Laden, members of the Al-Qaida organisation, and the Taliban and other individuals, groups, undertakings, and entities associated with them, OJ L 139 of 29 May 2002, p. 4. The EU's legal bases for the second UN regime is Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism, OJ L 344 of 28 December 2001, p. 93.

as well as the possibility to restrict the freedom of capital, if this is foreseen in a common position or joint action in the framework of the CFSP. However, Art. 301, 60 TEC only allow for sanctions against a country or at least state actors, but not for persons or entities in no way linked to the governing regime of a state, which is the case for the UN Resolutions. Thus, the Community had to face the general dilemma of international law after the attacks of 9/11 in that the international legal system is designed on State action whereas terrorism involves non-state, but nevertheless powerful actors.[34] Therefore, the Community legislator made additional recourse to Art. 308 TEC, which grants the power for the Community to act where none yet exists if it is necessary to attain one of the *objectives of the Community* (flexibility clause).

In a recent judgment, the European Court of Justice (ECJ) backed this legal basis for Regulation EC/881/2002, which implements the first UN sanctions regime addressed against the al-Qaeda network and the Taliban. In view of the problematic recourse to Art. 308 TEC in order to justify Community action against individuals or entities, the Court particularly stressed that Art. 60 and 301 TEC already provide for an implicit objective of the Community, namely the adoption of restrictive measures of an economic nature in order to implement actions decided on under the CFSP through the efficient use of a Community instrument.[35] In doing so, the ECJ takes up a commonly used method for argumentation in Community law, namely the principle of *effet utile*, i.e. to give full effectiveness to Art. 60 and 301 TEC in imposing smart sanctions and, therefore enabling the Community to apply any restrictive measures against individuals or entities in the fight against terrorist financing.

This reasoning will also have an impact for the assessment of the competence of the Community to impose its own regime to counter financing of terrorists as established by EC Regulation 2580/2001, which implements the second UN sanctions regime relating to the funds of terrorists in general. Regulation 2580/2001 in conjunction with Common Position 2001/931/CFSP has established an autonomous EU blacklisting procedure. The obligation to freeze the assets of the listed persons therefore applies directly and automatically in all EU Member States.[36] Thus, the European Community itself directly enters into the sphere of the persons concerned. The "EU blacklisting decision" is taken in the Council by unanimous vote and prepared by an autonomous clearinghouse procedure – settled in Council working groups.[37] The Council reviews and updates the list at regular intervals, at least once every 6 months. There are two strands of criteria for listing: On the one hand, persons, groups, and entities identified by the UN Security Council as being related to terrorism and against whom the Security Council has ordered sanctions may be

[34] Vennemann (2003a), p. 242.

[35] ECJ Cases C-402/05 P and C-415/05 P, ("Kadi and Al Barakaat") mn. 226, 227. See also Meyer (2008), p. 81; Karayigit (2006), p. 394.

[36] National authorities are bound by the Regulation and can only issue acts enforcing the provisions of the EC Regulation. Meyer (2007), p. 9.

[37] See Art. 1 (4), (5), (6) Common Position 2001/931/CFSP.

included in the list. On the other hand, the Council takes up decisions taken by a competent EU Member State's authority against the person, group, or entity concerned; such a decision may concern the instigation of investigations or prosecution for terrorist acts, an attempt to carry out or facilitate such an act based on serious and credible evidence or clues, or condemnation for such deeds.

The autonomous "EU blacklist" raises several legal questions. First, it is questionable whether the case law of the ECJ on the legal bases of the Regulation transposing the special UN asset regime against al-Qaeda and the Taliban can transferred 1:1 to Regulation 2580/2001 because the EC implements smart sanctions through means of internal security, for which the EC has no competence.[38] Second, problems arise on how the concerned persons/organisations can undertake legal action against the Council's listing decision and on how fundamental rights as guaranteed by the EU are infringed. In addition, the Union's legislative framework, which implements the freezing of property by the UN sanctions committee, i.e. the UN-determined blacklisting, raises several legal problems, such as how individuals or organisations can seek legal protection before the Community courts. Both sanctions regimes already provided reason for several proceedings before the European Court of Justice by listed subjects.

4.4 The EU's Counter-Terrorism Arsenal

After more than 7 years of action, it is nearly impossible to review all counter-terrorism measures, activities, and instruments hitherto taken by the EU. By addressing the multifaceted nature of the phenomenon "terrorism", the EU has established a remarkable set of measures, rules, strategies, etc. in the post-9/11 phase, which is referred in the following as *acquis anti-terrorisme*.[39] The following sections can therefore only highlight important EU's counter-terrorism measures. They are systematised under various categories that reflect their different nature:

The EU's first reactions to terrorist attacks were, above all, of political nature, particularly solidarity declarations and political dialogues with third countries. Political responses further helped to formulate the EU's more coherent counter-terrorism policy by a strategy and accompanying action plans on which the analysis of the EU's "*political acquis anti-terrorisme*" will focus in the following. The strategy and accompanying action plans read as an inventory of the EU's past and future counter-terrorism activities, particularly its panoply of legal instruments that aim at strengthening law enforcement cooperation between the EU Member States or set

[38] Critical regarding the legal basis for the EU's smart sanction regime also Bartelt and Zeitler (2003), p. 715. Cf. also Hörmann (2007), pp. 120ff.

[39] Knelangen (2008), pp. 118/119; Monar (2004), p. 150 who emphasises that the EU established structures and possibilities to act, however there was no legal acquis on terrorism at the moment of the attacks on 11 September 2001.

minimum standards of counter-terrorism measures among the EU Member States ("*legal acquis anti-terrorisme*"). In addition, right from the beginning, the EU emphasised enhancements of operational interactions between the national law enforcement and criminal justice systems of the Member States. Closely connected with this "*operational acquis anti-terrorisme*" are the European Union's efforts to strengthen capacity building of central bodies at the European Union level ("*institutional acquis anti-terrorisme*"). Lastly, the EU has entered as a collective actor at the international stage by using foreign policy tools to enhance anti-terrorism cooperation with international organisations and third countries ("*external acquis anti-terrorisme*").

Taking a closer look at the EU activities after the attacks of 9/11 until today, there are some guiding lines. Foci of the EU's counter-terrorism policy have shifted and the measures taken are very much event driven. Whereas, in the phase between the attacks in the United States of 9/11 and the attacks of Madrid of 11/3, the terrorism threat was perceived as an attack to a third country that must be assisted by the European Union – especially by closer police and judicial cooperation – the phase after Madrid is very much influenced by the impression of terrorism against the EU's area of freedom, security, and justice, and by "home grown" terrorism. Therefore, in the post-11/3 phase, EU efforts increased to protect the EU's critical infrastructure and to counter radicalisation and recruitment of terrorism.

4.4.1 The Political Acquis Anti-terrorisme, in Particular, the EU's Counter-Terrorism Strategy and Action Plan

The fact that EU action in the field of anti-terrorism goes across all pillars and affects nearly all policies for which the European Union is empowered becomes obvious if one looks at the European Union's Counter-Terrorism Strategy and the European Union's Plan of Action on Combating Terrorism. The first Action Plan dates from 21 September 2001, thus immediately after the terrorist attacks of 9/11.[40] It was further amended several times and now encompasses approximately 200 concrete measures/actions.[41] The Action Plan specifies the concrete measures and responsible actors (Member States, Council, Commission, other bodies at the EU level) as well as deadlines for achieving the various steps needed for the defined objective. It further provides for the status of implementation.[42]

The EU's counter-terrorism strategy was officially adopted by the Justice and Home Affairs Council in December 2005.[42] It can be considered the overall concept of a "comprehensive and proportionate" response of the European Union to the

[40] Council Doc. SN 140/01.

[41] Council Doc. 7233/1/07 REV 1.

[42] Council Doc. 14469/4/05 REV 4.

international terrorist threat. The strategy regroups the agenda of work that was constituted by the EU Action Plan under the following four main headings; they constitute the four pillars or "strands of work" of the EU's counter-terrorism policy:

- "*Prevention*" means to prevent people from turning to terrorism and to stop the next generation of terrorists from emerging. The single issues focus on combating radicalisation and recruitment of terrorists by identifying the methods, propaganda, and instruments they use.
- "*Protection*" refers to the protection of citizens and infrastructure and the reduction of the vulnerability of targets to attack. In this field, the EU mainly takes action to improve border security, transport, and critical infrastructure.
- "*Prosecution*" unifies a series of aims: The prosecution and investigation of terrorists across the borders and globally; the impediment of planning, travel, and communications; the disruption of support networks, and the cutting off funding and access to attack materials; and eventually – as a more general aim - bringing terrorists to justice. The mass of EU actions to date have been taken in this pillar.
- The objective of "*response*" takes into account the management and minimisation of the consequences after a terrorist attack by improving capabilities to deal with the aftermath, the coordination of the response, and the needs of victims.

The evolution of the EU counter-terrorism strategy took longer than 4 years calculated from September 2001. However, the main elements and trends were already contained in the first policy reactions after the attacks of 9/11,[43] and further in the declarations in the aftermath of the attacks of Madrid on 11 March 2004 and London on 7 July 2005, which very much influenced the strategy.[44] By emphasising EU action in the area of justice and home affairs, borders security, and terrorist financing as well as external action of the EU in cooperation with the UN, key partner countries including the USA, and priority third countries, the strategy, on the one hand, fills old wine into new bottles and does not invent a new approach.[45] On the other hand, the formulation of a common counter-terrorism policy of all 27 EU Member States is rather unique at the international stage and must be considered one of the EU's major achievements.[46] It is also interesting that the EU attempts to define its own internal security policy by clarifying that contemporary terrorism threat is no longer a domestic criminal issue of the nation state.[47] In this

[43] Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, Council Doc. SN 140/01, which headed measures to be taken under the following five objectives: (1) Enhancing police and judicial cooperation; (2) Developing international legal instruments; (3) Putting and end to the funding of terrorism; (4) Strengthening air security; and (5) Coordinating the European Union's global action.

[44]The Declaration of the European Council of 25 March 2004 (Council Doc. 7906/04) identifies seven objectives to combat terrorism, which build the fundaments of the strategy of 2005.

[45]Knelangen (2008), p. 118; Bossong (2008b), p. 8

[46]Monar (2007), p. 312.

[47]Cf. Zimmermann (2006), pp. 125, 127.

regard, the strategy talks, for instance, about "*our* vulnerability", the need for Member States to "focus on the security of the Union *as a whole*", and the *ability of the EU* to take *concerted and collective action* to an effective and efficient response".[48] Thus, it is endorsed that the EU itself must be defended and as such must be capable to act against terrorism.

Communications from the *Commission* to the Council and/or other institutions are a further important instrument on the political track. Communications contain non-binding recommendations or opinions and mainly reflect a certain topic. They normally give a crucial impetus to political discussions. Frequently, reflections in communications end in concrete legislative proposals of the Commission or communicate concrete action of the Commission. Important communications in the field of combating terrorism were:

- Communication from the Commission to the European Parliament and the Council – Stepping up the fight against terrorism,[49] which sets the scene for EU action in the field of counter-terrorism and analysis of the added value of the EU in the different areas in which the EU should plan to take further action, such as violent radicalisation, critical infrastructure protection, urban transport security, exchange of information, etc.
- Communication from the Commission to the European Parliament and the Council on enhancing the security of explosives.[50] This communication takes up the above-mentioned "increasing openness" of the European Union's area and reacts to the fact that the Madrid bombings as well as the foiled attacks in London and Glasgow in 2007 and Germany in 2006 were carried out by using commercially available explosives. The Communication contains an action plan that aims at combating the use of explosive devices by terrorists within the EU.
- The Communication from the Commission to the European Parliament and the Council concerning terrorist recruitment[51] forms the basis for the European Union's "Strategy for Combating Radicalisation and Recruitment", which was adopted by the Council in December 2005.[52]
- In 2004, the Commission launched a package of four communications regarding new measures for fighting terrorism. These Communications mainly respond to the attacks of Madrid and put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks respectively on terrorist financing, on prevention, and consequence management, and finally on critical infrastructure protection.[53]

---

[48] Council Doc. 14469/4/05 REV 4, p. 3, no. 23, no. 33. Emphasis added by author.

[49] COM(2007) 649.

[50] COM(2007) 651.

[51] COM(2005) 315.

[52] Council Doc. 14781/1/05 REV 1. Elaborately on the EU's response to radicalisation and recruitment Dittrich (2007), pp. 54 ff.

[53] COM(2004) 698; COM(2004) 700; COM(2004) 701; COM(2004) 702.

4.4.2 The Legal Acquis Anti-terrorisme

4.4.2.1 Harmonisation of Substantive Criminal Law

One focus within the adoption of legal anti-terrorism instruments are actions of the EU Member States regarding the *harmonisation of their substantive criminal law* based on Art. 29 and 31(1e) TEU.[53a] For a detailed analysis of the harmonisation of criminal law in the European Union, see Sieber (2008), p. 385ff.
Rather quickly after the attacks of 9/11, the Justice and Home Affairs Ministers of the EU Member States agreed on the *Framework Decision on Combating Terrorism*.[54] Agreement was reached in December 2001, and the Framework Decision (FD) could be adopted on 13 June 2002. The Member States were given a rather short period for the implementation of the obligations contained in the FD in comparison with other FDs: Implementation had to be effected by 31 December 2002, thus only a bit longer than a half year instead of the usual 2 years. The FD obliges all EU Member States to establish minimum rules relating to the constituent elements of criminal acts and to penalties and sanctions for terrorist offences. According to the Council, the terrorist offence is constituted by three elements (Art. 1(1)):[55] First, the definition contains an objective element referring to – mainly ordinary - offences (as defined in national law), such as attacks on a person's life that may cause death; attacks on the physical integrity of a person; kidnapping; seizure of aircraft; or the manufacture, possession, acquisition, etc. of weapons or explosives (Art. 1 (1 a-i). The second objective element is the context of the acts referred to, i.e. given their nature or context, they may seriously damage a country or an international organisation. Third, the acts become terrorist offences by a subjective element and a special motivation: the acts referred to must be committed intentionally and with the aim of (1) seriously intimidating a population, or (2) unduly compelling a Government or international organisation to perform or abstain from performing any act, or (3) seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation.

After having defined the term of "terrorist group", Art. 2 of the FD obliges Member States to punish the acts of (1) directing a terrorist group and (2) participating in the activities of a terrorist group including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group. As a subjective element, these acts must be committed intentionally.

A further obligation for the Member States is that the acts of aggravated theft or extortion connected to any of the terrorist offences listed in Art. 1(1), or drawing up false administrative documents with a view to committing a terrorist offence or participate in a terrorist group, must be provided for as terrorist-linked offences in the

---

[53a] For a detailed analysis of the harmonisation of criminal law in the European Union, see Sieber (2008), p. 385ff.

[54] OJ L 164 of 22 June 2002, p. 3.

[55] Peers (2003), p. 228; Vennemann (2003a), p. 235f.

Member States (Art. 3). According to Art. 4, Member States must also criminalise the inchoate offences of inciting, aiding, or abetting any terrorist offence, linked offence or terrorist group offence, and they must criminalise attempts to commit any terrorist offence or linked offence, except for attempts to possess nuclear, biological, or chemical weapons or attempts to threaten to commit terrorist offences.

Detailed penalties are largely left to the discretion of the Member States. Art. 5 sets out the commonly used formula that the offences referred to in Art. 1–4 must be punishable by effective, proportionate, and dissuasive *criminal* penalties, which may entail extradition. Terrorist offences as referred to in Art. 1 and related inchoate offences (Art. 4) are to be punished by heavier sentences than common criminal offences in all the EU Member States. The Council FD goes much beyond what has proposed by the Commission since it only defines specific penalties for two offences: a minimum maximum custodial sentence of 15 years for directing a terrorist group,[56] and 8 years for participating in the activities of a terrorist group (Art. 5(2)). Art. 6 allows Member States to reduce the penalty if the person concerned renounces terrorism and provides the authorities with evidence to prevent offences or to catch other offenders.[57]

The FD on Combating Terrorism is one of the core pieces of the EU's anti-terrorism legislation. It does not only take the effect of harmonising the national criminal law of all EU Member States, but has also a "cross-sector" character. Actually, the main *raison d'être* for the FD was to develop novel measures for enhancing police and judicial cooperation in criminal matters based on the common definition.[58] The FD can be regarded as the reference system for subsequent EU counter-terrorism actions.

The main value of the FD was that terrorism is recognised as a special offence in all EU Member States. This is especially important because only 6 out of the then 15 EU Member States had particular rules on terrorist acts prior to the FD[59] and the rules of the Member States, which had special legislation, each reflected their own approaches to tackle "domestic" terrorism as occurred in the 1970s and 1980s. Because the new EU Member States that joined the Union in 2004 and 2007 had to implement the FD on Combating Terrorism into their national legislation prior to their accession, a comprehensive criminalisation and prosecution of terrorist offences throughout the EU is ensured. The FD has also contributed to an enhanced cooperation between the EU and the USA because both sides had a common basis for dealing with a crime legally recognised as a special offence.[60] The FD on

[56] Reduced to 8 years if the group has only threatened to commit such terrorist offences (Art. 5(2) sentence 2).

[57] Other provisions of the FD compel Member States to foresee the liability of and penalties for legal persons (Art. 7, 8), and to take jurisdiction (Art. 9). As regards liability of and penalties for legal persons, the FD follows a common pattern of other FDs, which harmonise substantive criminal law. In contrast, the rules on jurisdiction are rather extensive compared with other FDs (see Peers (2003), p. 233). Art. 10 relates to the protection of, and assistance to, victims.

[58] Vennemann (2003a), p. 234; Symeonidou-Kastanidou (2004), p. 17.

[59] COM(2001) 521, p. 7.

[60] Bures (2006), p. 67.

Combating Terrorism has insofar a rather *symbolic character* because it demonstrates the EU's will to fight terrorism also at a global level. It is likewise a reaction to the experience that criminal acts that led to the attacks in the USA were conducted on EU territory (such as the cells in Germany), thus the FD also applies to conduct that can contribute to acts of terrorism in third countries.

The main weakness of the FD is that an approximately similar level of punishment could legally not be reached because of the openness of the provisions on "minimum maximum" penalties leaving Member States a too wide margin of discretion for implementation. It is further questionable whether the FD should not have provided for clearer rules in order to avoid frictions in the setting of penalties and sanctions in Member States' legislation.[61] In this context, the first question is whether the individual Member State maintained a balance between the sanctioning of the "ordinary" offences as described in Art. 1(1 a–i), on the one hand, and the "terrorist offences" as defined by the FD, on the other hand, considering that the special motivation and the danger inherent to acts committed with such a motivation are the only reasons for the aggravation of the sentence. The second question is whether Member States did not "over-sanction" the terrorist-linked acts (Art. 3) because these acts are often committed at the very beginning of the preparations for terrorist acts and at a stage at which the interests protected by the penalisation of terrorist acts are not yet at risk.[62]

Due to the usage of vague terms and the broadening of the definition by the subjective elements, particularly NGOs feared the inclusion of urban violence and anti-globalisation demonstrations under the definition of the "terrorist offences".[63] The Council countered these arguments, by introducing recital 10 and Art. 1 (2) of the FD, which refer to the protection of fundamental rights within the EU. Recital 10 states that nothing in the FD may be interpreted as being intended to reduce or restrict fundamental rights or freedoms, such as, inter alia, the freedoms of assembly, of association, or of expression. One can rely on this guideline and follow a restrictive interpretation of the terrorism definition excluding urban violence or anti-globalisation demonstrations from the scope.[64]

New discussions regarding fundamental rights and freedoms will be sparked by the latest *amendment to the Framework Decisions on Combating Terrorism*. Following the latest EU focus on reinforcing the fight against radicalisation and recruitment of terrorists, the Council identified that action must be taken against the use of the Internet and other modern information and communication technologies for the propagation of the terrorist threat. Based on a proposal of the Commission of 2007, the Council agreed in late 2008 that, in the future, the terrorist-linked

[61] See for this problem in general Pastor-Nunoz (2008), p. 73.

[62] Vennemann (2003a), pp. 256–258.

[63] Bunyan (2002); Bures (2006), p. 67 with reference to the report by the EU Network of Independent Experts in Fundamental Rights.

[64] Vennemann (2003a), pp. 236f. Recital 11 explicitly excludes freedom fighters and state terrorism from the ambit of the FD.

offences of Art. 3 will also encompass the public provocation of terrorism, recruitment for terrorism, and training for terrorism.[65] Again, the public and particularly the European Parliament raised concerns that the three new acts could contradict fundamental freedoms, such as the freedom of speech and freedom of association.[66] The Council reacted by stipulating in Art. 2 of the FD that it shall not have the effect of requiring Member States to take measures in contradiction to fundamental principles relating to freedom of expression. However, it is doubtful whether Art. 2 is a suitable restriction of too broadly formulated criminal acts and whether the national legislator is required to recur to other forms of restriction in the course of implementation.[67]

Further problematic is that the definitions of the new acts extend penalization of behaviours that are far from a concrete terrorist threat. Because the FD does not contain concrete prerequisites for penalties of the new terrorist-linked offences of propagandism, it is again up to the national legislator to find the right balance between sanctioning of offences in the far run-up of a concrete threat and the actual terrorist offences as defined in Art. 1 of the FD. Nevertheless, the FD makes the EU a forerunner in the implementation of the substantive law provisions of the 2005 CoE Convention on the Prevention of Terrorism, which are taken up in the FD.[68]

Similar motivations lay behind the *Council Framework Decision on attacks against information systems* of 2005.[69] The FD takes up the elements of the 2001 Council of Europe Convention on Cybercrime that are related to the threats to computer infrastructures, which concern operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer and networks themselves. The approach followed by the European Union is therefore the approximation of substantive criminal law regarding the illegal access to information systems, illegal system interference, and illegal data interference.[70] Member States are obliged to punish these acts by effective, proportional, and dissuasive criminal penalties. As the FD on Combating Terrorism, the FD on attacks against information systems has a cross-sector effect, i.e. its objective is to leave behind barriers for an effective police and judicial co-operation in the area of attacks against information systems. Although the CoE Convention on Cybercrime did not make any reference to threats caused by terrorism,[71] the Council and the Commission stood under the impression of the attacks of 9/11 and declared that the EU instrument

[65] Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, OJ L 330 of 9 December 2008, p.21. The acts are defined in the new Art. 3 (1) of the FD.

[66] EP, legislative resolution of 23 September 2008, T6-0435/2008.

[67] Zimmermann (2009), p. 6. For the problems regarding the implementation of the new FD into the German legal order, see Sieber (2009).

[68] Art. 5, 6, and 7 of the Convention, ETS No. 196.

[69] OJ L 69 of 16 March 2005, p. 67.

[70] Art. 2, 3, 4 of the FD. Cf. also Art. 2, 4, and 5 of the CoE Cybercrime-Convention (ETS No. 185).

[71] For the use of the Cybercrime-Convention against terrorist attacks to the Internet, see Sieber (2006), pp. 395ff.

is simultaneously an appropriate tool to protect critical infrastructure of vital information systems against possible terrorist attacks.[72] The FD, which was proposed in April 2002, can therefore be regarded a direct consequence of the attacks of 9/11, although it was on the agenda a long time before and approximates the domestic criminal law in the area of cybercrime in general. Again, the EU took the "criminal law approach" for guaranteeing security, this time of computer networks.[73]

4.4.2.2 Judicial Cooperation in Criminal Matters

A second main field of EU action post-9/11 has been legislation to facilitate cooperation of judicial authorities in criminal matters. Here, the *Framework Decision on the European Arrest Warrant* (FDEAW) is widely recognized as the second core piece of the Union's efforts to react to terrorism.[74] Together with the abovementioned FD on Combating Terrorism, the FDEAW was agreed on already in December 2001 and formally adopted in June 2002. The aim of this instrument is to facilitate extradition between EU Member States by replacing existing instruments, namely extradition conventions, that had turned out during the centuries to be lengthy, cumbersome, and unpredictable.[75] The new mechanism is based on the *principle of mutual recognition* of judicial decisions in criminal matters across the EU. It means that once a decision has been made by a judicial authority of one EU Member State, this decision shall be recognised and executed in other EU Member States as quickly as possible, and with as little control as possible, as if it was a national decision.[76] The European Arrest Warrant (EAW) aims at achieving the implementation of the mutual recognition principle mainly by the following means:

– Replacement of the two-step procedure of extradition and surrender, which involves not only judicial authorities but also a political decision of the ministries, by a single system of surrender where decisions on the surrender of sentenced or suspected persons are only taken by judicial authorities.
– Acceleration of the procedure by setting rather tight time limits for taking a surrender decision by the executing state[77] and for the transfer of the arrested persons.[78]

---

[72] Recitals 2 and 8 of the FD. See also COM(2002) 173.

[73] Gercke (2005), p. 468.

[74] Council FD 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18 June 2002, p.1.

[75] Wilkinson (2005).

[76] For a definition of the mutual recognition principle, see COM(2000) 495; Vernimmen and Surano (2008), p. 23.

[77] In principle, the final decision on the execution of the EAW should be taken within a period of 60 days after the arrest of the requested person. If the requested person consents to his surrender, the final decision on the execution should be taken within 10 days (Art. 17 FDEAW).

[78] Art. 23 FDEAW stipulates that the transfer shall be effectuated no later than 10 days after the final decision on execution of the EAW.

– Removal of a number of well-established grounds for refusal of traditional extradition law, in particular, the ban not to extradite own nationals, as well as the possibility of verifying whether the act in question is also punishable under the law of the requested State (principle of double criminality).

The latter is abolished if the act in question falls under a catalogue of 32 listed (serious) offences, including participation in a criminal organisation and terrorism as single offences as well as other offences that may be linked to terrorism, such as laundering of the proceeds of crime, "computer-related crime", murder, racketeering and extortion, unlawful seizure of aircraft/ships, and "sabotage". A condition is that the offence must be punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least 3 years and as they are defined by the law of the issuing Member States.[79]

The wide abundance of double criminality checks is the initial point for fierce criticism on the EAW in the literature. It is above all argued that the unclear definition of offences in the list does contradict the principle of legal certainty in criminal matters,[80] a matter that seemingly becomes very obvious as to the offence of "terrorism".[81] Ultimately, authors criticise that the European Arrest Warrant no longer observes human rights concerns because it paves the way also for extradition of warrants that have been issued for the purposes of prosecuting or punishing a person on the grounds of his or her sex, race, religion, ethnic origin, nationality, language, political opinions, or sexual orientation or that the person's position may be prejudiced for any of these reasons.[82]

The European Arrest Warrant is arguably the most prominent example for various strands, which became typical for the EU's anti-terrorism legislation in the aftermath of the attacks on 9/11. Although the EAW was enacted under the label of "combating terrorism", it is a general instrument for enhanced judicial cooperation in the EU. Indeed, the EAW was officially tabled to be a necessary complement of the above-mentioned FD on Combating Terrorism. Both instruments were designed to avoid the existence of safe havens for terrorists in one of the EU Member States: While the FD on terrorism aims at hindering terrorists to take advantage of differences in legal treatment between States, the FD EAW has the effect to enable a state

[79] Art. 2 (2) FDEAW.

[80] This argument was, among others, put forward by the Belgian association "*Advocaten voor de Wereld*" before the European Court of Justice (Case C-303/05). However, the ECJ rejected the objections of the association by arguing that the FD does not seek to harmonise the criminal offences in question and that it is therefore up to each Member State to define the offences and penalties applicable for a non-verification of double criminality.

[81] Plachta (2003), p. 185.

[82] Cf. Vennemann (2003b), p. 114, who puts forward true counter-arguments. Mainly, the FD itself contains a human rights clause to which the Member States are bound in case of execution of warrants. Most EU Member States maintain this limitation as a "European ordre public clause", which excludes the recognition of requests in the cases described by the critics.

to swiftly fetch the suspected terrorist from the society where he is most likely to be reintegrated.[83] However, the EAW is not a counter-terrorism-specific measure, but is designed for more general purposes and purposes much beyond terrorism.[84] The FDEAW is the Union's mutual extradition treaty. It applies to judicial cooperation against all forms of crimes, and, in fact today, it is also used for the surrender of persons for minor or medium criminality.[85] The EAW clearly demonstrates that the EU Member States seek to combat terrorism with the general tools of criminal law without inventing a special "counter-terrorism legislation". Here, the Member States also follow their approach as already taken in the phase prior to 9/11.

Furthermore, the EAW points out that most EU measures that were taken in the post-9/11 phase are a follow-up of the Tampere conclusions (see above) whose implementation had been awaited. Both the FD on Combating Terrorism and the FDEAW were already in the drawers of the Commission, which enabled the Commission to present the two legislative proposals already on 19 September 2001, i.e. 10 days after the attacks.[86] However, whereas beforehand the measures had failed because of resistance of some of the then 15 Member States, the attacks of 9/11 brought the "window of opportunity"[87] to rubber stamp essential measures that were already requested 2 years earlier at the Tampere summit.[88] The attacks triggered a legislation process of urgency that was nearly incomparable and was not reiterated afterwards, not even after the attacks of Madrid in 2004.

In conclusion, legislation in the post-9/11 phase has the following features:

- Terrorism is embedded into the EU's general programme on judicial cooperation and policing. In the following, terrorism even became an essential point in the general policy programmes of the EU on justice and home affairs.[89]
- General criminal law means are the preferred EU action to cooperate against the threat of terrorism.
- 9/11 provided a "catalyst effect" for a rapid enhancement of police and judicial cooperation between the Member States against all forms of cross-border crime, including terrorism.[90]

[83] Commission press release IP/01/1284 of 19 September 2001.

[84] Zimmermann (2006), p. 131.

[85] Wahl (2009).

[86] Vennemann (2003a), p. 231; Glaeßner and Lorenz (2005), p. 32.

[87] Den Boer and Monar (2002), p. 21.

[88] Den Boer (2003b), p. 5; Messelken (2003), p. 14.

[89] The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, OJ C 53 of 3 March 2005, p. 1 – the successor of the Tampere Programme of 1999.

[90] Spence (2007a), p. 2; Muguruza (2001), p. 234.

4.4.2.3 Financing of Terrorism

One focus of the EU's efforts to prevent terrorism as defined in the counter-terrorism strategy is to hinder access of terrorists to financial resources. As mentioned above, combating the financing of terrorism is considered a task affecting all three pillars. Beyond the explained EU regime to freeze funds and other assets of suspected terrorist or terrorist organisations, which derives from a combination of the second and first pillar, the EU adopted other legislative instruments.[91]

In the *third pillar*, the EU undertook particular measures that provide Member States with common standards for the confiscation of proceeds and instrumentalities of crime. The *Framework Decision on Confiscation of Crime-Related Proceeds, Instrumentalities and Property* of 2005 aims to ensure that all Member States have effective rules governing the confiscation of proceeds from crime, inter alia, in relation to the onus of proof regarding the source of assets held by a person convicted of an offence related to organised crime.[92] The FD extends for the first time the powers of confiscation to terrorist financing, i.e. the Member States are obliged to confiscate property of persons who were convicted of an offence covered by the above-mentioned FD on Combating Terrorism.[93] This FD on Confiscation is supplemented by two measures that shall enhance judicial cooperation for confiscation.[94] Both take up the principle of mutual recognition of judicial decisions (see Sect. 4.4.2.2).

In the *first pillar*, the EU put much effort into the tracking of monetary transfers across borders. Terrorist financing is linked with tools that outlaw the financial gains of organised crime. Right after 9/11, the Commission emphasised that the control and penalisation *of money laundering* is one of the cornerstones for curbing the financing of terrorism.[95] The measures of the European Community to combat money laundering and financing of terrorism are very much influenced by international standards, in particular by the 40 (+ 9) Recommendations of the Financial Action Task Force (FATF).[96] In 2005, the Council and the European Parliament

[91] Cf. also Communication from the Commission to the Council and the European Parliament on the Prevention of and the Fight against Terrorist Financing, COM(2004) 700, Annex 2 and Annex 3; Counter-Terrorism Coordinator, Revised Strategy on Terrorist Financing, Council Doc. 11778/08 of 11 July 2008.

[92] OJ L 68 of 15 March 2005, p. 49.

[93] Kilchling (2006), p. 89.

[94] FD on the execution in the EU of orders freezing property or evidence OJ L 196 of 2 August 2003, p. 45. FD on the application of the principle of mutual recognition to confiscation orders, OJ L 328 of 24 November 2006, p. 59.

[95] COM(2001) 611. See also associated measures: Regulation "on controls of cash entering or leaving the Community", which harmonises rules for the control of cash flow at the EU's external borders (OJ L 309 of 25 November 2005, p. 9), and Regulation laying down rules on information on the payer accompanying transfers of funds (OJ L 345 of 8 December 2006).

[96] Mitsilegas and Gilmore (2007), p. 119.

agreed, after a rather smooth decision-making process, on *Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*.[97] The Directive appeals the previous first anti-money laundering (AML) directive of 1991 as amended by the second one of 2001. The 2005 Directive (3rd AML Directive) is at present the reference system of anti-money laundering standards throughout the EU. The EC AML scheme contains both a repressive approach, i.e. the combating of money laundering by penal means, and a preventive approach. The preventive approach is mainly achieved by obliging Member States' financial sectors to identify their customers, keep records, establish internal control procedures, and report any indication of money laundering to the competent authorities. Despite their criminal law and its primary objective to combat crime, the Directives are based on Community law, i.e. to ensure the integrity of the Community financial system and the internal market.[98]

A comparison between the three AML directives shows that the scope and obligations have considerably extended, a principal reason of which was the threat of terrorism. In general, the EC legislation has involved persons and institutions of the private sector in the net of information in a much earlier stage, has extended the ban to execute business in case of suspicion, and has let obligations for supervision become a continuous activity.[99] However, it must be borne in mind that these intensifications owe much to international obligations as set by the FATF.

As to the criminal law-related aspects, the 3rd AML Directive obliges Member States first to prohibit money laundering. The definition of money laundering is aligned to the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. However, the range of predicate criminal offences that shall be covered by the Directive has extended to the proceeds of serious offences since the 2nd AML Directive and not only drugs trafficking. The 3rd AML Directive further clarifies the legal term "serious offences", which now includes all offences with a certain threshold.[100] Second, the 3rd AML Directive explicitly obliges Member States to prohibit terrorist financing, although the Member States agreed that the concept of serious offences should cover all offences relating to the

[97] OJ L 309 of 25 November 2005, p. 15.

[98] Art. 47 (2), 95 TEC. Because of the criminal law implications of the AML Directives acting upon the basis of the first pillar is highly disputed and it is argued that they should have been enacted via the third pillar (Art. 29 ff TEU). Cf. Mitsilegas and Gilmore (2007), p. 136; Hecker (2007) § 8 mn. 9ff.

[99] Sommer (2005), p. 50.

[100] Art. 3 (5 f) of the Directive: "all offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months".

financing of terrorism. However, the definition of terrorist financing now also encompasses lawful property being diverted to finance terrorism.[101]

On the preventive side, the new AML Directive considerably extended the level of detail as regards customer identification and verification in accordance with the FATF recommendations (more "know your customer" requirements). The Directive further follows a risk-based approach and distinguishes between situations where a higher risk of money laundering may justify enhanced measures and situations where a reduced risk may justify less rigorous controls. Accordingly, the addressees have to meet different levels of due diligence. In general, customer due diligence must be applied, for instance, already where there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption, or threshold. Under certain circumstances, institutions and persons covered by the Directive may apply simplified customer due diligence. In contrast, certain situations are expected to entail a higher risk of money laundering and terrorist financing, therefore a more profound identification and verification of the identity of customers is required. Enhanced due diligence measures apply for instance in the case of transactions with "politically exposed persons" (PEPs) – a very controversially discussed extension because of the vagueness of the notion[102], practical problems in identifying such PEPs, and doubts regarding an unjustified encroachment into fundamental rights such as privacy and data protection.

The AML Directives have also expanded the *ratione personae* scope: Whereas the 1991 AML Directive introduced the duties for credit and financial institutions, the 2001 Directive applies to other non-financial activities and professions, such as accountants, estate agents, dealers in high-value goods, and casinos, and the 2005 Directive now also covers life insurance intermediaries and trust and company service providers and applies to all persons trading in goods for payments of 15,000 euros or more. The 2005 AML Directive further perpetuates the extension of the duties prescribed to notaries and legal professions, which was included in 2001 after fierce debates between the Council and the European Parliament. The European Parliament was concerned about an encroachment into the rights to a fair trial and the principle of lawyer-client confidentiality. The controversy ended up in a compromise that exempts the professions from the obligations of information of and cooperation with the authorities in the case of legal advice.[103] However, the protection of legal professionals is further watered down because they are not exempt from the described

[101] Art. 1 (4): "terrorist financing means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Art. 1–4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism".

[102] Cf. Art. 3 (8) "natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons". Hetzer (2008), p. 469 notes that the legislator mainly envisaged foreign higher ranking politicians, officials, and officers in countries where corruption is prevalent.

[103] Details in Recital 20 and Art. 23 of the 3rd AML Directive.

extension of identification and reporting duties that apply to them and credit/financial institutions alike.[104] In addition, it must be noted that it is up to the discretion of the Member States to stipulate the legal advice exemption.

The main question is whether the device of money laundering that was initially designed for combating the financial gains of organised criminal groups can be transferred to terrorist financing. This can be disputed with good arguments.[105] First, the phenomena of organised crime and terrorist financing are different. Terrorism is not geared towards generating profits, which is the *raison d'être* of organised crime. As a result, curbing the financial resources of terrorists cannot remove the original danger, namely the commission of further attacks. Second, financial transactions to support the modern forms of terrorist activities are often legal, unlike actions of domestic terrorist in the 1970s and 1980s. It is therefore "clean money", whereas "traditional" organised crime focuses on the proceeds of crime, i.e. "dirty money". Thus, it is difficult to prove beforehand a link between the financial transaction and a concrete "terrorist offence". Third, in practice, anti-money-laundering measures against organised crime turned out to be difficult and cumbersome, e.g. due to the allocation of suspicious assets to concrete persons.

4.4.2.4 Data Retention

Right after the attacks of 9/11, the Council highlighted the importance of communications data in the fight against crime and terrorism.[106] However, it was not until the terrorist bombings in Madrid in 2004, when the access to telephone communications data by law enforcement proved indeed successful to catch alleged wire-pullers, that the EU Member States took intensified legal action. Action was pushed by the European Council, which then strongly urged the adoption of an instrument that harmonised the rules on retention of communications data for investigation purposes. The initial envisaged date, for adoption by June 2005, could not be met because of a row between the Council, on the one hand, and the European Parliament and the Commission, on the other hand, regarding the correct legal basis. Thereupon, in September 2005, the Council arranged a deal with the EP to give up a draft framework decision of 2004 and to pursue first pillar legislation, giving the EP stronger rights to amend the proposal under the co-decision procedure. In December 2005, both agreed on the Directive 2006/24/EC "on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC".[107]

---

[104] Mitsilegas and Gilmore (2007), p. 128.

[105] Kilchling (2004), p. 203; Kilchling (2001), p. 17.

[106] Council Doc. SN 3962/6/01.

[107] OJ L 105 of 13 April 2006, p. 54. The approach to consider the Directive as a matter of market regulation of the first pillar was recently backed by the European Court of Justice (judgment of 10 February 2009, Case C-301/06, Ireland v. Parliament and Council).

The data retention regime build up by the EU is based on the principle that retained data must be made available to law enforcement authorities for a certain period, but are not, in principle, accessed by anybody. It is only for a limited part of these data, and on a case-by-case basis, that law enforcement authorities may decide to look into this information. Another principle is that the scope of the regime does not deal with the interception of content of communications, i.e. it is not intended to cover what is actually said or written in a communication.[108] Accordingly, Member States must adopt measures that oblige providers of publicly available electronic communications services or of public communications networks to store traffic and location data,[109] in order to ensure that these data are available, on request, for law enforcement agencies. Data retention shall be carried out for the purpose of the investigation, detection, and prosecution of serious crime (not only terrorism and organised crime, as initially envisaged). It is up to the national law of each Member State to define what it understands under the term "serious crime".

The Directive applies to all forms of electronic communication, such as fixed and mobile phones, faxes, SMS, MMS, e-mails, surfing the internet, internet telephony, etc. The Directive also prescribes in detail the categories and types of data that must be retained.[110] The retention period is left up to the Member States within the following margin: The period shall be not less than 6 months and not more than 2 years.[111] However, Art. 12 of the Directive allows a Member State facing particular circumstances to extend for a limited period the maximum retention period. The reader does not learn from the Community legislator what "particular circumstances" means and how long the extension period may be.

From the outset, the mandatory European data retention framework for law enforcement purposes sparked fierce criticism by parliamentarians, data protection commissioners, civil rights organisations, the press, and last but not least the telecommunications and Internet service providers themselves. They put forward the arguments of disproportionality of the measure, and incompatibility of the storage of traffic data of all users without any concrete suspicions with fundamental rights. European NGOs concluded that the data retention directive infringes (1) the rights of the citizens under Art. 8 (the right to respect for private life and correspondence) and Art. 10 (freedom of expression) of the European Convention on Human Rights

[108] Instructive: Recitals 9, 13, 25 of Directive 2006/24/EC.

[109] Data that identifies the caller and the means of communication, e.g. subscriber details, billing data, email logs, personal details of customers, and records showing the location where mobile phone calls were made.

[110] Art. 5 of the Directive 2006/24/EC. For example, in the case of mobile phones, this includes: (1) calling phone number and numbers dialled, (2) name and address of the subscriber or registered user, (3) date and time of the start and end of the communication, (4) telephone service used, (5) data identifying the user's communication equipment, such as IMSI and IMEI, and (6) data identifying the geographic location (Cell IDs).

[111] Art. 6.

(ECHR) as well as (2) the rights of telecommunication companies under Art. 1 of the first protocol to the ECHR (protection of property).[112] The telecommunications industry rejects the regime for being disproportional in view of the technical and financial burdens of mandatory data retention in the envisaged amplitude.[113] Last but not least, the effectiveness of the measure is very much doubted because traffic data only have had a minor importance for prosecutions of crimes in practice; criminals can very simply bypass the storage of the envisaged data. As an example, successful queries in investigations only refer to data that are stored within the last 3 months, and searches in the data pool, using existing technology, would take 50–100 years.[114] The controversial discussion on the data retention Directive is further nourished by the fact that the Community legislator leaves open a series of important questions to the Member States, such as the exact retention period and the scope of crimes for which investigation data should be retained, so that the aim of the Directive to achieve a harmonisation of the Member States' laws is difficult to be reached.

Notwithstanding, EU governments tough it out that data retention is an "essential investigative tool" for investigators to follow communication "footprints" or perpetrators either in order to place them at the scene of the crime or to identify all associates and co-conspirators.[115] In doing so, the EU perpetrates trends of law enforcement in the fight against terrorism: First, law enforcement shall get principal access to data processed or used by privates through modern telecommunications technologies. Second, privates get increasingly involved in the fight against terrorism and crime. Third, an instrument actually conceived in connection with terrorism is expanded to be an investigative tool for all forms of (serious) crimes (spill-over effect of terrorism).

4.4.2.5 Illegal Migration and Border Controls

The events of 9/11 led also to a shift in the EU's policy in the field of visas, asylum, immigration, and other policies related to free movement of persons.[116] In effect, a more restrictive approach on the issues of visas, asylum, immigration, and border security was taken. Sound and efficient border management is officially considered essential to ensure a high level of internal safety against terrorism, to which the citizens are entitled.[117] This time, counter-terrorism legislation entailed a spill-over to

[112] http://www.vorratsdatenspeicherung.de/content/view/216/55/lang,de/#letter (last visited July 2009)

[113] In contrast to the Commission proposal, the final Directive does not foresee a provision for the compensation of incurred costs.

[114] For critical analyses, see Büllingen et al. (2004); Breyer (2007), p. 214; Zöller (2007), p. 392; Alvaro (2005), p. 47.

[115] Instructive: Addendum to Cover Note, Council Doc. 8958/04 ADD 1 of 20 December 2004.

[116] Title IV TEC.

[117] Cf. European Council, Laeken Summit, Conclusion 42, Council Doc. SN/300/1/01.

legislation in the immigration and asylum area.[118] As a result of the 9/11 events, a number of Commission proposals were postponed that showed an admission-friendly EU attitude towards third country nationals, such as proposals for directives on family reunion and asylum procedures, the definition of the term refugee, and admission of third-State nationals to employment.[119] Instead, the Council decided that appropriate measures against possible terrorist attacks on the EU territory shall include strengthened controls at the European external borders, strengthened surveillance measures of the police in the area of internal borders, a vigilant checking of identity papers and residence permits, and the application of procedures for the issue of visas with maximum rigour.[120] After the events of Madrid, the protection of security of international transport and securing effective systems of border controls were added to the focal points in the EU's strategy to protect from terrorism (see above). In the aftermath of the 2001/2004 terrorist attacks, several measures had been adopted in the fields of border control, combating illegal immigration, and document security that relate, albeit not exclusively, to the fight against terrorism.

One of the priorities of the EU is to be found in actions that improve the security of passports by use of *biometric data*. Here, the EU follows global approaches to identify the true links between the holder and the passport or travel document as well as to improve these documents against forgery. As a result, Regulation EC 2252/04 harmonises national law in view of security features for passports and travel documents.[121] Under the Regulation, Member States must introduce biometric identifiers in passports or travel documents by incorporating a storage medium containing the facial image and fingerprints (the latter with effect from 28 June 2009 at the latest). Recently, after hot debates, the European Parliament and the Council agreed on an amendment of the Regulation, exempting children under the age of 12 years from giving fingerprints as well as persons who are physically unable.[122] Additional technical specifications, such as additional security features and requirements, technical specifications for the storage medium of the biometric features and their security, and requirements for quality and common technical standards for the facial image and the fingerprints will be further established. The EU will also integrate biometric identifiers into the second generation of the Schengen Information System and the Visa Information System.[123]

---

[118] Den Boer (2003b), p. 11.

[119] Vennemann (2003a), p. 264.

[120] Conclusion adopted by the Council (Justice and Home Affairs), Brussels 20 September 2001, Council Doc. SN 3926/6/01.

[121] OJ L 385 of 29 December 2004, p. 1.

[122] Cf. http://www.europarl.europa.eu/oeil/file.jsp?id=5548432. The European Parliament mainly opposed an initial Commission proposal to exempt children under the age of 6 years (COM(2007) 619). For a critical analysis of the proposal in view of data protection, see Opinion of the European Data Protection Supervisor OJ C 200 of 6 August 2008, 1.

[123] Cf. 4.4.3.3.

Security measures after the attacks of 9/11 as regards border controls led to a temporarily fortification of checks at the external borders of the Schengen area, and a new definition of conditions and procedures, in the Schengen borders code, for the (temporary) reintroduction of border control at internal borders in the Schengen area by Member States in the event of a serious threat to their public policy or internal security, which especially eyes terrorist threats.[124] Currently under discussion are practical proposals of the Commission from February 2008 that seek to improve EU border security by reinforcing border checks, border surveillance, and operational coordination between Member States. The Commission, inter alia, proposed the gradual development of a European Border Surveillance System (EUROSUR), whose purpose will not only be the reduction of the number of illegal immigrants losing their life at sea, but also increasing the internal security of the EU as a whole by helping to prevent cross-border crime.[125] Furthermore, automated border checks procedures are envisaged to be introduced for bona fide travellers who shall be registered in an Electronic System for Travel Authorisation (ESTA). The Commission expects that the system – as a side-effect – will also be better at dealing with persons illegally remaining in Member States, because the automatic registration of the time and place of entry and exit of third-country nationals could especially help to identify overstayers. The consideration is not fallacious that this system is also of advantage to combat suspected terrorists.

4.4.2.6 Transport Security

Another area of the first pillar, which is very much affected by legal action of the European Community since 2001, is international transport security. Regulation 2320/2002 establishes common standards on civil aviation security, including staff screening, screening of passengers and cabin baggage, security checks on cargo, and requirements for aircraft security.[127] Regulation 725/2004 on enhancing ship and port facility security incorporates the maritime security measures adopted in December 2002 by the International Maritime Organisation (IMO) into Community legislation in order to prevent acts of terrorism against ships.[128] Directive 2005/65 complements the Regulation – which was limited to security measures on board vessels and the immediate ship/port interface – and aims at ensuring the fullest protection possible for maritime and port industries.[129] Therefore, security measures should be

[124] Chapter II of Regulation (EC) No 562/2006, OJ L 105 of 13 April 2006, p. 1.

[125] COM(2008) 68.

[126] COM(2008) 69.

[127] OJ L 355, 30.12.2002, p. 1. The Regulation has been amended several times by implementing legislation.

[128] OJ L 129 of 29 April 2004, p. 6.

[129] OJ L 310 of 25 November 2005, p. 28.

introduced, covering each port within the boundaries defined by the Member State concerned, and thereby ensuring that security measures taken pursuant to Regulation 725/2004 benefit from enhanced security in the areas of port activity.

Currently, the Council is negotiating a Commission proposal to introduce an EU-wide, harmonised system allowing law enforcement to process and analyse Passenger Name Record (PNR) data,[130] which are provided by air carriers.[131] Although the proposal may include ensuring air security, it was based on Art. 29 ff TEU because the use and purpose of the collection of the PNR data is confined to the prevention of and fight against terrorism and "other serious crime, including transnational organised crime", hence purposes of the third pillar. The PNR data should mainly make it possible for law enforcement authorities to identify unknown high-risk passengers, allowing for a secondary screening on their arrival and refusal of entry. The proposal on the PNR largely mirrors the agreement that was concluded between the EU and the USA on the use of PNR data.[132] Air carriers would be obliged to make available to law enforcement authorities of the EU Member States a set of 19 pieces of air passenger data that they collect and process in their reservation systems, including passport data, name, address, telephone numbers, travel agent, credit card number, history of changes in the flight schedule, seat preferences, etc.[133] Discussions in view of the PNR scheme are very reminiscent of data retention. Although EU governments consider the use of PNR data a necessary tool to prevent and fight terrorism, privacy concerns can not be denied. Additionally, the trends described for data retention come to light here again.

4.4.3 Operational Acquis Anti-terrorisme

In parallel to the aforementioned legislative counter-terrorism measures, the EU has placed, right from the beginning, a focus on enhancing the operational interaction between the national law enforcement authorities – particularly police services – of the EU Member States. Emphasis was put on stimulating, promoting, and facilitating the exchange of relevant information between the police authorities as well as of sharing intelligence and best practices between the police, intelligence, and security services of the different EU Member States. Included is the supply of information to central EU bodies and units, such as Europol and the Joint Situation Center (SitCen), which will be dealt with in the section "institutional acquis anti-terrorisme" below.

---

[130] PNR is a record in the database of a Computer Reservation System (CRS) that contains the travel record for a passenger, or a group of passengers travelling together. The concept of a PNR was first introduced by airlines that needed to exchange reservation information in case passengers required flights of multiple airlines to reach their destination ("interlining").

[131] COM(2007) 654.

[132] Cf. Wahl (2007a), pp. 9–11; Wahl (2006c), pp. 48–49; Wahl (2006a), pp. 3–4.

[133] For further details on the proposal, controversial reactions, and the state of play of negotiations, see Wahl (2007d), pp. 101–104. In early 2008, the Council redrafted the proposal, see Wahl and Staats (2008a), pp. 29–30.

4.4.3.1 Operational Interaction Through Joint Investigation Teams

The third flagship of the EU's immediate legal reaction to the 9/11 events, beside the FDs on Combating Terrorism and on the European Arrest Warrant, is the Council Framework Decision on Joint Investigation Teams (JITs) of 13 June 2002.[134] It is the counterpart for police cooperation to the swifter cooperation of the judicial authorities by the European Arrest Warrant and allows law enforcement authorities to pool their resources.[135] Two or more Member States have the possibility to set up joint investigation teams that are entitled to carry out, in one or more of the Member States involved, criminal investigations into specific matters for a limited period. In cases of the investigation and prosecution of terrorist acts, a team may comprise police officers and magistrates who specialise in counter-terrorism. The team may also include officers from Europol and Eurojust under the condition that the Europol Convention is adapted.[136] Much criticism has faced an "open clause" that allows, inter alia, even the request for assistance from third countries, such as the USA.[137] The inclusion of the US authorities in joint teams was interpreted as being intrusive.[138]

It is again noteworthy that the framework of joint investigation teams is not a terrorism-related instrument. Investigations on terrorist offences may be one opportunity, but the framework actually applies to ordinary crime cases, such as drugs offences or organised car thefts with trans-border character, which have proved the habitual occasions for creating joint investigation teams. This is only one of the typical features of EU policy post 9/11, which was already described in the context of the European Arrest Warrant. Likewise, the legal framework for JITs owed much to the Tampere Programme,[139] and the events of 9/11 provided for the crucial accelerated factor to push through implementation of an awaited investigative tool.

4.4.3.2 Excessive Exchange of Law Enforcement Information

That JITs are considered a necessary tool to enhance the internal security of the EU is reiterated in Art. 3 of the Council Decision 2005/671/JHA of 20 September 2005 on the *exchange of information and cooperation concerning terrorist offences*.[140]

---

[134] OJ L 162 of 20 June 2002, p. 1.

[135] Zimmermann (2006), p. 132.

[136] Therefore, the Europol Convention had to be adapted by a Protocol of 2002 (OJ L 162 of 20 June 2002). The ratification of the protocol lasted rather long and entered into force on 29 March 2007. The legal basis for Eurojust derives from the Eurojust Decision of 2002 (see also below, Sect. 4.4.4).

[137] Art. 1 (12) of the FD; see also recital 9.

[138] Zimmermann, ibid.

[139] And the need to implement the 2000 EU Convention on Mutual Legal Assistance. Therefore, the FD contains identical wording to Art. 13 of the 2000 EU MLA Convention. After the Convention entered into force in August 2005, the FD lapsed. For the trajectory of the FD and the consequences of the dual legal basis (framework decision vs. convention), see Rijken (2006), p. 99; Plachta (2005), p. 284.

[140] OJ L 253 of 29 September 2005, p. 22.

This 2005 Decision, which is a direct response of the Commission to the attacks to Madrid in March 2004, leads to the topic of exchange of information because the Decision acknowledges the need for ever greater exchanges of information due to the persistence of the terrorist threat and the rise in the complexity of the phenomenon.[141] It ensures that information is exchanged between operational services responsible for combating terrorism. The Decision foresees extended obligations for the specialised law enforcement authorities to make available all relevant information in connection with criminal investigations or criminal proceedings in connection with terrorist offences.[142] Any such information (e.g. suspects' personal data, the activity under investigation, the type of offence, etc.) that may affect two or more Member States is to be transmitted to Europol and Eurojust (see below).

The reaction to the attacks of Madrid demonstrates a clear shift of the EU policy towards a proactive, robust, and excessive "European exchange of information approach for law enforcement authorities". In this wave, the Commission tabled several considerations on the introduction of a free circulation of information between the law enforcement authorities of the EU Member States and the authority in charge of crime prevention. These authorities would include the police forces, customs authorities, financial intelligence units, the judicial authorities, and all the public bodies involved in the detection of security threats, conviction, and punishment. In addition, European bodies, notably Europol, would be involved in the information flow and would benefit greatly.[143]

Perhaps in order to thwart a too far-reaching simplification of exchange of law enforcement data by Commission proposals, perhaps in order to simply react to the Madrid bombing, as requested by the European Council on 25 March 2004, Sweden tabled a draft for a "*Framework Decision on simplifying the exchange of information and intelligence* between law enforcement authorities of the Member States, in particular as regards serious offences including terrorist acts" in June 2004. The Framework Decision was finally adopted in 2006.[144] The purpose is that Member States' law enforcement authorities may exchange existing information and intelligence more effectively and more expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.[145] Present obstacles of mutual assistance in criminal matters should be overcome and the information exchange as established by the Schengen Convention should be sped up. This is achieved by (1) standardizing the procedure to request and collect information,

[141] Recital 4.

[142] The 2005 Decision repeals the earlier Decision 2003/48/JHA, which was limited to blacklisted persons and convictions.

[143] COM(2004) 429.

[144] Council Framework Decision 2006/960/JHA of 18 December 2006, OJ L 386 of 29.12.2006, p. 89.

[145] Cf. Art. 1 (1) of the FD.

(2) setting time limits to answer requests for information regarding certain types of offences, and (3) abolishing discrimination between the exchange within one Member State and cross-border exchange.[146] The Framework Decision is not limited to specific types of information, but applies to any information or data that can be useful in a crime investigation, including information or intelligence in police records or files as well as telephone, mobile phone, or e-mail subscriptions or addresses kept by telecom operators.

Another integrative step towards exchange of operational data is achieved by Council Decision of 23 June 2008 on the *stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*.[147] The Decision integrates into the EU legal order the substantial part of a convention that was agreed on by seven EU Member Sates outside the EU framework in 2005 (the Prüm Treaty). It is founded on the idea of attaining the maximum possible level of cooperation for the exchange of information, especially with regard to the fight against terrorism. The main feature is that Member States authorities are granted online access to each others automated DNA analysis files and automated dactyloscopic identification systems (on the basis of a "hit/no hit system").[148] In contrast to the just-mentioned Framework Decision, data exchange is thus limited *ratione materiae*, but establishes the principle of mutual availability of DNA and fingerprint data. The Decision furthermore allows closer cooperation between police authorities, including joint security operations and cross-border interventions. Chap. 4 foresees that Member States should exchange personal data – if necessary, spontaneously – about suspicious persons who may commit terrorist offences. The Decision is again an example that terrorism is attached to the general combat of crime. Indeed, the first successes with the implementation of the Prüm Treaty relate to ordinary offences outside terrorism, which is why nearly all EU governments showed their interest on an EU-wide application of the Treaty.

4.4.3.3 Harnessing Central Databases for the Fight Against Terrorism

The EU undertook additional actions in order to harness common databases for the fight against terrorism. As a result, after 2001, work commenced to introduce new functions for databases that increase operational capacity so as to facilitate effective

[146] Art. 1 sets forth further limits for the provision of information, e.g. law enforcement authorities are not obliged to obtain information by means of coercive measures (but may provide information or intelligence *previously* obtained by means of coercive measures). Likewise, there is no obligation to communicate information that is likely to be used as evidence before a judicial authority, although the agency supplying the information may expressly consent to this.

[147] Council Decision 2008/615/JHA, OJ L 210 of 6 August 2008, p. 1.

[148] Another category foreseen is the automated searching of vehicle registration data. The provisions follow a gradual approach, which means that they provide specific rules for each type of information, taking into account the specific nature of these data types.

cooperation in view of terrorism. The first of these databases to name is the *Schengen Information System (SIS)*. The SIS is arguably the core "compensatory measure" after the creation of the Schengen area in the 1990ies with free movement of persons without internal borders and only one single external border where immigration checks for the Schengen States are carried out. The SIS became operational in 1995. To counter fears that criminals may operate without obstacles, the SIS was designed as a joint computerised information system for exchange of information on wanted persons or wanted objects. Its purpose is to allow, through an automated query procedure, checks on persons to be made at border controls or within a territory, in order to detect criminals and illegal immigrants moving into and from one Schengen country to another.[149] In its original format, the SIS allows a limited number of operations because (1) there are strict regulations on the purpose limitation (the request must be specified according to the purpose as described); (2) only certain categories of data can be registered;[150] (3) entry of personal data is confined (to certain items); and (4) access to the system is exclusively reserved for designated officials, namely officials responsible for police, customs, and border controls as well as visa authorities for only one category.

Widely unperceived by legal scholars and the public, the Council finalised legislation in 2004/2005 that opens the SIS for the purposes of fighting terrorism.[151] The main purpose of the amendment is that cooperation between law enforcement departments specialising in counter-terrorism is stepped up and the work of Europol and Eurojust in the fight against terrorism is improved. Therefore, the main amendments to the SIS concern access to the SIS for national judicial authorities responsible for investigating and prosecuting crime as well as access for Europol and the national members of Eurojust to a limited number of categories of SIS data.

The wider access to SIS data is considered the first phase on the extension of the SIS facility. Already in December 2001, the further development of the SIS towards its second generation (SIS II) was launched. Not a minor reason for the development was the need for adaptation of the first-generation SIS to modern forms of cross-border criminality, including international terrorism. The SIS II will be made ready to take up larger capacities and to include new technologies, including the possibility of storing biometrics data, i.e. photographs and fingerprints. Furthermore,

[149] The SIS is regulated in Art 92–119 CISA, which includes data protection rules. The SIS consists of a national section for each of the Contracting Parties and a central technical support function. Users search the central file in Strasburg, which itself is fed by the national files. The SIS is the largest European centralised database and is the most important tool for cross border police work in practice. Since 1995, more than 15 million records have been created in the SIS and there are approximately 125,000 access terminals within the participating states.

[150] Art. 94 ff. CISA. The categories are: persons wanted for extradition; persons to be refused entry; missing persons or those in need of protection; witnesses or those subject to a criminal judgement or summonses to appear; persons to be kept "under surveillance" or subject to specific checks; and a defined range of objects.

[151] Council Regulation (EC) No 871/2004, OJ L 162 of 30 April 2004, p. 29 and Council Decision 2005/211/JHA, OJ L 68 of 15 March 2005, p. 44.

the functions of the SIS are newly defined because the SIS will become not only a reporting system but an investigation system.[152]

Europol and "designated national authorities" will in the near future also have access to the *Visa Information System (VIS)*, which is due to be operational soon and will represent the second significant European central database. Although the VIS is actually designed for the support of the Union's common visa policy and facilitation of the exchange of visa data between the Member States' consulates and other administrative authorities,[153] the attacks of Madrid at the latest contributed to the consideration that the VIS is an essential tool for securing internal security and combating terrorism.[154] The VIS as a source of information for law enforcement authorities is particular interesting because the VIS – like the SIS II – will include the storage of biometrics identifiers – i.e. photographs and fingerprints – of visa applicants. In view of data protection, the rather wide access of law enforcement[155] to an administrative visa database leads to the dilution of the purpose limitation principle. A breach is particularly feared if access of these authorities becomes routine and is not limited to access on a case-by-case basis and not accompanied by strict safeguards.[156]

4.4.4 Institutional Acquis Anti-terrorisme

The attacks of 9/11 led to the strengthening, extension, and even creation of central European bodies. The essential developments regarding this institutional side of the EU's fight against terrorism are analysed in the following.

---

[152] COM(2001) 720. Although the legal bases for the SIS II were established (Council Decision 2007/533/JHA of 12 June 2007, OJ L 205 of 7 August 2007 and Regulation (EC) No 1987/2006, OJ L 381 of 28 December 2006), the operation of the SIS II is still awaiting. After several delays, the Commission plans to get the SIS II operable in 2009. Europol and Eurojust are granted similar access rights as SIS I.

[153] Council Decision 2004/512/EC, OJ L 213 of 15 June 2004, p. 5; Regulation (EC) No 767/2008, OJ L 218 of 13 August 2008, p. 60.

[154] Recitals 1–3 of Council Decision 2008/633/JHA, OJ L 218 of 13 August 2008, p. 129.

[155] As the term "designated authorities" implies, the Member States are largely free to decide which of their national authorities should have access to the VIS. The term is rather broadly defined: "designated authorities" mean authorities that are responsible for the prevention, detection, or investigation of terrorist offences or of other serious criminal offences (Art. 2 (1 e) Council Decision 2008/633/JHA).

[156] Opinion of the EDPS, OJ C 97 of 25 April 2006, p. 6; Opinion of the Joint Supervisory Body of Europol (Opinion 06/22). For the conception of purpose limitation and general trends, see Wahl 2006e, 130 ff.

4.4.4.1 A Broker for Police Information and Intelligence on the Terrorism Threat: The Expansion of Europol

Above all, the role and more effective involvement of the European Police organisation (Europol) in the EU's strategy to fight terrorism increased. On 21 September 2001, the European Council declared that "Member States will share with Europol systematically and without delay all useful data regarding terrorism. A specialist anti-terrorist team will be set up within Europol as soon as possible and will cooperate closely with its US counterparts".[157] Europol had been created in 1995 based on a convention[158] as a response to the opening of the European Union's internal frontiers by the Schengen Convention, which required reaction from the side of the police.[159] The European Union law enforcement organisation handles criminal intelligence and aims to improve the effectiveness and cooperation between the competent authorities of the Member States in preventing and combating serious international organised crime. Europol's mandate had been steadily extended, but is limited to certain forms of (serious international) crime.[160] Europol's support applies where an organised criminal structure is involved and two or more Member States are affected. Short before Europol took up its full activities as of 1 July 1999, the Council instructed Europol also to deal with crimes committed or likely to be committed in the course of terrorist activities against life, limb, personal freedom, or property, i.e. Europol's competence was extended to include counter-terrorism.[161]

Europol's principal tasks are as follows: (1) facilitation of the exchange of information between the Member States; (2) obtaining, collating, and analysing information and intelligence; (3) notification to the competent authorities of the Member States of information concerning them and of any connections identified between criminal offences; and (4) aiding investigations in the Member States by forwarding all relevant information. Additional tasks include (1) the development of specialist

---

[157] Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, Council Doc. SN 140/01.

[158] OJ C 316 of 27 November 1995, p. 2. A consolidated version of the Europol Convention after the entry into force of three amending protocols of 2007 is available at: http://www.europol.europa.eu/legal/Europol_Convention_Consolidated_version.pdf (last visited July 2009).

[159] As to the rationale of Europol, see Bunyan (1995).

[160] Art. 2 of the Europol Convention and relevant Annex to Art. 2 para. 2. Since 2002, all crimes in the annex are covered. Europol supports the law enforcement activities of the Member States mainly against illicit drug trafficking; illicit immigration networks; forgery of money (counterfeiting of the euro) and other means of payment; trade in human beings (including child pornography); trafficking in nuclear and radioactive substances; motor vehicle crime; and money laundering (except for predicate offences). In addition, other main priorities for Europol include crimes against persons, financial crime, and cybercrime. Europol's competence also covers related criminal offences.

[161] Council Decision of 3 December 1998, OJ C 26 of 30 January 1999, p. 22. That Europol was initially not conferred a counter-terrorism mandate resulted from a dispute between Member States, mainly between Spain, which pleaded for a counter-terrorist mandate of Europol, and the UK, which objected. A compromise was then settled in Art. 2 (2) of the Europol Convention that the Council shall decide by unanimous vote to extend Europol's remit to these crimes.

knowledge of the investigative procedures of the competent authorities in the Member States and provision of advice on investigations; (2) provision of strategic intelligence to assist with and promote the efficient and effective use of resources available at the national level for operational activities; and (3) preparation of general situation reports. Europol can also improve its international law enforcement cooperation by negotiating bilateral operational or strategic agreements with other states outside the European Union and international organisations.

In sum, Europol's task is to facilitate the exchange of information, analyse it, and coordinate operations involving several Member States. In fact, Europol is an "information broker" or a "clearing house" for the exchange of police data. The exchange of information is effectuated by national units and liaison officers. Unlike national police services, Europol does not have executive powers, i.e. it can neither detain individuals nor can it conduct home searches, for instance.

The core tool for Europol to perform its tasks as an information broker and to produce strategic information that will uncover patterns of criminal activity, is a computerised information system, the so-called Europol Computer System (TECS). It consists of three separate databases, each with different levels of access by Europol staff and liaison officers: (1) The information system, which enables the Member States to have quick reference to crimes and the involved criminals. Thus, in this system, personal data of suspects and some further details on the criminal offence can be input. (2) The analysis work files (AWFs), in which data are edited analytically by analyses groups. The AWFs are intended to be used in drawing up strategies in the fight against serious crimes and terrorism that fall into the remit of Europol; the findings could then be used for the purposes of initiating or accompanying investigations. (3) The index system.

As indicated above, immediately after the attacks of 9/11, the European Union made increased use of the existing structures of Europol and extended the capacities of Europol. Although terrorism was not a new competence for Europol, terrorism is, since 2001, a priority area of Europol's daily work, and ties up many human and financial resources to and for Europol.[162]

In 2001, Europol continued two analysis work files relating to counter-terrorism and expanded them continuously. Based on information and intelligence provided by the police forces and intelligence services of the EU Member States, Europol maintains two AWFs on assessing the terrorist threat in Europe, one focusing on Islamic fundamentalist terrorism and another focused on all other terrorist groups and activities in the EU.[163] Further efforts were made on the institutional side within Europol. The Member States allocated additional financial means and personnel to a team of counter-terrorism specialists within Europol.[164] This Counter-Terrorism

[162] Cf. Europol Annual Reports 2001 and 2007, p. 23.

[163] Deflem (2006), p. 344; Dittrich (2005), p. 31. According to the Europol Annual Report 2003, Europol opened another work file dealing with indigenous terrorism.

[164] According to Statwatch, 3.16 Mio. euros were added in 2002, which corresponds to an increase of approximately 7% in comparison with the original budget for Europol.

Task Force (CTTF) was mandated to (1) collect in a timely manner all relevant information and intelligence concerning the current terrorism threat in the EU; (2) analyse the collected information and undertake the necessary operational and strategic analysis; and (3) draft a threat assessment document based on information received, including targets, damage, potential modus operandi, and consequences for the security of the Member States. The Task Force, consisting of experts and liaison officers from both police and intelligence services, became operational on 15 November 2001, barely 2 months after the Council decisions were adopted.[165]

To date, the CTTF has produced several threat assessment reports, which include an Assessment Document on Islamic Extremist Terrorism, the financing of terrorism, various analyses of information concerning terrorist movements in Europe, alternative remit systems, and the profits from the sale of false and stolen documents. Further results of their work were the preparation of some strategic tools, such as a specific manual for the investigators in the field of counter-terrorism and the establishment of an Arabic-to-English translation system for the evaluation of the large amount of intelligence in Arabic transmitted by Member States to Europol. In 2007, the CTTF was transferred to the First Response Network, which became operational as of 2 July 2007. This new "EU tool", which is the result of lessons learned from past incidents, allows flexible support for EU Member States' investigations immediately after terrorist incidents. It consists of a network of more than 50 anti-terrorist experts from all Member States.[166]

Since 2001, Europol has also been involved in the preparation of the EU Terrorism Situation and Trend Reports (TE-SAT), which had been presented by the Council Terrorist Working Party to the European Parliament. In 2006, the Council mandated Europol to approve on its own the situation and trend report and endorsed widening the data collection for the TE-SAT. With this new methodology, Europol is expecting to achieve a better quality of the TE-SAT. The first TE-SAT under this new mechanism was presented by Europol in 2007.[167] The new TE-SAT is defined as an unclassified document, which is intended to inform the European Parliament of the phenomenon of terrorism in the EU.[168] It will also be forwarded to the Council and can be used to inform the public.[169] The TE-SAT distinguishes between different categories of terrorism, i.e. – pragmatically - between Islamist terrorism, ethno and separatist terrorism, left wing and anarchist terrorism, and right wing terrorism. It describes the outward manifestations of terrorism, i.e. terrorist attacks

[165] Europol Annual Report 2001.

[166] Europol Annual Report 2007, p. 24.

[167] The new TE-SATs are published at the Europol homepage: www.europol.europa.eu.

[168] Not contained in the TE-SAT is information that is classified, falls under data protection law, or information that could jeopardise ongoing investigations.

[169] Council Doc 8196/2/06 of 18 May 2006.

and activities,[170] seeks to establish basic facts and figures regarding terrorist attacks and activities in the EU, and provides for general tendencies in the way the terrorist situation is changing or developing within the European Union.

In addition, Europol provides several other products and services related to counter-terrorism, such as a reference of counter-terrorism responsibilities in the Member States; a glossary of terrorist groups and national contact points for illicit trafficking of nuclear and radioactive substances; a central reference database on bombs; and technical support and joint training activities in relation to the criminal use of Chemical, Biological, Radiological, and Nuclear (CBRN) weapons and substances. In 2007, Europol successfully launched the project "Check the Web", which is an information portal at Europol that centralises information on observation and analysis of propaganda and other activities of Islamic terrorist groups using the Internet.[171] The portal is to include a list of links to monitored web sites, statements by terrorist organisations, and details on other experts checking the web in EU countries, including their language competence and technical expertise. On the operational side, Europol supports live investigations in Member States against terrorists and terrorist groups and assists Member States in ensuring security of major international events against possible terrorist attacks, e.g. by contributing threat assessments or seconding liaison officers to assist with the events.

The Council also put much effort into strengthening the obligation of Member States' national law enforcement authorities to provide Europol with relevant information. As mentioned under 4.4.3.2, in 2005, the Council stipulated that Member States must communicate intelligence information to Europol, at least: (1) Data that identify the person, group, or entity; (2) acts under investigation and their specific circumstances; (3) the offence concerned; (4) links with other relevant cases of terrorist offences; (5) the use of communications technologies; and (6) the threat caused by the possession of weapons of mass destruction.[172] However, plans to set a new legal footing regarding relations between Europol and the national security and intelligence services – in the wake of the bombings of Madrid and London – were given up. The plans would have established contact points in the Member States' services to develop the efficient transmission of information between the Member States and Europol to combat terrorism.[173]

---

[170] In this context, the TE-SAT 2007 emphasises that the report does "neither attempt to analyse the root causes of terrorism nor to assess the threat posed by terrorism. Furthermore, the TE-SAT does not assess the impact or effectiveness of counter-terrorism policies and law enforcement measures taken, despite the fact that they form an important part of the phenomenon".

[171] See also Council Conclusions on cooperation to combat terrorist use of the Internet ("Check the Web"), Council Doc. 8457/2/07 of 16 May 2007.

[172] Art. 2 (3, 4) of the Council Decision 2005/671/JHA.

[173] Cf. COM(2005) 695. Withdrawn in 2007 (OJ C 66 of 22 March 2007, p. 6).

4.4.4.2 The Judicial Hub for Terrorist Prosecutions: The Emergence of Eurojust

A second institution, "sailing with the tide of EU anti-terrorism efforts"[174] was Eurojust – a centralised unit that was held necessary to improve judicial cooperation between the EU Member States to overcome existing obstacles thrown up by mutual legal assistance agreements. Eurojust took up its work in December 2004 after the legal basis was finalised in 2002.[175] The policy strands that we could observe with the European Arrest Warrant, the terrorism definition, and other anti-terror related EU instruments also apply to Eurojust: First, the EU could build on existing structures and spadework, in particular, preparations of the Tampere summit, which took the political decision on establishing Eurojust.[176] In addition, Eurojust could rely on practical experience by the provisional judicial cooperation unit (known as Pro-Eurojust) – a roundtable of a prosecutor or judge from each EU Member State using the Council infrastructure, which has been working since March 2001. Second, the attacks of 9/11 provided the decisive catalyst effect, which settled a dispute among Member States on the strength of Eurojust's structure.[177]

Eurojust is the first permanent network of judicial authorities in the world and it is widely considered a key player in the EU's fight against terrorism.[178] Notwithstanding, Eurojust is not a dedicated counter-terrorism organisation as well.[179] In comparison with Europol, its remit to deal with cross-border crime is a bit wider,[180] however its resources to build up strong EU capacities to counter terrorism have remained limited. Eurojust's role is above all advisory and – like Europol – it has a clearinghouse function. Eurojust's goal is not only to promote coordination between competent authorities in the Member States but also to facilitate the implementation of international mutual legal assistance and of extradition requests.[181] Eurojust supports the competent authorities of the Member States in order to render their investigations and prosecutions more effective when dealing with cross-border crime. Eurojust is able to organise coordination meetings between the countries involved in case of a crime with cross-border dimension in which the parties can

[174] Den Boer (2003b), p. 12.

[175] Council Decision 2002/187/JHA setting up Eurojust, OJ L 63 of 6 March 2002, p. 1.

[176] Conclusion No. 46.

[177] Cf. von Langsdorff (2003), p. 472; Wahl (2001), p. 23.

[178] Cf. among others Messelken (2003).

[179] Zimmermann (2006), p. 132.

[180] Art. 4 Eurojust-Decision. For types of offences other than those referred to, Eurojust may in addition assist in investigations and prosecution at the request of competent national authorities.

[181] After the entry into force of the European Arrest Warrant, Eurojust can be considered as the "Union's judicial lever relative to the EAW" (Zimmermann (2006), p. 132).

exchange information and agree on future actions. In a nutshell, Eurojust can be considered a promoter for Europe-wide co-operation on criminal justice cases.

Eurojust fulfils its tasks through national members (senior magistrates, experienced prosecutors, or judges) seconded by each Member State or as a College that consists of all the national members and in which each national member has one vote. The main added value of this structure is that the team is capable of putting any case referred to Eurojust into an EU context and more easily spot any patterns of trends in EU crime than colleagues in their home countries.[182] Eurojust was conferred legal personality, so that it can conclude formal agreements with third countries or international organisations. Eurojust also maintains close cooperation with other EU bodies. With Europol, Eurojust coordinates its activities and exchanges operational, strategic, and technical information.[183]

The ministers of the EU Member States reiterated several times after terrorist attacks that national authorities should make the maximum possible use of and intensify the exchange of information through Eurojust.[184] In this context, it is noteworthy that already the Eurojust Decision stipulated under Art. 12 that each Member State, as a matter of high priority, shall put in place or appoint a national correspondent for terrorism matters in their country who works as a relay station to the national member at Eurojust. In 2003, Member States were explicitly obliged to give the national correspondent all relevant information concerning and resulting from criminal proceedings with regards to terrorist offences involving blacklisted persons.[185] In 2005, the Council extended this obligation to provide Eurojust with a minimum of information concerning all criminal investigations or prosecutions on terrorist offences (similar to the regulation for Europol, see above).[186]

Like Europol Eurojust also provided for specific anti-terrorism structures within its internal organisation. In the wake of the Madrid bombings of 2004, the Eurojust College created a terrorism team of several national members that provided specialist work to facilitate and deal more effectively with requests for assistance. The tasks for this team are mainly (1) to establish a centre of expertise within Eurojust regarding terrorism; (2) to ensure terrorism coordination meetings are well prepared and organised; (3) to enhance the exchange of information related to terrorism via regular contacts with nominated correspondents on terrorism; (4) to establish a general database of legal documents related to terrorism; (5) to verify the practical use and added value of existing EU or UN instruments in the area of financing of terrorism; and

[182] Bures (2006), p. 64.

[183] Details relating to the cooperation between Eurojust and Europol are stipulated in an agreement of 9 June 2004 (cf. http://www.europol.europa.eu/legal/agreements/Agreements/17374.pdf (last visited July 2009)). In the near future, the relationship between Eurojust and Europol will be based on a revised agreement which was adopted on 5 June 2009 by the JHA Council (cf. Council doc. 10019/09 of 15 May 2009).

[184] Council Doc. SN 3926/6/01, European Council, Declaration on Combating Terrorism of 25 March 2004, point 5b); Council Doc. 1116/05, p. 7.

[185] Art. 3 (1) Council Decision 2003/48/JHA.

[186] Art. 2 (3, 5) of Council Decision 2005/671/JHA.

(6) to define a better approach to the receipt and handling of terrorism information from open and closed sources.[187] The Eurojust Terrorism Team has also provided Europol with information for the Terrorism Trend and Situation Report and improves interaction with Third States, such as the USA, regarding terrorism issues.[188]

In practice, Eurojust particularly supported anti-terrorist prosecutions in the Member States by holding joint meetings with national prosecutors, be they for the purpose of coordination of concrete operations, support tactics, or developing general strategies on significant casework topics, such as fundamental terrorist activities and the financing of terrorism.[189]

Eurojust's annual reports outline that, since 2001, terrorism remains one of the top priorities of Eurojust's work. A reform aims at further strengthening Eurojust's anti-terrorist framework, however in a more or less moderate way. The system of national correspondents will be strengthened and institutionalised towards a Eurojust national coordination system; the information flow from the national authorities to the national member at Eurojust will be improved by a more timely and earlier supply of terrorism-related information. To this end, EU Member States are obliged to set up a national correspondent for Eurojust for terrorism matters. Eventually, the Commission will regularly monitor Eurojust's capacities to support Member States in fighting terrorism.[190]

4.4.4.3 Integrated Border Control and Terrorism: The Establishment of Frontex

As mentioned above, the EU inextricably linked its policy on immigration and border controls with the combat of terrorism and considers a coherent, common effective management at the external borders of the EU Member States a significant booster for the security of the shared area.[191] Therefore, changes were also undertaken on the institutional side by establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU (in short: Frontex).[192] The Agency should serve as a complement to the above-mentioned legislative measures on tighter checks of the EU's external borders and closer surveillance of illegal immigration. Although the legal act establishing Frontex as well as preparatory legislative work does not expressly mention a link between Frontex and combating terrorism, it became clear from political declarations

[187] Eurojust Annual Report 2004, p. 24, Annual Report 2005, p. 34; Annual Report 2006, p. 31f.

[188] Eurojust Annual Report 2006, p. 31f.

[189] See Eurojust Annual Reports 2001–2008, available at: http://www.eurojust.europa.eu/press_annual.htm (last visited July 2009 The reports also contain casework studies in which Eurojust was involved in terrorist investigations.

[190] Council Decision 2009/426/JHA on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 138 of 4 June 2009, p. 14.

[191] COM(2002) 233 and COM (2001) 672.

[192] Council Regulation (EC) No 2007/2004 of 26 October 2004, OJ L 349 of 25 November 2004, p. 1.

that the new border agency should also be involved in the EU's fight against terrorism. In addition to the European Council's Laeken summit declaration of 2001, the declarations after the attacks of Madrid and London again stressed that priority should be placed on building on a strong EU framework for pursuing and investigating terrorists across borders and that the need is obvious to strengthen border controls.[193] Frontex took up its work on 1 May 2005.

The essential task of Frontex is to coordinate operational cooperation between Member States as regards management of external borders as well as to carry out risk assessments.[194] The essential contribution of Frontex in view of combating terrorism is the inclusion of terrorism in the risk analysis of Frontex. In addition, Frontex maximises the capacity of existing border systems to monitor, and where relevant, counter the movement of suspected terrorists across the internal and external borders of the EU, e.g. by developing and maintaining records for technical equipment and national experts which/whom can be resorted to "in particular situations".[195] On balance, Frontex is the EU's second security body with the mandate to support operational actions of the EU Member States in addition Europol.[196] Like Europol, Frontex's main tasks are the processing of intelligence, analysis work, and coordination. Frontex has also no direct executive powers.[197]

4.4.4.4 Guiding Multilateral Police Operations: The Development of the European Police Chiefs Task Force

Another actor in the field of police cooperation, whose role and tasks have been widely shaped by the terrorist events of 2001 and 2004, is the European Police Chiefs Task Force (PCTF). From the outset of its establishment by the European Council at the Tampere summit of 1999, the majority of Member States made a point of the PCTF being a permanent but informal forum for building personal links without giving it a legal basis. Regular meetings of the police chiefs as heads of delegations from the EU Member States are to ensure "the exchange (…) of experience, best practices and information on current trends in cross-border crime and contribute to the planning of operative actions".[198] Although the PCTF has no legal decision-making powers under the EU/EC Treaty, it is an important high-level group of officials that takes, at the EU level, strategic decisions on the future of police organisations in the EU Member States, discusses challenges and difficulties faced by police forces in the EU, and attempts to find adequate solutions.

---

[193] Vaughan-Williams (2008), p. 66; Jahn (2006), p. 207.

[194] Council Regulation (EC) No 2007/2004 of 26 October 2004, OJ L 349 of 25 November 2004, p. 1.

[195] Points 2.5.8 and 3.2.3 of the revised EU Action Plan on combating terrorism, Council doc. 7233/1/07 of 29 March 2007.

[196] Art 13 of Council Regulation 2007/2004 states that the Frontex Agency shall work closely with Europol in the framework of working arrangements.

[197] Cf. also Holzberger (2006), p. 56.

[198] Recommendation 44 of the Tampere Conclusions, footnote 23.

In 2000, the year of its first meeting, the PCTF still had difficulties in defining its own role between the various EU actors (notably Europol) and Council working groups in the police field,[199] however after 9/11/2001 and 7/3/2004, the Council assigned new roles and remits to the PCTF and strengthened its influence in counter-terrorism.[200] On 31 October 2001, the PCTF performed the Council's mandate of 20 September 2001 to draw up an inventory of national anti-terrorism measures as well as to work out alert and intervention plans to deal with any trans-frontier terrorist acts.[201] Furthermore, the PCTF was charged with preparing measures to strengthen controls at external borders. After the events of Madrid in 2004, the PCTF became part of the EU's general line to "maximise capacity within the EU bodies to detect, investigate and prosecute terrorists and prevent terrorist attacks". The PCTF was called on to reinforce its "operational capacity and to focus on pro-active intelligence".[202] As a consequence the support of the PCTF work by Europol was tightened to improve the PCTF's contribution to the planning and coordination of operational actions (meanwhile, joint meetings between the PCTF, Europol, and Eurojust were also held).[203] Within the revised counter-terrorism action plan of 2007, the PCTF seems now to be focused on the multilateral planning and strategic guidance of operational projects (including terrorism alongside organised crime) at the EU level. In particular, the PCTF assists in the development of a European Crime Intelligence Model.[204]

While the current tasks are rather focusing on joint exercises, a more operational role is under discussion. Worth mentioning is also that the weight of the PCTF has been behind a number of counter-terrorism legislative acts for the purpose of law enforcement, such as on the "PNR scheme" and data retention (see above).[205] The development of the PCTF is another good example on how tasks of "supra-national" bodies have increased and been tailored against the background of the terrorist threat. However, the informal structure of the PCTF is assessed critically against the background that the group has been enabled to have an increasing influence on legislation and operations and strategies although it has no legal basis yet. Furthermore, actions of the PCTF are problematic because it receives data from Europol and other law enforcement authorities, but is not bound to data protection rules. This is even more true because the PCTF is not accountable to the European Parliament or national parliaments and its democratic legitimacy may be considered low.[206]

---

[199] Cf. Council documents of the UK delegation, 5858/00 of 2 February 2000 on the one hand, and of the Belgian Delegation, 8120/00 of 3 May 2000, on the other hand.

[200] For the development of the PCTF, see Bunyan (2006).

[201] Council Doc 14841/01 of 11 December 2001; Monar (2004), p. 153; Den Boer (2003b), p. 14.

[202] European Council, Declaration on Combating Terrorism of 25 March 2004, points 5, 8.

[203] Council Doc. 14938/04.

[204] Council Doc. 7233/1/07, points 3.3.1 and 3.3.2.

[205] Bunyan (2006).

[206] Den Boer et al. (2008), p. 114; Bunyan (2006).

4.4.4.5 Pooling Intelligence: The EU Joint Situation Center (SitCen)

Terrorism did not spare changes of formal structures within the Council, or more precisely within the General Council Secretariat. Here, two essential institutional developments have to be examined, the first is a reorientation and restructuring of the Joint Situation Center (SitCen), the second is the setting up of a European Counter-Terrorism Coordinator (CTC). Both structures aim at strengthening the coordinative role of the EU and to centre counter-terrorism information at the EU level.

The SitCen has been developed from a Policy Planning and Early Warning Unit, which was created in 1999 within the Council General Secretariat and worked for the High Representative for the Common Foreign and Security Policy, Javier Solana.[207] The unit initially convened experts from Member States (mostly diplomats) and were charged to support the Secretary General/High Representative for the CFSP and its staff with information and strategic analyses to help take appropriate decisions on the EU's foreign policy (e.g. assessments on potential and current crisis regions).[208] Until 2004, the SitCen's priorities were therefore focused on second pillar issues, i.e. on Common Foreign and Security Policy, and did not much serve to provide the necessary input for Justice and Home Affairs. This situation changed with the terrorist attacks in Madrid, when the unit was explicitly mandated to provide (with effect from 1 January 2005) the Council with strategic analysis of the terrorist threat within and outside the EU territory and to base these analyses on intelligence from Member States' intelligence and security services.[209]

Although Member States already shared sensitive information with SitCen for intelligence assessments after the attacks of 9/11,[210] SitCen was now officially restructured and a counter-terrorist cell was created to also cover internal security. The cell became active on 1 February 2005. Thus, SitCen now also contributes to the Justice and Home Affairs work by delivering strategic intelligence-based assessments on counter-terrorism matters – in support of current policy discussions.[211] In this context, the evolution of SitCen shows that terrorism is regarded at the institutional stage as a comprehensive task too, so that assessments can not only

[207] Javier Solana has a "double hat". He holds office of both Secretary-General of the Council of the European Union and High Representative for the Common Foreign and Security Policy. Mr. Solana assists the Council in foreign policy matters, through contributing to the formulation, preparation, and implementation of European policy decisions. He acts on behalf of the Council in conducting political dialogue with third parties.

[208] Instructive for the development of the SitCen, see the evidence given by W. Shapcott, Director of the Joint Situation Center, before the UK House of Lords, Shapcott (2005), p. 53.

[209] The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, OJ C 53 of 3 March 2005, 2.2.

[210] Shapcott (2005), who mentioned that SitCen "had existed as a sort of empty shell" until 11 September 2001 but that soon after the sharing of intelligence and assessments on external relations started.

[211] Cf. Written answer of Charles Clarke, UK Home Secretary, to the Parliamentarian John Hayes, 27 June 2005, http://www.theyworkforyou.com/wrans/?id = 2005-06-27a.503.h. (last visited July 2009).

be focused on external issues but must recognise internal (third pillar) and even economic (first pillar) issues as well, because terrorists do not care about the EU's pillar divide.[212] As a result, the assessments of the 20 or so national experts from domestic state security services and military intelligence units today support not only the High Representative, Javier Solana, and other parts of the Council structures of the second pillar, such as the Political and Security Committee (PSC) and the Working party on Terrorism (COTER), but also the Art. 36 Committee (CATS) and the Terrorism Working Group (TWG) in the third pillar, as well as, finally, all decision makers interested in the analyses.[213]

The analyses relating to terrorism include, for example, assessments on threats to modes of transport; threats to critical national infrastructure targets in EU Member States; and an assessment on the trends in terrorist financing. SitCen terrorist assessments are, as Müller-Wille states, "directly applied in the securitization of the terrorist threats at the political European level, trying to determine how serious it is, how urgently action must be taken and, somewhat tentatively, what instruments and policies are likely to be most effective".[214]

The SitCen analysts, who observe the current developments on a 24/24-h basis, resort to open sources, (e.g. reports in media), assessments of situations, and reports from the Member States and the European Commission, as well as reports and analyses of national security and intelligence services from all EU Member States. Information is also exchanged with Europol, although the SitCen does not have the power for direct access to the national police information/intelligence because this is exclusively reserved for Europol.[215]

It is worth mentioning that the quality of SitCen's terrorism analyses largely depends on the willingness of national intelligence and security services to feed SitCen with appropriate information. However, national services provide the SitCen with already assessed intelligence rather than raw intelligence, so intelligence is not looked for from scratch.[216] In effect, the SitCen is a compiler of intelligence assessments from the Member States but generates its own product, which is customized for its clients, i.e. the Council and the High Representative.[217] In doing so, the added value of the SitCen is revealed because it is able to bundle all pieces of information from all Member States and can additionally build on own experience and observations.[218] Moreover - because its service products are tailored for the EU decision-making process - no national agency would have been willing to do so or it would

[212] Shapcott, ibid.

[213] Müller-Wille (2008). An overview of the further structures within the Council dealing with terrorism is provided for instance by Dittrich (2006), p. 26 and Bendiek (2006), p. 21.

[214] Müller-Wille (2008), p. 60.

[215] Monar (2005a), p. 10.

[216] Keohane (2005); Müller-Wille (2008), p. 61.

[217] Müller-Wille (2008).

[218] Bendiek (2006), p. 21.

not have been accepted by others.[219] Others see SitCen more critically, arguing that it has received a growing executive power and does in reality work comparable to EU agencies, but, in contrast to them, without legal basis. In addition, there is no parliamentary scrutiny. Thus, the SitCen appears in a shady light of democratic legitimacy and accountability.[220]

4.4.4.6 The Watchdog for Implementing EU Anti-terrorism Measures: The EU Counter-Terrorism Coordinator

"The European Council emphasises that a comprehensive and strongly coordinated approach is required in response to the threat posed by terrorism. The European Council accordingly agrees to the establishment of the position of a Counter-Terrorism Co-ordinator". With these words, the heads of EU states and governments created the institution of the EU Counter-Terrorism Coordinator (CTC).[221] The creation of the post is a direct response to the plots in Madrid on 11 March 2004, which revealed two major deficits of the Union's fight against terrorism. First, so reads the Declaration of the European Council of 25 March 2004, a lot of measures agreed on at the Union's level had not been implemented in the EU Member States. Second, flaws in the practical cooperation still existed, because, for instance, Spanish authorities did not know about the suspects involved in the bombings of Madrid, although the suspects were already known to other Member States' secret services.

Against this background, the CTC was mandated to co-ordinate the work of the Council in combating terrorism and, with due regard to the responsibilities of the Commission, maintain an overview of all the instruments at the Union's disposal with a view to regular reporting to the Council and effective follow-up of Council decisions. The CTC works within the Council Secretariat and is directly subordinated to the Secretary-General of the Council (and the High Representative for the Common Foreign and Security Policy, Javier Solana. The office holders to date (Mr. Gijs de Vries until 2007, and currently Mr. Gilles de Kerchove) filled in the role of the CTC, inter alia, by monitoring regularly the implementation of the EU Action Plan on Combating Terrorism, producing policy papers, help précising the EU's counter-terrorism strategy, and securing the visibility of the Union's policies in the fight against terrorism, in particular by travelling to third countries where the CTC communicates the EU counter-terrorism policy. The position of the CTC is therefore restricted to be a coordinator of the counter-terrorism policies at the EU level, to be an advisor to the EU institutions and Member States, and finally to be a "counter-terrorism" representative towards media and third countries.

[219]Müller-Wille (2008), p. 61.

[220]Den Boer et al. (2008), p. 115.

[221]Declaration on Combating Terrorism of 25 March 2004.

The CTC neither has rights to initiatives nor decision-making powers nor an own budget.[222] The CTC is further neither entitled to oblige Member States to provide information to the EU bodies nor coordinate individual Member States' national counter-terrorism structures or operations, but is only able to "shame and name" laggard Member States.[223]

4.4.5 External Acquis Anti-terrorisme

Already, in the first reactions to the attacks of 9/11, the EU stressed that it will integrate the fight against terrorism into all aspects of the EU's external policy.[224] The EU assigned itself a role on the international stage to help prevent and prosecute terrorist acts. In parallel to the previously mentioned measures, the EU used its external relations instruments to pursue counter-terrorism objectives. Here, two strands of work have been crystallised. The first is the development of external action in the domain of justice and home affairs cooperation with third countries – most importantly with the United States. The second is a combination of the application of instruments of the second pillar (CFSP) and its military ancillary, the European Defence and Security Policy (ESDP), together with the use of external economic instruments provided for in the first pillar (cross-pillarisation of anti-terrorism objectives).[225]

4.4.5.1 EU–US Relations as an Example for the External Dimension of Justice and Home Affairs

Since 2001, the EU has developed specific forms of cooperation in its relations to other partners (e.g. Russia), focusing on intensified dialogue on justice and home affairs. However, the most significant evolution in this regard was the cooperation with the USA after the attacks of 9/11/2001. Although terrorism had been on the agenda on the transatlantic cooperation prior to this date, not much had been achieved other than a general exchange of information. The main reasons were reservations of some EU Member States and the European Parliament regarding the differences on the level of protection of personal data, different practices of police work, and the different criminal law systems in the USA. After 9/11, the EU demonstrated its solidarity with the USA mainly by increased cooperation in the domains of justice and home affairs. In addition to actions including the common

[222] Bendiek (2006), p. 19; Spence (2007a) p. 17f.; Monar (2005a), p. 10.

[223] Dittrich (2005), p. 30; Bossong (2008b), p. 7.

[224] Cf. Council Doc. SN 140/01 and Council Conclusions on the EU external action against terrorism of 22 July 2002, Council Doc. 10945/02 (Presse 210).

[225] For this distinction, see Monar (2008), p. 219.

drafting of threat assessments, the granting of access of US representatives to relevant EU counter-terrorism working groups and committees, the exchange of liaison officers, and close cooperation via dialogues on issues such as border control, airport, and airline security or container security, etc.,[226] three principal cooperation agreements on law enforcement should be highlighted here:

1. On 6 December 2001, the USA fulfilled its longstanding desire to get access to Europol data: The USA and Europol concluded an agreement that allows the exchange of "strategic and technical" information. The transmission of data related to an identified individual or identifiable individuals, i.e. personal data, was excluded.[227] After partly difficult negotiations, both parties agreed on a supplementary agreement in December 2002 that includes the exchange of personal data between Europol and "competent US federal, state or local authorities".[228] Until the final signature, this agreement came across with concerns from national parliaments and data protection commissioners. The main concerns were that the USA did not (and still does not) provide for a comprehensive data protection law, not to mention a central data protection office; the agreement leaves open a wide list of US authorities that may receive Europol data; and the agreement does not provide for any data protection rules specifying the rights of the data subject.[229] Most striking is that the agreement also allows, under certain conditions, for the exchange of sensitive data, i.e. personal data revealing race, political opinions, or religious or other beliefs, or concerning health and sexual life (Art. 6) - actually a tabu under European data protection law.
2. Not less difficult proved the conclusion of two agreements in the domain of judicial cooperation. On 23 June 2003, the EU and the USA signed two agreements on extradition and mutual legal assistance.[230] First, it was doubtful whether the EU can conclude such agreements with the USA because the EU has no legal personality (see Sect. 4.2). However, these concerns were set aside by finally basing the agreement on both second and third pillar provisions (Art. 24 and 38 TEU). Second, as regards the extradition treaty, objections were raised, inter alia, whether a nod can be given to extraditions of European citizens to a country that still carries out the death penalty and applies military jurisdiction, which does not correspond to European ideas of law and order. As regards the mutual legal assistance agreement, misgivings were expressed that the agreement waters down data protection rules and paves the way for self-regulating joint investigation teams.[231]

---

[226] For transatlantic cooperation measures, see Cameron (2007), p. 135; Monar (2004), p. 157.

[227] http://www.europol.europa.eu/legal/agreements/Agreements/16268–2.pdf (last visited July 2009). The agreement also provides for the assignment of liaison officers and the exchange of expertise.

[228] http://www.europol.europa.eu/legal/agreements/Agreements/16268-1.pdf (last visited July 2009).

[229] Peers (2002); Monar (2004), p. 158.

[230] OJ L 181 of 19 July 2003 p. 27 and 34, respectively.

[231] Cf. Report of MEP Jorge Salvador Hernández Mollar, A5-0172/2003 of 22 May 2003; Holzberger (2003), p. 91.

The extradition treaty makes extraditable every offence that is punishable under the law of the requesting and requested States by deprivation of liberty for a maximum period of more than 1 year or by a more severe penalty. Thus, the extradition between EU Member States and the USA is not limited to terrorist offences or organised crimes only – again a reminder of the general strand of EU legislation to cover criminal offences to a wide extent. Art. 13 of the extradition agreement stipulated that for persons extradited by an EU Member State to the USA, the death penalty shall not be imposed or carried out. However, an equivalent clause is lacking in the treaty on mutual legal assistance, thus allowing for assistance in which the offender may face a death penalty. The agreement on mutual legal assistance contains several innovative provisions, including allowance of authorities' access to bank information, the formation and operation of joint investigation teams, the use of video conferencing for testimony, and mutual legal assistance to administrative authorities.

3. With the third, and arguably the most controversially discussed agreement, the EU meets US policy on tightened border controls. In 2004, the EU concluded a first agreement that obliges Europe's airlines to provide the United States border security authority with electronic access to the data contained in their reservation and departure control system (Passenger Name Records [PNR]). The agreement was replaced by a new interim agreement in 2006 after the European Court of Justice annulled the 2004 agreement because it was erroneously based on the first pillar instead of the third pillar. Finally, in 2007, the EU and the USA reached a deal on a long-term PNR agreement on the processing and transfer of PNR data by air carriers to the US Department of Homeland Security (DHS).[232] The data will be used for the purposes of preventing and combating terrorism and related crimes as well as other serious crimes that are transnational in nature, including organised crime. The USA was successful in its demands to keep data for a longer period of time and to be able to pass on the data to other US authorities without tight restrictions. The DHS now may store data in "an active analytical database for 7 years after which time the data will be moved to dormant non-operational status" for a further 8 years. In fact, data can be retained for 15 years. Under the 2004 agreement, access to PNR data was limited for a period of 3.5 years and the data were even destroyed after that period if they had not been manually accessed during that period of time.

The objections against the "EU–US PNR deal" are manifold. Most concerns are put forward in view of infringements of European data protection principles. The European Parliament, for instance, in a resolution examining the 2007 agreement, regrets that the agreement is "substantively flawed in terms of legal certainty, data protection and legal redress for EU citizens, in particular as a result of open and vague

[232]For details, see Wahl (2007a), p. 9; Wahl (2006c), p. 48, and Wahl (2006a), p. 3f. with Internet link references to the agreements.

definitions and multiple possibilities for exceptions". The Members of the European Parliament further state that the new deal fails to offer an adequate level of data protection and lacks democratic oversight because it has been concluded without any involvement of parliaments.[233] The European Data Protection Supervisor denied the regime by opposing the extension of the time that passenger data is kept – effectively increasing from 3.5 to 15 years in all cases - introducing a concept of "dormant" data that is without precedence. He further criticised the accessibility of the data to a broad range of US agencies, and the absence of an effective redress mechanism of EU citizens to challenge the misuse of their personal data.[234]

4.4.5.2 Anti-terrorism Foreign Policy with the Means of the Second and First Pillars

The instruments of the Common Foreign and Security Policy (second pillar) were mainly used by the EU to make a contribution to the formation of the international coalition against terrorism. High on the agenda after the attacks of 9/11 were the systematic use of political dialogues with third countries (e.g. China and India) or groups with third countries (such as EUROMED, ASEM, and the Gulf Cooperation Council). In the meetings, the EU above all urged the international partner to quickly adopt measures against the financing of terrorism. The fight of terrorism is also an aspect of the EU's enlargement and neighbourhood policy. Applicant countries for accession (such as Bulgaria, Romania, Turkey, and Croatia); EFTA countries, such as Iceland and Liechtenstein; and other countries such as the Ukraine and Moldova have been obliged to adapt their national anti-terrorism policies to the EU anti-terrorism policy. At the multilateral level, the EU has been actively involved in the work of international bodies, such as the UNCTC, UNODC, OSCE, and FATF.

On the military side, however, the EU was not capable of using its European Security and Defence Policy (ESDP) as a reactive tool against terrorism to the plots of 9/11. Member States were not ready to agree on a Rapid Reaction Force, because, on the one hand, ESDP structures were not well developed by that time, and, on the other hand, there was too much disagreement among the Member States regarding the military intervention of the USA and of the UK in Afghanistan.[235] Reinforced by the attacks of Madrid, the EU has made headway in including the ESDP in its counter-terrorism programme by making the ESDP more operative (e.g. the possibility of using military means in the fields of CBRN, protection of soldiers and EU citizens in foreign countries, and equipment support),[236] although it has not been proven in real crises situations yet.

---

[233]For the main concerns in more detail, see Wahl (2007a), p. 10 with further reference.

[234]Wahl, ibid, with further reference.

[235]Den Boer and Monar (2002), pp. 15 ff.

[236]Bendiek (2006), p. 24.

First pillar instruments have been used, for example, to help establish adequate counter-terrorism infrastructures in certain third countries by technical and financial support from the EU. Instruments such as preferential trade quotas are utilised to support moderate political leaders in countries with a high potential of terrorist recruitments (e.g. Pakistan). External economic relationships of the EU to third countries have been increasingly influenced by terrorism. Since 2002, the EU systematically has inserted anti-terrorism clauses into many trade cooperation and association agreements with third countries. The clauses set forth cooperation in preventing and repressing terrorist acts, as required by UN Security Council resolution 1373, and on sharing information and expertise. However, the main flaw of the clauses is that they do not entail consequences, i.e. their non-respect does not lead to a suspension of the agreements.[237]

4.5 Concluding Remarks and Perspectives

The aforementioned external action, among other things, let the EU appear to be an independent, self-determined, counter-terrorism actor vis-à-vis third countries and international organisations, notably the USA and the UN. The EU, for instance, was able to enter into agreements with the USA on behalf of its Member States or to second own EU officials to UN missions what let appear the EU a seemingly uniform organisation. The EU's own power has been further made visible by enacting the freezing of assets of individuals as part of the UN Resolution 1373 via directly applicable EC Regulations. In addition, other issues presented in this paper "are a forcible reminder to the public that the EU is far more than a powerful economic organisation and has already made a valuable contribution to protecting its citizens from the scourge of terrorism".[238] Examples are the counter-terrorism strategy (which is unique on the international stage), the finding of a common terrorism definition through the Framework Decision on Combating Terrorism, the quantum leap in judicial cooperation through the European Arrest Warrant, the provision of "technical assistance" for law enforcement through the data retention Directive, the safety device of passports through the inclusion of biometrics data, the establishment of its own structures of analytical and tactical assessments through central entities like Europol and SitCen, etc.

However, these arguments cannot disguise that there are several deficits that reinforce the impression that the EU's counter-terrorism activity remains a "paper tiger".[239] The main flaws are briefly sketched in the following, before examining whether the new reform treaty of Lisbon may entail an essential change in the future.

---

[237] Spence (2007a), p. 23; see also Keohane (2005), p. 34, who points out the vagueness of the clauses make them meaningless.

[238] Wilkinson (2005), p. 37.

[239] Bures (2006).

The first, arguably most striking deficit, is that there is a gap between the laws we pass and their effect in practice, which does not render Europe safer.[240] The main reason is that the bulk of legal measures must be implemented by the Member States, and EU institutions have rather limited possibilities to ensure effective and timely enforcement, especially because most measures are taken within the intergovernmentally structured third and second pillars. *The list of delayed and inadequate implementation* of described EU's counter-terrorism measures since 2001/2002 could be drafted almost ad infinitum. To name only a few examples relating to the so-called flagships of EU's post 9/11 actions:

By the end of March 2004, i.e. in the month of the attacks of Madrid, only 10 out of the then 15 old Member States finalised their national legislation process for implementation of the FD on Combating Terrorism, which had actually to be implemented by 31 December 2001. In 2004, the Commission concluded that only three of the old Member States appear to have entirely fulfilled the obligation emerging from the FD, and yet, in 2007, the Commission found that key elements of the Framework Decision, such as the criminalisation of the terrorist offences (Art. 1) and the harmonisation of penalties relating to terrorist groups (Art. 5 (3)) are still deficiently implemented in several Member States.[241]

The list of legal deficiencies regarding the European Arrest Warrant is even longer. The EAW has been revealed as a model example for a very uneven and inadequate implementation (not to mention the fact that only half of the Member States met the envisaged deadline for transposition by 31 December 2003). The EAW mainly illustrates that diverse legal traditions collide with the requirements of EU framework decisions in the area of freedom, security and justice. Several Member States had to revise their implementation law after collisions with their constitutions came out, in particular as regards the abolishment of the "non-extradition of own nationals rule". Other Member States introduced unforeseen elements regarding the grounds for refusals, implemented optional grounds for refusals as mandatory ones, or even maintained/reintroduced grounds for refusals that the EAW thought to have eliminated.[242]

Joint Investigation Teams "have so far not lived up to the high expectations", their operational benefit as a tool for countering international terrorism – in particular Islamic terrorism – could not be assessed – now, more than 6 years after its coming into existence.[243] The instrument remained on paper for a long time. By the end of December 2005, three old Member States could still not report successful legal implementation and the Commission had to state in January 2005 that only the legislation of 1 Member State (out of the 19 Member States whose legislation was examined) fully complied with the FD on Joint Investigation Teams.[244]

---

[240] In this sense Gijs de Vries in: Le Monde, 18 May 2004.

[241] Cf. COM(2004) 409 and Commission Staff Working Paper SEC(2004) 688 as well as COM(2007) 681 plus Commission Staff Working Document SEC(2007) 1463.

[242] Cf. reports of the Commission on the EAW: COM(2005) 63; COM(2006) 8; COM(2007) 407.

[243] For the problems in connection with the operational use of JITs, see Rijken (2006), p. 99.

[244] COM(2004) 858 of 7 January 2005.

Not much has changed until today as demonstrate the annexes of the 6-month reports of the CTC on the implementation of the EU's Counter Terrorism Action Plan.[245] It is thus obvious that for the EU to be a strong actor in the fight against terrorism remains very dependent on the will (and willingness) of its Member States, and that the EU is lacking muscular mechanisms to enforce its policy. This fate is further mirrored as regards the vertical cooperation between the national authorities and EU bodies. Essentially held evolutions have been far beyond timely implementation, such as Europol's possibility of taking part in Joint Investigation Teams (4½ years after ratification of the relevant protocol). In 2005, two of the old Member States (Spain and Greece) had still failed to adopt the necessary legislation to implement the Decision setting up Eurojust; in addition, the Member States' transposing laws differ considerably and are considered far from satisfactory, which hampers the effectiveness of Eurojust's activity.[246]

On the practical side, Europol and Eurojust have faced reluctance from the part of national authorities for cooperation. The two bodies are struggling with the persistent problem that Member States' authorities often delay transferring or even do not pass information – an incomprehensible fact especially in view of Europol, which was elected the EU's lead institution for counter-terrorism analysis.[247] The EU is also in a very weak position as a hub of sharing intelligence. Although the EU may be the only international organisation today that has the institutional infrastructure to play a central role in the development of international and cross-agency intelligence cooperation, intelligence data go through Europol and SitCen only to a very minor extent.[248] Main reasons for not sharing essential counter-terrorism information with EU bodies are arguably the lack of mutual trust, together with more cooperation on the ground.[249]

The discrepancy between the "EU paper" and application of the instruments at the national levels calls into question the credibility of the EU's counter-terrorism strategy. Against the just-mentioned background, in addition, questionable *effectiveness* of the EU's counter-terrorism work[250] – the second deficit - undermines EU's credibility. In general, most striking is that there is hardly any empirical research on the question of whether the single measures have delivered a significant contribution to the fight against terrorism or on how effective cooperation has turned out in practice in terrorist cases.[251] As we have seen above, the effectiveness of many instruments hitherto can be doubted, such as the combat of terrorism financing with

[245] Council doc. 15912/08 ADD 1 of 19 November 2008.

[246] Eurojust Annual Report 2005; Council Doc. 7318/06, p. 13; COM(2004) 457.

[247] Council doc. 7868/06 of 29 March 2006; House of Lords Report (2005), mn. 63.

[248] Müller-Wille (2008), p. 69; Dittrich (2005), p. 29.

[249] Council doc. 7868/06, p. 4; Dittrich (2005), p. 33; Müller-Wille (2008), p. 57.

[250] Knelangen (2008), p. 107; Reinisch (2004).

[251] For the problem of a lack of empirical research concerning police cooperation and terrorism, Fijnaut (2004), pp. 272f. The view on police cooperation can certainly generally be transferred to the other EU counter-terrorism measures. See also Knelangen (2008), p. 115. Keohane (2005), p. 38, points out that the EU's security policies (internal and external) are young and relatively untested, and that citizens must still be convinced about the effectiveness of the EU's counter-terrorism policies.

the means of money laundering (because the phenomena differ on ground); the combat of cybercrime with EU measures (because the phenomenon has remained fictitious so far); or the exertion of tighter border controls (because catching terrorists at the EU's (external) borders is rather marginal).[252]

Doubts on the effectiveness are further caused by the EU's anti-terrorism structures at the horizontal level. The EU's counter-terrorism venue at the horizontal level was entitled a "crowded policy area",[253] consisting of several council working groups and committees (TWG, COTER, Art. 36 Committee = CATS, SCIFA, PSC, WP on Civil Protection, etc.), Council units (e.g. SitCen, CTC), bodies (e.g. Europol with the CTTF), Commission Directorate-Generals (notably JLS), informal fora (e.g. PCTF, Heads of Security and Intelligence Services), etc. There is no single, strong EU body that deals with all aspects of terrorism taking a comprehensive view on the cross-institutional and the cross-pillar aspects of the EU's anti-terrorism efforts. As a consequence, the EU lapses into tremendous coordination efforts, hampering the EU's functionality in this area. The CTC, who could ensure inter-institutional interaction, has a difficult stand because, from the outset, the CTC has faced inherent limitations of the post; cooperation with the other Council structures has remained outside the given mandate; and acceptance from the part of many Member States' governments and the Commission has been lacking.[254]

Ultimately, as a third deficit, the *EU's pillar structure* is a self-inherent brake for effective and robust counter-terrorism work. We have seen that the legal bases for several counter-terrorism measures are not clear at all, prompting the European Court of Justice to enter the scene for clarification. This was the case, for example, for the EU's scheme of freezing assets, the EU–US PNR agreement, and the 2006 data retention Directive. In addition, flaws inherent to the third pillar, which has dominated EU's activities hitherto, undermined credibility as well as accountability of the EU as a powerful counter-terrorism actor. Decision-making in the Council is cumbersome and lengthy because of the unanimity requirement. Furthermore hard battles on single issues are fought because of different priority settings and legal cultures in the national orders. Democratic control is considered low because national parliaments have in effect minor influence, and the European Parliament remains often "outside" with its non-binding legislative resolutions, not to mention the not mandatory consultation of the European Data Protection Supervisor. Weak parliamentary control and independent data protection oversight naturally raise questions of legitimacy and accountability of the EU's "executive third pillar measures". As indicated in the overview of the measures, doubtful compliance of some EU measures with human rights further reduce legitimacy.[255]

---

[252] Bossong (2008b), p. 15.

[253] Den Boer (2003b), p. 15. See also the Report of the House of Lords (2005), p. 27, which emphasises: "In an area where clarity of roles and responsibilities is vital, we found the structures within the EU for combating terrorism complex and confusing. Although some of our witnesses promised us a map of all the interlocking and overlapping groups, no one was able to produce one".

[254] Spence (2007a), p. 17f; Keohane (2005), p. 19.

[255] The human rights aspect cannot be deepened here, this is why reference must be made to special legal literature.

It is questionable whether the presented deficits will be remedied by the *Lisbon Treaty*, which, once ratified by all 27 EU Member States, will herald the next step of the European unification process. On the one hand, new legal features will be introduced that will strengthen the power of the EU: The European Union will get a single legal personality and will replace the European Community. The new Treaty puts an end to the controversial pillar divide by integrating police and judicial cooperation in criminal matters (the existing "third pillar") into the regime of the Treaty of the European Community. This means principally the application of the "Community method" to all justice and home affairs issues, the application of the ordinary legislative procedure, and unrestricted judicial control of the legislative acts by the European Court of Justice. In particular, the European Parliament and the Council will jointly adopt regulations, directives, and decisions for criminal law issues and policing. National Parliaments will get formally involved in the decision-making process. The Commission can bring forward infringement procedures if Member States fail to implement justice and home affairs legislation.

The Treaty also promises reinforced action of the EU to counter terrorism within the CFSP. The ESDP is strengthened because the tasks of the ESDP may now also be used for contributions to the fight against terrorism, including the support of third countries in combating terrorism in their territories (Art. 43 TEU). The shift towards the increasing use of military means to combat terrorist threats is also demonstrated in the "solidarity clause" (Art. 222 TFEU), which stipulates that the Union (and the Member States) shall assist a Member State that is the object of a terrorist attack by mobilising all the instruments at its disposal, including the military resources made available by the Member States.

On the other hand, Member States retain intergovernmental elements in a decisive way. Inter alia, Member States pushed through a 5-year transitional period within which existing measures of policing and criminal law that were adopted under the current treaties may not be subject to the powers of the Commission to initiate infringement proceedings and to the full jurisdiction of the European Court of Justice. In the fields of acts on mutual recognition, police and judicial cooperation in criminal matters, and approximation of criminal laws, the Member States compensated their right to veto in the third pillar by "emergency brake clauses" that allow the suspension of qualified majority voting in the Council if a Member State considers a legislative proposal "affecting fundamental aspects of its legal system". In addition, the intergovernmental character of CFSP remains relatively untouched by the reform.

The Lisbon Treaty will also not eradicate main dilemmas of the EU in the counter-terrorism policy, in particular its further dependence on the will and willingness of Member States and its rather weak position to enforce its authority vis-à-vis its Member States. It can be expected that Member States continue to perceive the Union a *cadre priviligé de cooperation*, as they have done hitherto. This perception corresponds to the current structure of the EU as argued for introductorily, i.e. the European Union as a special forum for Member States to form their will and make decisions. Thus, the EU will remain caught in a "policy pendulum" that moves between extreme reluctance to share counter-terrorism powers with EU

institutions and eagerness to gradually establish a more integrative approach towards anti-terrorism cooperation.[256]

A possible way out of this pendulum could be that the EU compiles its achieved specific "counter-terrorism *acquis*" in a single framework, because, as we have seen in Sect. 4.4, Member States were less reluctant when it came to instruments specifically designed to counter terrorism, but problems occurred when instruments were extended from terrorism to cover all (serious) criminal offences. A compendium of the EU's counter-terrorism acquis will further increase visibility of the EU and transparency towards EU citizens. The compilation should be accompanied with a consolidation of the framework taking into account the effectiveness of the measures and their compliance with fundamental rights guarantees.

References

Al-Jumaili, D. (2008). Stationen im Kampf gegen die Terrorismusfinanzierung – New York – Brüssel - Berlin, *Neue Juristische Online Zeitschrift (NJOZ)* 8, 188–211.

Alvaro, A. (2005). Positionspapier zur Einführung einer Vorratsspeicherung von Daten, *Recht der Datenverarbeitung (RDV)* 47–50.

Anderson, M., Den Boer, M., Cullen, P., Gilmore, W., Raab, C., Walker, N. (1995). *Policing the European Union*. Oxford: Oxford University Press.

Balzacq, T. (2008). The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies, *Journal of Common Market Studies (JCMS)* 46, 75–100.

Balzacq, T., Carrera, S. (2005). The EU's Fight Against International Terrorism – Security Problems, Insecure Solutions, *Centre for European Policy Studies (CEPS) Policy Brief No. 80, July 2005*.

Bartelt S., Zeitler H. E. (2003). "Intelligente Sanktionen" zur Terrorismusbekämpfung in der EU, *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)* 14, 712–717.

Bauer, M., Algieri, F. (2006). Viel erreicht, aber noch mehr zu tun: Die Vielschichtigkeit europäischer Maßnahmen zur Bekäömpfung des Terrorismus. In E. Müller, P. Schneider (eds.), *Die Europäische Union im Kampf gegen den Terrorismus: Sicherheit vs. Freiheit?* Baden-Baden: Nomos.

Bendiek, A. (2006). Die Terrorismusbekämpfung der EU, *Stiftung Wissenschaft und Politik: SWP-Studie 21*, *August 2006*.

Blanke, H.-J. (2007). EUV Art. 2. In C. Calliess, M. Ruffert (eds.), *Kommentar zum EU-Vertag und EG-Vertrag*. 3rd ed. Munich: Beck.

Bossong, R. (2008a). The Action Plan on Combation Terrorism: A Flawed Instrument of EU Security Governance, *Journal of Common Market Studies (JCMS)* 46, 27–48.

Bossong, R. (2008b). The EU's Mature Counterterrorism Policy – A Critical Historical and Functional Assessment, *LSE Challenge Working Paper, June 2008*.

Breyer P. (2007). Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, *Strafverteidiger (StV)* 214–220.

Bruggemann, W. (2004). Countering the Threat of Terrorism in the EU in a Broader Organised Crime Perspective. In C. Fijnaut, J. Wouters, F. Naert (eds.), *Legal Instruments in the Fight Against International Terrorism*. Leiden: Nijhoff.

Büllingen, F., Gillet, A., Gries, C-I., Hillebrand, A., Stamm P. (2004). *Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich*. (Bad Honnef: WIK). www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf

[256] Cf. Den Boer (2003b), p. 22.

Bunyan T. (1995). The Europol Convention, London: *A Statewatch publication*.
Bunyan, T. (2002). The "War on Freedom and Democracy", *Statewatch analysis, September 2002*.
Bunyan, T. (2005). While Europe Sleeps…, *European Civil Liberties Network, Essays for civil liberties and democracy in Europe*.
Bunyan, T. (2006). The EU's Police Chief Task Force (PCTF) and Police Chiefs Committee, *Statewatch analysis March 2006*.
Bures, O. (2006). EU Counterterrorism Policy: A Paper Tiger? *Journal of Terrorism and Political Violence* 18, 57–78.
Bures O. (2008). Europol's Fledging Counterterrorism Role, *Journal of Terrorism and Political Violence* 20, 498–517.
Burghardt, G., Tebbe, G., Marquardt S. (2003/2004). Art. 11 EUV. In H. von der Groeben, J. Schwarze (eds.), *Kommentar zum EU-/EG-Vertrag*. 6th ed. Baden-Baden: Nomos.
Cameron F. (2007). Transatlantic Relations and Terrorism. In D. Spence (ed.), *The European Union and Terrorism*. London: Harper Publishing.
Coninsx, M. (2004). Eurojust and EU Judicial Cooperation in the Fight against Terrorism. In C. Fijnaut, J. Wouters, F. Naert (eds.), *Legal Instruments in the Fight Against International Terrorism*. Leiden: Nijhoff.
Dannecker G. (2007). Die Entwicklung des Wirtschaftsstrafrechts unter dem Einfluss des Europarechts. In H-B. Wabnitz, T. Janovsky (eds.), *Handbuch des Wirtschafts- und Steuerstrafrechts*. Munich: Beck.
Deflem, M. (2006). Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective, *Justice Quarterly* 23, 336–359.
De Kerchove, G. (2004). L'action de l'Union Européenne en matère de lutte contre le terrorisme, *Revue du Marché commun et de l'Union européenne*, n° 480, 421–424.
Delpech, T. (2002). International Terrorism and Europe, *Chaillot Paper n° 56, December 2002*.
Demaret, P. (1994). The Treaty Framework. In D. O'Keefe, P. Twomey (eds.), *Legal Issues of the Maastricht Treaty*. New York: Chancery Law Publishing.
Den Boer, M. (2003a). The EU Counter-Terrorism Wave: Window of Opportunity or Profound Policy Transformation? In M. van Leeuwen (ed.), *Confronting Terrorism: European Experiences, Threat Perceptions and Policies*. Den Haag: Kluwer Law International.
Den Boer, M. (2003b). 9/11 and the Europeanisation of Anti-Terrorism Policy: A Critical Assessment, *Notre Europe Policy Papers No 6, September 2003*.
Den Boer, M., Monar J. (2002). Keynote Article: 11 September and the Challenge of Global Terrorism to the EU as a Security Actor, *Journal of Common Market Studies (JCMS)* 40, 9–28.
Den Boer, M., Hillebrand C., Nölke A. (2008). Legitimacy under Pressure: The European Web of Counter-Terrorism Networks, *Journal of Common Market Studies (JCMS)* 46, 101–124.
Dittrich, M. (2005). Facing the Global Terrorist Threat. A European response, *European Policy Centre (EPC) Working Paper N° 14, January 2005*.
Dittrich, M. (2007). Radicalisation and Recruitment: The EU Response. In D. Spence (ed.), *The European Union and Terrorism*. London: John Harper Publishing.
Dörr, O. (1995a). Zur Rechtsnatur der Europäischen Union, *Europarecht (EuR)*, 334–348.
Dörr O. (1995b). Noch einmal: Die Europäische Union und die Europäischen Gemeinschaften, *Neue Juristische Wochenschrift (NJW)* 3162–3165.
Douglas-Scott, S. (2004). The Rule of Law in the European Union – Putting the Security into the Area of Freedom, Security and Justice, *European Law Review (ELRev)* 29, 219–242.
Drake H. (2000). *Jacques Delors*: *A Political Biography*. New York: Routledge.
Dubois D. (2002). The Attacks of 11 September: EU-US Cooperation Against Terrorism in the Field of Justice and Home Affairs, *European Foreign Affairs Review* 7, 317–335.
Dumitriu, E. (2004). The EU's Definition of Terrorism: The Council Framework Decision on Combating Terrorism, *German Law Review* 5, 585–602.
Eaton, M. R. (1994). Common Foreign and Security Policy. In D. O'Keefe, P. M. Twomey (eds.), *Legal Issues of the Maastricht Treaty*. New York: Chancery Law Publishing.

Edwards, G., Meyer, C. O. (2008). Introduction: Charting a Contested Transformation, *Journal of Common Market Studies (JCMS)* 46, 1–25.
Ekengren, M. (2007). Terrorism and the EU: The Internal-External Dimension of Security. In D. Spence (ed.), *The European Union and Terrorism*. London: Harper Publishing.
Fijnaut, C. (2004). Police Co-operation and the Area of Freedom Security and Justice. In N. Walker (ed.), *Europe's Area of Freedom, Security and Justice*. Oxford: OUP.
Frattini, F. (2006). Internal and External Dimension of Fighting Against Terrorism. In E. Müller, P. Schneider (eds.), *Die Europäische Union im Kampf gegen den Terrorismus: Sicherheit vs. Freiheit?* Baden-Baden: Nomos.
Georgopoulos, T. (2005). What kind of Treaty Making Power for the EU? *European Law Review (ELRev)* 30, 190–208.
Gercke, M. (2005). Der Rahmenbeschluss über Angriffe auf Informationssysteme, *Computer und Recht (CR)* 468–472.
Glaeßner, G. J., Lorenz, A. (2005). Europa und die Politik der inneren Sicherheit. In G.-J. Glaeßner, A. Lorenz (eds.), *Europäisierung der inneren Sicherheit*. Wiesbaden: Vs Verlag.
Gueydan, C. (1997). Cooperation Between Member States of the European Community in the Fight Against Terrorism. In R. Higgins, M. Flory (eds.), *Terrorism and International Law*. New York: Routledge.
Guild, E. (2008). The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the 'Terror Lists', *Journal of Common Market Studies (JCMS)* 46, 173–193.
Gusy, C. (2005). Möglichkeiten und Grenzen einer europäischen Antiterrorpolitik, *Goltdammers Archiv für Strafrecht (GA)* 152, 215–227.
Hecker B. (2007). *Europäisches Strafrecht*, 2nd ed. Berlin: Springer.
Herzog F., Hoch, T. (2007). Politisch exponierte Personen unter Beobachtung, *Wertpapiermitteilungen Zeitschrift für Wirtschafts- und Bankrecht (WM)* 1997–2003.
Hetzer W. (2008). Geldwäsche und Terrorismusfinanzierung, *Kriminalistik* 468–475.
Hill, C. (2004). Renationalizing or Regrouping? EU Foreign Policy Since 11 September 2001, *Journal of Common Market Studies (JCMS)* 42, 143–163.
Holzberger, M. (2003). Auslieferungs- und Rechtshilfeübereinkommen mit den USA, *Bürgerrechte & Polizei/ CILIP* 75, 91–92.
Holzberger, M. (2006). Europols kleine Schwester, Die Europäische Grenzschutzagentur "Frontex", *Bürgerrechte & Polizei/CILIP* 84, 56–63.
Hörmann, S. (2007). Die Befugnis der EG zur Umsetzung von Resolutionen des UN-Sicherheitsrates zur Bekämpfung des internationalen Terrorismus, *Europarecht (EuR)* 120–132.
Horspool, M., Humphreys M. (2007). *European Union Law*. 5th ed. Oxford: OUP.
House of Lords (2005). European Union Committee, 5th Report of Session 2004–05, *After Madrid: the EU's response to terrorism*.
Jahn S. (2006). Die Europäische Grenzschutzagentur, *Die Polizei* 207–211.
Jimeno-Bulnes, M. (2004). After September 11th: The Fight Against Terrorism in National and European Law, *European Law Journal* 10, 235–253.
Joffé, G. (2008). The European Union, Democracy and Counter-Terrorism in the Maghreb, *Journal of Common Market Studies (JCMS)* 46, 147–171.
Jour-Schröder, A., Wasmeier, M. (2003/2004). Vorbem zu den Artikeln 29 bis 42 EUV. In H. von der Groeben, J. Schwarze (eds.), *Kommentar zum EU-/EG-Vertrag*. 6th ed. Baden-Baden: Nomos.
Kaiafa-Gbandi, M. (2006). Recent Developments in Criminal Law in the EU and Rule-of-Law Deficits. In B. Schünemann (ed.), *A Programme for European Criminal Justice*. Köln: Carl Heymanns Verlag.
Karayigit, M. T. (2006). The Yusuf and Kadi Judgments: The Scope of the EC Competences in Respect of Restrictive Measures, *Legal Issues of Economic Integration* 33, 379–404.
Keohane, D. (2005). The EU and Counter-Terrorism, *Centre for European Reform (CER) Working Paper, May 2005*.
Keohane, D. (2008). The Absent Friend: EU Foreign Policy and Counter-Terrorism, *Journal of Common Market Studies (JCMS)* 46, 125–146.

Kilchling, M. (2001). Eine Zauberformel, die den Terrorismus bannt? *MaxPlanckForschung* 4, 16–20.

Kilchling M. (2004). Financial Counterterrorism Initiatives in Europe. In C. Fijnaut, J. Wouters, F. Naert (eds.), *Legal Instruments in the Fight Against International Terrorism*. Leiden: Nijhoff.

Kilchling, M. (2006). Rechtliche Instrumente zur Bekämpfung der Terrorismusfinanzierung im internationalen Vergleich. In Gehl, G. (ed.), *Terrorismus – Krieg des 21. Jahrhunderts?* Weimar: Bertuch-Verlag.

Kleine, M. (2004). Die Reaktion der EU auf den 11. September, *Forschungsberichte Internationale Politik 31*. Münster et al.: LIT Verlag

Knelangen, W. (2006) Die innen- und justizpolitische Zusammenarbeit der EU und die Bekämpfung des Terrorismus. In E. Müller, P. Schneider (eds.), *Die Europäische Union im Kampf gegen den Terrorismus: Sicherheit vs. Freiheit?* Baden-Baden: Nomos.

Knelangen, W. (2008). Die Europäische Union: eine "starke Macht" im Kampf gegen den Terrorismus? In Peter Nitschke (ed.), *Globaler Terrorismus und Europa*. Wiesbaden: Vs Verlag.

Kotzur, M. (2006). Eine Bewährungsprobe für die Europäische Grundrechtegemeinschaft: Zur Entscheidung des EuG in der Rs. Yusuf u.a. gegen Rat, EuGRZ 2005, 592 ff, *Europäische Grundrechte-Zeitschrift (EuGRZ)* 19–26.

Marquardt S. (2003/2004). Vorbem. Art. 11 EUV. In H. von der Groeben, J. Schwarze (eds.), *Kommentar zum EU-/EG-Vertrag*. 6th ed. Baden-Baden: Nomos.

Mégie, A. (2004). Le 11 septembre: élément accélérateur de la cooperation judiciaire eurpéenne? *Les cahiers de sécurité intériere* 55, 91–120.

Messelken, D. (2003). Europas Antiterrorismus-Politik: Entstehung, Entwicklung, Perspektiven, *Berliner Transformationszentrum für Transnationale Sicherheit (BITS) Briefing Note 03.3 Dezember 2003*.

Meyer, F. (2007). Lost in Complexity – Gedanken zum Rechtsschutz gegen Smart Sanctions in der EU, *Zeitschrift für Europarechtliche Studien (ZEuS)* 1–69.

Meyer, F. (2008). EU Terrorism Lists in the Eye of the Rule of Law, *eucrim* 1–2, 81–88.

Mitsilegas, V., Gilmore, B. (2007). The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards, *International & Comparative Law Quarterly (ICLQ)* 56, 119–141.

Moiny, Y. (2005). Protection of Personal Data and Citizens' Rights of Privacy in the Fight against the Financing of Terrorism, *Centre for European Policy Studies (CEPS) Policy Brief No. 67, March 2005*.

Monar, J. (2004). Die EU und die Herausforderung des internationalen Terrorismus. In W. Weidenfeld (ed.), *Herausforderung Terrorismus. Die Zukunft der Sicherheit*. Wiesbaden: Vs Verlag.

Monar, J. (2005a). "Braucht die Europäische Union ein 'European Bureau of Investigation' (EBI) und eine ?European Intelligence Agency?" *Working Paper (Gutachten) Bertelsmann Stiftung*. Gütersloh: Bertelsmann.

Monar, J. (2005b). Die politische Konzeption des Raumes der Freiheit, der Sicherheit und des Rechts: Vom Amsterdamer Vertrag zum Verfassungsentwurf des Konvents. In Peter-Christian Müller-Graff (ed.), *Der Raum der Freiheit, der Sicherheit und des Rechts*. Baden-Baden: Nomos.

Monar, J. (2007). Common Threat and Common Response? The European Unions's Counter-Terrorism Strategy and its Problems, *Government and Opposition* 42, 292–313.

Muguruza, C. C. (2001). The European Union's Reaction to the Terrorist Attacks on the United States, Humanitäres Völkerrecht 14, 234–243.

Müller-Wille, B. (2004). For our eyes only? Shaping an Intelligence Community within the EU, *European Institute for Security Studies, Occasional Papers n° 50, January 2004*.

Müller-Wille, B. (2008). The Effect of International Terrorism on EU Intelligence Co-operation, *Journal of Common Market Studies (JCMS)* 46, 49–73.

Nehm, K. (2002). Ein Jahr danach – Gedanken zum 11. September 2001, *Neue Juristische Wochenschrift (NJW)*, 2665–2736.
O'Neill, M. (2008). A Critical Analysis of the EU Legal Provisions on Terrorism, *Terrorism and Political Violence 20*, 26–48.
Oppermann, T. (2005). *Europarecht*. 3rd ed. München: C.H. Beck.
Pastor-Nunoz, N. (2008), *eucrim* 1–2, 73–80.
Pechstein, M., Koenig C. (2000). *Die Europäische Union*. 3rd ed. Tübingen: Mohr Siebeck.
Peers, S. (2002). The Exchange of Personal Data Between Europol and the USA, *Statewatch analysis, 15 November 2002*.
Peers, S. (2003). EU Responses to Terrorism, *International and Comparative Law Quarterly (ICLQ)* 52, 227–243.
Peers, S. (2006). *EU Justice and Home Affairs Law*. 2nd ed. Oxford: OUP
Plachta, M. (2003). European Arrest Warrant: Revolution in Extradition? *European Journal of Crime, Criminal Law and Criminal Justice* 11, 178–194.
Plachta, M. (2005). Joint Investigation Teams, *European Journal of Crime*, *Criminal Law and Criminal Justice* 13, 284–302.
Reinisch, A. (2004). The Action of the European Union to Combat International Terrorism. In A. Bianchi (ed.), *Enforcing International Law Norms Against Terrorism*. Oxford: Hart Publishing.
Rhinhard, M., Boin, A., Ekengren, M. (2007). Managing Terrorism: Institutional Capacities and Counter-Terrorism Policy in the EU. In D. Spence (ed.), *The European Union and Terrorism*. London: Harper Publishing.
Rijken, C. (2006). Joint Investigation Teams: Principles, Practice, and Problems, *Utrecht Law Review* 2, 99–118.
Saurer, J. (2005). Die Ausweitung sicherheitsrechtlicher Regelungsansprüche im Kontext der Terrorismusbekämpfung, *Neue Zeitschrift für Verwaltungsrecht (NVwZ)* 275–282.
Schneider L. (2007). Commission Report on FIU Cooperation, *eucrim* 3–4, 97–98.
Schünemann B. (2003). Europäischer Haftbefehl und EU Verfassungsentwurf auf schiefer Ebene, *Zeitschrift für Rechtspolitik (ZRP)* 185–189.
Schünemann B. (2004). Fortschritte und Fehltritte in der Strafrechtspflege der EU, *Goltdammers Archiv für Strafrecht (GA)* 151,193–209.
Schweitzer, M., Hummer, W. (1996). *Europarecht*. 5th ed. Neuwied: Luchterhand.
Schweitzer, M., Hummer, W., Obwexer W. (2007). *Europarecht*. Wien: Manz.
Shapcott, W. (2005). "After Madrid: The EU's Response to Terrorism", *European Union Committee, 5th Report of Session 2004–05, Report with Evidence*, *March 2005*.
Sieber, U. (2006). International Cooperation against Terrorism use of the Internet, *Revue International de Droit Pénal* 77, 395–449.
Sieber, U. (2008), The Forces behind the Harmonisation of Criminal Law. In Delmas-Marty, M., Pieth, M., Sieber, U. (eds.), *Les chemins de l'harmonisation pénale/Harmonising Criminal Law.* Paris: Société de lègislation comparée.
Sieber, U. (2009), Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt. Eine Analyse der Vorfeldtatbestaende im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten". *Neue Zeitschrift fuer Strafrecht (NStZ)*, 353-364.
Sommer, U. (2005). Das Schnüffeln geht weiter, *Anwaltsblatt (AnwBl)* 50–52.
Spence, D. (2007a). International terrorism – in the Quest for a Coherent EU Response. In D. Spence (ed.), *The European Union and Terrorism*. London: Harper Publishing.
Spence, D. (2007b). The Continuing Quest for Coherence: Sovereignty Human Rights and EU Coordination. In D. Spence (ed.), *The European Union and Terrorism*. London: Harper Publishing.
Sugman, K., Jaeger, M. (2008). The Influence of Terrorist Events on the Development of EU Criminal Law. In Steven W. Becker, Davor Derenčinović (eds.), *International Terrorism: The Future Unchained?* Zagreb: University Press.
Stein, T., Meiser, C. (2001). Die Europäische Union und der Terrorismus, *Die Friedens-Warte* 76, 33–54.

Streinz, R. (2008), Europarecht. Heidelberg: C.F. Mueller.
Symeonidou-Kastanidou, E. (2004). Defining Terrorism, *European Journal of Crime, Criminal Law and Criminal Justice* 12, 14–35.
Szyszkowitz, T. (2005). The European Union. In K. von Hippel (ed.), *Europe Confronts Terrorism*. New York: Palgrave Macmillan.
Tempest, M. (2004). EU to Appoint Anti-terror tsar', *The Guardian*, 19 March 2004.
Tietje C., Hammelmann, S. (2006). Gezielte Finanzsanktionen der Vereinten Nationen im Spannungsvehältnis zum Gemeinschaftsrecht und zu den Menschenrechten, *JuS* 299–302.
Vaughan-Williams N. (2008). Borderwork beyond Inside/Outside? Frontex, the Citizen-Detective and the War on Terror, *Space and Polity* 12, 63–79.
Vennemann, N. (2003a). Country Report on the European Union. In C. Walter, S. Vöneky, V. Röben, F. Schorkopf (eds.), *Terrorism as a Challenge for National and International Law*. Berlin: Springer.
Vennemann, N. (2003b). The European Arrest Warrant and Its Human Rights Implications, *Zeitschrift für ausländsiches öffentliches Recht und Völkerrecht (ZaöRV)* 63, 103–121.
Verbruggen, F. (2004). Bull's-eye? Two Remarkable EU Framework Decisions in the Fight against Terrorism. In C. Fijnaut, J. Wouters, F. Naert (eds.), *Legal Instruments in the Fight Against International Terrorism*. Leiden: Nijhoff.
Vernimmen, G., Surano, L. (2008). Analysis of the Future of Mutual Recognition in Criminal Matters in the European Union, *European Criminal Law Academic Network (ECLAN) Study – Final Report*, *November 2008*.
Voigt, S. (2006). Der EU-Rahmenbeschluss zur Terrorismusbekämpfung – ein wirksames Mittel der Terrorabwehr? In E. Müller, P. Schneider (eds.), *Die Europäische Union im Kampf gegen den Terrorismus: Sicherheit vs. Freiheit?* Baden-Baden: Nomos.
von Bogdandy, A., Nettesheim, M. (1996). Die Europäische Union: Ein einheitlicher Verband mit eigener Rechtsordnung, *Europarecht (EuR)* 3–26.
Von Bubnoff, E. (2002). Terrorismusbekämpfung – eine weltweite Herausforderung, *Neue Juristische Wochenschrift (NJW)* 2672–2676.
von Langsdorff, H. (2003). Maßnahmen der Europäischen Union zur Vereinfachung und Beschleunigung der Rechthilfe und insoweit vorgesehene Beschuldigten- und Verteidigerrechte, *Strafverteidiger (StV)* 472–477.
Wahl, T. (2001). Eurojust, *AGON* No. 33, 21–23.
Wahl, T. (2006a). Community Powers in Criminal Matters - The European Court's Ruling on PNR Data, *eucrim* 3–4.
Wahl, T. (2006b). Customs Empowered for Cash Controls, *eucrim* 12.
Wahl, T. (2006c). PNR Data – New Agreement, *eucrim* 48–49.
Wahl, T. (2006d). Regulation on Transfers of Funds in Force, *eucrim* 59–60.
Wahl, T. (2006e). Datenschutz im Rahmen der polizeilichen Zusammenarbeit unter besonderer Berücksichtigung des SIS. In A. Epiney, S. Theurkauf (eds.), *Datenschutz in Europa und die Schweiz*. Zürich: Schulthess.
Wahl, T. (2007a). EU and USA Conclude Controversial Long-Term PNR Agreement, *eucrim* 9–10.
Wahl, T. (2007b). New Decision Establishing Europol on Track, *eucrim* 83.
Wahl, T. (2007c). Initiative on Eurojust, *eucrim* 84–85.
Wahl, T. (2007d). Data Protection, *eucrim* 101–104.
Wahl, T. (2008a). Europol's Transformation into EU Agency Agreed *eucrim* 13f.
Wahl, T. (2009). The Perception of the Principle of Mutual Recognition of Judicial Decisions in Criminal Matters in Germany. In Vernimmen-Van Tiggelen, G., Surano, L., Weyembergh, A. (eds.), The future of mutual recognition in criminal matters in the European Union. Brussels: Editions de l'Université de Bruxelles.
Wahl, T., Staats, S. (2008a). EU PNR Scheme - Redraft by the Council, *eucrim* 29–30.
Wahl, T., Staats, S. (2008b). Transfer of Prüm Treaty Finalised, *eucrim* 305.
Wiener, A. (2008). European Responses to International Terrorism: Diversity Awerness as a New Capability? *Journal of Common Market Studies (JCMS)* 46, 195–218.

Wilkinson, P. (2005). International Terrorism: The Changing Threat and the EU's Response, *Chaillot Paper n° 84*, *October 2005*.

Wouters J., Naert F. (2004a). Of Arrest Warrants, Terrorist Offences and Extradition Deals: An Appraisal of the EU's main Criminal Law Measures against Terrorism after "11 September", *Common Market Law Review (CMLRev)* 41, 909–935.

Wouters, J., Naert F. (2004b). Police and Judicial Cooperation in the European Union and Counterterrorism: An Overview. In C. Fijnaut, J. Wouters, F. Naert (eds.), *Legal Instruments in the Fight Against International Terrorism*. Leiden: Nijhoff.

Wright, J. (2006). The Importance of Europe in the Global Campaign Against Terrorism, *Terrorism and Political Violence 18*, 281–299.

Zimmermann, D. (2006). The European Union and Post-9/11 Counterterrorism: A Reappraisal, *Studies in Conflict & Terrorism 29*, 123–145.

Zimmermann, F. (2009). Tendenzen der Strafrechtsangleichung in der EU - dargestellt anhand der Bestrebungen zur Bekämpfung von Terrorismus, Rassismus und illegaler Beschäftigung, *Zeitschrift für internationale Strafrechtsdogmatik (ZIS)* 1–10.

Zöller M. (2007). Vorratsdatenspeicherung zwischen nationaler und europäischer Strafverfolgung, *Goltdammers Archiv (GA)* 392–414.

Chapter 5
Instruments of International Law: Against Terrorist Use of the Internet

Ulrich Sieber*

5.1 Introduction

5.1.1 The Need for International Cooperation Against Cyberterrorism and Other Uses of the Internet for Terrorist Purposes

Terrorism is a global phenomenon that transcends national borders. Computer networks and computer data also disregard physical boundaries, creating a global cyberspace. In addition, computer networks such as the Internet allow for the development of new forms of technology that enable users to maintain their anonymity, to engage in hidden communication, and to make use of sophisticated encryption programs in the transfer and storage of data. Thus, global cyberspace provides a unique environment in which to carry out cyberterrorism and to pursue other international terrorist goals.[1]

As a result of these specific features of computer networks, three major areas for terrorist activities on the Internet have opened up: the commission of destructive attacks by means of the Internet; the mass dissemination of illegal content via the Internet; and the use of the Internet for individual communication and for the

U. Sieber (✉)
Director at the Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany

* This analysis is based on the author's report prepared for the Committee of Experts on Terrorism (CODEXTER) of the Council of Europe. See *Sieber* in: *Council of Europe* (2007), pp. 44–97. Thanks are due to Emily Silverman and Indira Tie for invaluable translation and editing assistance.

[1] For a more detailed analysis of these problems, see *Sieber* in: *Council of Europe* (2005b), pp. 212–218.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_5, © Springer Science+Business Media, LLC 2010

commission of traditional forms of crime. In the first area, *destructive attacks against computer systems carried out by means of the Internet* (cyberterrorism) can lead not only to the destruction, corruption, and rendering inaccessible of intangible computer data, thus blocking production processes, banking systems, or public administration. Internet-based attacks can also damage physical property and human life if, for example, the attacked computer systems are responsible for the administration of nuclear power stations, dams, flight control systems, hospital computers, or military weapon systems. Because many aspects of modern society are highly dependent on computer systems, the risks posed by this type of criminal activity are considerable. However, at this time, very few cases involving these kinds of attacks are known. In contrast, terrorist use of the Internet and other electronic communication systems in the second of these areas – the *public dissemination of illegal content* – is common. Here, the Internet and other communication systems are exploited by terrorists in order to threaten the commission of terrorist acts; to incite, advertise, and glorify terrorism; to engage in fundraising for and financing of terrorism; to provide training for terrorism; to recruit for terrorism; and to disseminate racist and xenophobic material. As a result, the Internet has become an important tool by means of which terrorists send their messages to a broad audience. Finally, the Internet and other computer systems play a significant role in the third area mentioned above, the *logistical preparation of terrorist offences*, including internal communication, acquisition of information (e.g. on bomb building, hostage taking, or hijacking), analysis of targets, and other forms of information gathering.[2]

The investigation and prosecution of most of these crimes is complex and challenging due to the technical nature of the Internet. Investigation and prosecution in this area require both adequate substantive criminal law provisions as well as adequate procedural capabilities, such as the authority and the technical ability to identify foreign attackers, preserve stored computer data, issue production orders requiring the submission of specified computer data, engage in search and seizure of computer systems, break encryption, engage in the real-time collection of traffic data, and intercept content data. In many cases, these phenomena have an international dimension, which may require concerted investigation in numerous countries. As a consequence, the prosecution and prevention of terrorist activities on the Internet depend to a great extent on the existence of appropriate international conventions and other instruments of international cooperation. These instruments must address the specific legal and forensic challenges posed by the Internet, they must make use of new Internet-based investigation techniques, and, at the same time, they must balance the need for effective prosecution against the obligation to protect citizens' civil liberties.

[2]For the phenomena of cyberterrorism and other use of the Internet for terrorist purposes, see *Brunst* in: *Council of Europe* (2007), pp. 14–46; *Sieber* in: *Council of Europe* (2005b), pp. 173–175; Weimann (2005), pp. 129–149 as well as Brunst, this volume.

5.1.2 Aim, Method, and Structure of this Analysis

The *aim of this analysis* is to determine whether existing international conventions and other instruments of legal cooperation are adequate for the containment of cyberterrorism and other use of the Internet for terrorist purposes or whether the instruments should be amended. In light of this aim, the analysis focuses on the questions of whether the computer-specific international instruments are applicable with respect to terrorism and whether the terrorist-specific instruments are applicable in the IT environment. Furthermore, while this report is the result of a specific study and does not reflect a comprehensive evaluation of international instruments in general, it will provide an initial analysis with respect to the question of whether the various international instruments provide adequate coverage of crimes associated with the use of the Internet for terrorist purposes or whether the instruments exhibit gaps or other general problems regarding this kind of criminal activity that should be addressed in the future.[3] The term "gap", it should be pointed out, is understood broadly: because the effects of the criminal law are felt both in the area of security as well as in the area of liberty, gaps can exist with respect to the effective prosecution of crime *and* with respect to the effective protection of human rights.[4]

The *method of the study* involved the selection and analysis of international instruments. In this process, all relevant conventions of the Council of Europe (CoE) concerning terrorist use of the Internet were included as well as those of other major organisations, such as the United Nations and the European Union.

The following analysis encompasses all three areas of law that require international legal coordination as a prerequisite for effective transnational prosecution. Thus, the report addresses the development and harmonisation of national substantive criminal law (infra 5.2), national criminal procedure (infra 5.3), and the law of international cooperation (infra 5.4).

5.2 Developing and Harmonizing National Substantive Criminal Law

The basic requirement for the prosecution of cyberterrorism and other use of the Internet for terrorist purposes is the existence in all countries of adequate national substantive criminal law provisions that cover the various terrorist acts. Thus, this

[3] For a general analysis of deficits in the international conventions on terrorism, see Tomuschat (2005), p. 299 ff.

[4] The identification and elimination of any such gaps requires a normative evaluation that depends, to some extent, on subjective attitudes. Thus, the identification of gaps is understood as the identification of a situation that – based on the subjective consideration of the author – might benefit from changes in the international law of cooperation, either to improve efficiency or to enhance the protection of civil liberties.

chapter analyses the relevant international standards that govern the three aforementioned types of exploitation of the Internet for terrorist purposes: (1) destructive attacks on computer systems carried out by means of the Internet, (2) computer-based communication of illegal content to the public, and (3) other computer-based planning and support.

5.2.1 Destructive Attacks Carried Out by Means of the Internet

5.2.1.1 Structural Analysis of the Relevant Attacks With Respect to the Existing Legal Framework

The analysis of destructive attacks on computer systems carried out by means of the Internet shows a wide variety of possible techniques: terrorists could circumvent the integrity, confidentiality, and availability of computer systems and data either by hacking computers, deceiving victims, or spreading viruses and worms, thus manipulating systems, or by bringing about mass queries and other large-scale attacks on the victim's computer system (such as distributed denial of service attacks using bot nets).[5] If the attacked IT systems are connected to other critical systems and infrastructures, both the disruption of services as well as physical harm and loss of life could result. Physical damage could be brought about, for example, by attacking the computers of electrical supply systems, hospitals, food production or pharmaceutical companies, air, railroad or other transport control systems, hydroelectric dams, military control systems, or nuclear power stations.[6] Thus, in order to respond to the question of whether international legal instruments have gaps with respect to the coverage of terrorist attacks on computer systems, a wide variety of abuses involving different attack techniques and different results must be considered.

The national substantive criminal law provisions and the various international standards in question are characterised by descriptions of acts, results, and intents. Thus, the investigation of the applicability of these provisions to terrorist attacks on computer systems carried out by means of the Internet requires a systematic analysis not only of the acts themselves but especially of the various results (actual and intended) of the attacks. This leads to the following pattern, which is valid for the analysis of all destructive attacks on computer systems carried out by means of the Internet:

[5]For a general overview on destructive attacks against computer systems via the Internet, see *Brunst/Sieber* in: *Council of Europe* (2007), pp. 12–21; Foltz (2004), pp. 154–166; *Sieber* in: *Council of Europe* (2005b), pp. 173–175 and Brunst, this volume.

[6]This can be achieved by manipulating the "supervisory control and data acquisition" (SCADA) systems that measure and control other systems, if these systems are connected to the Internet.

- The *primary result* of all destructive acts against computer systems carried out by means of the Internet must be *interference with data*, that is, destruction, alteration, suppression, or the rendering unavailable of data. This is due to the fact that in the absence of such interference, the perpetrator can neither influence an attacked computer system nor affect the accessibility or availability of the system.[7]
- *Secondary results* of this kind of interference with data can be seen in *two types of damage*: Digital (or intangible) damage may result if data are rendered unavailable or manipulated so that services can no longer be delivered or if the computer system of the victim is compromised. Physical (or tangible) damage may result if the attacked computer system is used in the administration of property (such as hydroelectric dams or power plants) or human life (such as medical records).
- In causing these primary and secondary results, the perpetrator *intends* to bring about a *third result*, namely, the effectuation of his or her *political goals* (such as intimidating a population, compelling a government to act in a certain way, or destabilising political structures).

The development and use of this analytical pattern for Internet-based attacks on computer systems offers the opportunity to understand better the different approaches and the relationship between the existing regulations that target cybercrime and those that target terrorism: attacks on computer systems carried out by means of the Internet can be addressed by means of special IT-based statutes that focus on the first "result level" mentioned above, that is, the integrity, availability, and confidentiality of data and computer systems (as does the Cybercrime Convention). In cases of additional (proprietary and especially human) harm, attacks can also be addressed by means of offences that focus on the second "result level", namely, physical damage (as do the UN conventions on typical terrorist acts), possibly in combination with a specific terrorist intent on the third "result level" (as does the EU Framework Decision). In sum, cyberterrorism can be tackled with a "computer-specific" data approach (focusing on the intangible harm to data) and/or with a "terrorist-specific" tangible damage approach (focusing on the physical harm and – possibly – also on a certain political intent).

This analysis will start with the computer-specific instruments on cyberterrorism, that is, the Convention on Cybercrime of the Council of Europe and the EU Council Framework Decision on attacks against information systems. It will then deal with the terrorism-specific instruments, that is, the EU Council Framework Decision on combating terrorism and the various UN conventions that obligate states to enact substantive criminal law provisions.

[7] Furthermore, if the attacked system is protected by security measures, the intrusion cannot be achieved without the application of additional technical manipulations or deceptions, such as hacking techniques or methods of social engineering.

5.2.1.2 Analysis of the Relevant Instruments

Computer-Specific Instruments

CoE Convention on Cybercrime of 2001

The Council of Europe's Convention on Cybercrime,[8] which takes the data approach described above, is the most comprehensive of the existing international instruments that address computer crime. It includes obligations with respect to substantive criminal law, criminal procedure, and international cooperation.

In the area of substantive criminal law (Chapter II Section 1), Articles 4 and 5 address the "damaging, deletion, deterioration, alteration or suppression of computer data" and the "serious hindering … of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data". They cover all types of interference with data and computer systems that – as shown – are a prerequisite for terrorist attacks on computer systems carried out by means of the Internet. Because Article 4 is not limited to the deletion of data but also encompasses the alteration and suppression of data (and is extended to the hindering of a computer system by Article 5), such interference is not limited to IT-based attacks on computer systems but also occurs in the context of the aforementioned IT-based attacks on other infrastructures, on physical property, or on the life or well-being of persons.[9] This consequence of the underlying concept of the Cybercrime Convention on the comprehensive protection of the integrity and availability of computer systems is confirmed in the Explanatory Report of the Convention, which explains that Article 5 is formulated in "a neutral way so that all kinds of functions can be protected by it".[10] As a result, all types of terrorist attacks against computer systems fall under Articles 4 and 5.

In addition, Articles 2 and 3 of the Cybercrime Convention criminalise illegal access and interception, respectively, and thus cover the intrusion techniques of hacking and interception of computer data (e.g. by means of technical manipulations or by misusing intercepted information), which in many cases must be engaged in order to overcome the security measures in place on the victim's computer system so that the intruder can interfere with and alter data.

These provisions are extended in scope by rules on attempt and aiding and abetting (Article 11) and on corporate liability (Article 12) and are supported by rules requiring effective, proportionate, and dissuasive sanctions, including the deprivation of liberty (Article 13). In addition, Article 6 on the "misuse of devices" aims at the criminalisation of acts preparatory to intrusion, such as the illegal production, sale, procurement for use, or otherwise making available of "a device, including a

[8] Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185).

[9] Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, No. 65 interpreting Article 5 states that "the protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly".

[10] Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, No. 65 interpreting Article 5. See also Nos. 60 and 61 describing the concept of Article 4.

computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2–5" or a "computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed", with the intent that the device or data be used for the purpose of committing any of the offences established in Articles 2–5. Article 6 also targets the possession of these items with the intent that the item be used for the purpose of committing any of the offences established in the aforementioned articles.[11] Thus, with respect to terrorist attacks via the Internet, Articles 2, 3, and 6 give additional protection, allowing perpetrators to be prosecuted at an early stage.

As a consequence, the implementing requirements of the Cybercrime Convention in the area of substantive criminal law provide for a broad criminalisation of IT-based terrorist attacks on computers and all other legal interests that depend on the functioning of computer systems. As shown above, physical harm to property or human life and well-being is not a prerequisite for punishment under the Cybercrime Convention, but leads to the applicability of additional "traditional" offences of national criminal law. Thus, the Cybercrime Convention achieves the criminalisation of attacks on computer systems by means of a "data approach" that does not require, consider, or evaluate physical damage or the (political) intent of the perpetrator.

EU Council Framework Decision on Attacks Against Information Systems of 2005

The EU Council Framework Decision on attacks against information systems[12] is based on the Cybercrime Convention of the Council of Europe and, like the Convention, requires Member States to ensure that illegally accessing information systems (Article 2), illegally interfering with systems (Article 3), and illegally interfering with data (Article 4) are punishable as criminal offences.[13] In addition, it includes requirements concerning the criminalisation of instigation, aiding and abetting, and attempt. As a consequence, it can also cover the necessary interference with data in IT-based cyberterrorism attacks.

Terrorism-Specific Instruments

EU Council Framework Decision on Combating Terrorism of 2002/2008

Cyberterrorism is also addressed in the EU Council Framework Decision on combating terrorism.[14] In contrast to the aforementioned instruments, this Framework

[11] Furthermore, there is a provision against computer-related forgery (Article 7), which can apply to preparatory electronic falsifications that might also facilitate intrusion.

[12] EU Council Framework Decision 2005/222/JHA of 24.2.2005 on attacks against information systems (OJ L 69/67 of 16.3.2005).

[13] The Framework Decision does not contain a provision on misuse of devices.

[14] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002), as amended by Council Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

Decision follows a "terrorist-specific", traditional corporeal damage approach (focusing on physical or human corporeal harm). Unlike the Cybercrime Convention, the focus of the Framework Decision is not on the interference with data or on the IT-based forms of attack, but on the result of the perpetrator's action and on his or her intent with respect to the political aim of the attack. Article 1 of the Framework Decision reads as follows (emphasis added):

> Each Member State shall take the necessary measures to ensure that intentional acts referred to below …, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:
>
> – Seriously intimidating a population, or
> – Unduly compelling a Government or international organisation to perform or abstain from performing any act, or
> – Seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation, shall be deemed to be terrorist offences:
>
> … (d) causing extensive destruction to a Government or public facility, a transport system, *an infrastructure facility, including, an information system*, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or *result in major economic loss* …
> … (i) threatening to commit any of the acts listed in (a) to (h).

Articles 2 and 4 contain additional rules on participation (including supplying information, material resources, or funding) and on attempt. Thus, the Framework Decision applies a "corporeal damage approach" that focuses more specifically on terrorist attacks than do the data and system interference provisions of the Cybercrime Convention. In contrast to the Cybercrime Convention, it takes into consideration the extent of the damage to a computer infrastructure, thus covering serious attacks on infrastructures and against a multitude of computers by large-scale virus attacks or distributed denial-of-service (DDoS) attacks and excluding minor attacks against individual computer systems. In addition, it takes into consideration the "terrorist" intent of the perpetrator, that is, whether he or she pursued specific political aims. As a consequence of these aggravating factors, Article 5 of the Framework Decision requires that such offences be punishable by custodial sentences longer than those that can be imposed under national law for offences committed without special intent.

Recitals 3, 4, 8, and 11 of the 2008 Council Framework Decision amending the EU Council Framework Decision on combating terrorism[15] specifically refer to the extensive terrorist use of the Internet and the resulting danger[16], whereas recital 11 of the same Council Framework Decision clarifies that the EU Council Framework Decision on combating terrorism covers both traditional violent attacks as well as

[15]Council Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

[16]See Recital 4: "The Internet is […] thus functioning as a 'virtual [terrorist] training camp'".

IT-based attacks.[17] Thus, there are no gaps in criminalisation when the provision is applied to attacks via the Internet.

UN Conventions and Protocols Against Specific Acts of Terrorism of 1970 et seq

The UN has elaborated numerous multilateral conventions and protocols relating to states' instruments for combating violent acts and terrorism.[18]

- The Convention for the Suppression of Unlawful *Seizure of Aircraft*, the Convention for the Suppression of Unlawful Acts Against the Safety of *Civil Aviation*, and the Protocol for the Suppression of Unlawful Acts of Violence at *Airports Serving International Civil Aviation*.[19] These conventions could be applied, for example, in cases of computer-based manipulation of flight control systems in airplanes or airports.
- The Convention on the Prevention and Punishment of *Crimes Against Internationally Protected Persons*.[20] This bears relevance, for example, to an attack committed by manipulating a hospital computer system in order to kill a person protected by the Convention.
- The International Convention Against the *Taking of Hostages*.[21] The relevant provisions could be applied, for example, in a case in which terrorists communicate demands for ransom via email.
- The Convention on the Physical *Protection of Nuclear Material*[22] and the Convention for the Suppression of *Acts of Nuclear Terrorism*.[23] Convention offences could be committed, for example, by terrorists manipulating the computer system of a nuclear power plant with the intent to set free nuclear material.

---

[17]Recital 11, second sentence: "These forms of behaviour should be equally punishable in all Member States irrespective of whether they are committed through the Internet or not".

[18]See Bassiouni (2001); Nuotio (2006), p. 1002 ff. For the UN Conventions on the Suppression of the Financing of Terrorism of 1999, see 5.3.2 and 5.4.2 infra.

[19]Convention for the Suppression of Unlawful Seizure of Aircraft of 16.12.1970, UN Treaty Series Reg. No. 12325; Convention for the Suppression of Unlawful Acts Against Safety of Civil Aviation of 23.9.1971, UN Treaty Series Reg. No. 14118; Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation of 24.2.1988 (http://www.un.org/chinese/terrorism/1988E.pdf [last visited: 25 February 2009]). In addition, the Convention on Offences and Certain Other Acts Committed on Board Aircraft of 14.9.1963, UN Treaty Series Reg. No. 10106, regulates the powers of the aircraft commander with respect to offences committed on board.

[20]Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons of 14.12.1973, UN Treaty Series Reg. No. 15410.

[21]Convention Against the Taking of Hostages of 17.12.1979, UN Treaty Series Reg. No. 21931.

[22]Convention on the Physical Protection of Nuclear Material of 3.3.1980, UN Treaty Series Reg. No. 37517.

[23]International Convention for the Suppression of Acts of Nuclear Terrorism of 13.4.2005, see http://untreaty.un.org/English/Terrorism/English_18_15.pdf [last visited: 25 February 2009]; for status of signatures and ratifications, see http://treaties.un.org/doc/publication/mtdsg/volume%20ii/chapter%20xviii/xviii-15.en.pdf [last visited: 25 February 2009].

- The Convention for the Suppression of Unlawful Acts Against the *Safety of Maritime Navigation*.[24] This Convention could become relevant where an electronic ship control system is manipulated.
- The Protocol for the Suppression of Unlawful Acts Against the Safety of *Fixed Platforms Located on the Continental Shelf*.[25] This Convention would be applicable where destruction of a fixed platform is planned or achieved by electronic interference with the platform's security control system.
- The International Convention for the Suppression of *Terrorist Bombings*.[26] This Convention demands criminal law provisions that might be applied in a case of cyberterrorism in which a bomb is triggered via the Internet. However, the definition of Article 1 and the aim of the Convention do not allow an extension to "virtual bombs" (such as "mail bombs" or other destructive software tools) that cause only intangible damage.

The enumeration shows that the criminal provisions of the UN conventions follow the traditional "corporeal damage approach" mentioned above by protecting certain persons (e.g. senior representatives of States) or infrastructures (e.g. air and sea traffic or maritime platforms) or by criminalizing certain dangerous acts (e.g. bombing, uncontrolled transfer of nuclear material, and hostage-taking). Concentrating as they do on specific dangerous acts that are punishable per se, they do not contain a subjective requirement of political ("terrorist") intent. All of them have additional provisions that regulate attempt and participation.

With respect to cyberterrorism and the use of the Internet for terrorist purposes, it is important to note that all criminal provisions contained in the conventions and protocols discussed above are worded in general terms. They are applicable regardless of how the acts are committed, that is, whether the acts are committed by traditional means or by means of IT-based attacks. For example, the provisions demanded by the aforementioned UN Conventions are applicable if the Internet is used to take control over an airport or a ship navigation system, if a computer network is used to trigger a bomb or an attack on an aircraft, or if computer manipulations are undertaken in order to misroute the transfer of nuclear material. The non-applicability, mentioned above, of the Convention for the Suppression of Terrorist Bombings to "virtual bombs" is not an exception to this rule, but rather a desired result of the legal framework of the UN conventions on terrorism, which are directed at specific, enumerated acts only. Thus, the UN instruments are generally applicable and do not have gaps in criminalisation with respect to IT-based attacks. However, due to the system of the UN conventions on terrorism, these conventions do not cover all terrorist

[24] Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation of 10.3.1988, UN Treaty Series Reg. No. 29004.

[25] Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf of 10.3.1988, UN Treaty Series Reg. No. 29004.

[26] Convention for the Suppression of Terrorist Bombings of 15.12.1997, UN Treaty Series Reg. No. 37517. In this connection, see also the Convention on the Marking of Plastic Explosives for the Purpose of Detection of 1991, UN Treaties Series Reg. No. 36984, which provides for chemical marking to facilitate detection of plastic explosives, e.g. to combat aircraft sabotage.

acts in a general way. Thus, the evaluation of existing international conventions raises the question of whether a new convention, one that would specifically address terrorist attacks on computer systems or computer infrastructures, is necessary.

5.2.1.3 Summary, Evaluation, and Consequences of Legal Policy

General Evaluation

The previous analysis has shown that international instruments promoting the harmonisation of criminal law take two complementary approaches to IT-based attacks against computer systems, infrastructures, and other legal interests:

- The "computer-specific" data approach taken by the Cybercrime Convention (which focuses, beyond the interception of and illegal access to computer systems, on the damage caused by such attacks to data) covers the interference with data that is the necessary prerequisite for any attack via the Internet. The provisions are broad and cover even the early stages of perpetrating (e.g. by means of provisions prohibiting the possession of illegal devices).
- In contrast, the traditional "corporeal damage" or "terrorist-specific" approach (which focuses on the physical or human corporeal damage caused by the attack and – possibly – also on the perpetrator's political intent) found in the EU Council Framework Decision on combating terrorism and in the various UN conventions covers many attacks with traditional corporeal results, even when these attacks are committed by means of information technology.

As a consequence, all serious attacks against computer systems, infrastructures, and other legal interests are covered by the international conventions and instruments discussed above, which require states parties to ensure the existence of criminal law sanctions.

Pros and Cons of an Additional Infrastructure Offence

Thus, the question remains regarding whether IT-based terrorist attacks against computer systems and other infrastructures should be addressed by these provisions alone or whether they should also be addressed by a more specific provision that takes into account the fact that destructive attacks are committed against computer systems via the Internet, that destructive attacks are committed with terrorist intent, and/or that destructive attacks against IT systems, other infrastructures, and other legal interests are potentially extremely dangerous. Technically, such special protection could be achieved by adopting one of the following approaches to the introduction of new criminal offences:

- The first approach would be to require states parties to create an *aggravated "IT offence"* – perhaps in an additional protocol to the Cybercrime Convention – whose

elements would include and combine abuse of the Internet, terrorist intent, and – possibly – serious harm to an IT system or IT infrastructure.
- The second approach would be to require states parties to create an *aggravated "infrastructure offence"* for the protection of IT infrastructures or – more generally – for the protection of various types of infrastructures, either as such or in combination with a specific political (terrorist) intent (e.g. following the example of the specific UN resolutions against special acts of terrorism or following the example of the EU Council Framework Decision on combating terrorism of 2002 with its general infrastructure clause).

The practical advantages of such amendments would be relatively minor the new provisions could symbolise the seriousness of attacks on (IT) infrastructures and could provide for more serious sanctions and – possibly – for the exclusion of the political offence exception, a topic discussed in more detail later on in this paper. However, there are substantial arguments against such provisions:

- Illegal destruction and alteration of computer data alone are already treated as punishable acts by the provisions of the Cybercrime Convention. Thus, the creation of new criminal offence definitions with additional offence elements is unnecessary, as special intent and special harm can be considered at the sentencing level (where significant differences exist among the various legal systems[27]).
- Terrorist intent, in particular, should not become a general aggravating factor for all types of traditional offences.[28] Defining and proving terrorist intent is difficult. This is particularly true for offences involving the Internet, where the majority of attacks against computer systems are carried out by hackers and malicious crackers and where – due to the difficulties in identifying the origin of the attack – the identity of the perpetrators and the nature of their intent may remain unknown for a long time during investigation. Because of its subjective nature, a terrorist intent requirement in a criminal provision might afford law enforcement agents more latitude than desirable in the investigation and prosecution of suspects and might prove difficult to control. Thus, it is for good reason that many of the UN conventions discussed above focus on the *actus reus* elements of an offence (such as "bombing").
- Developing a definition of specifically protected infrastructures for the purpose of a new infrastructure offence would be less problematic. However, it might be difficult to achieve agreement at the international level regarding which infrastructures (in addition to the obvious: power, water, and food supply) should be protected and/or to agree on the level of harm required to fulfil the aggravation requirement of a specific offence. In the terrorism context, the complex question of terrorist acts against tangible and intangible property would arise.[29] Establishing the level of harm necessary to satisfy the offence element would be difficult in cases involving

[27] See Sieber (2004), p. 26 ff.

[28] See also Council of Europe, Parliamentary Assembly, No. 8 of Recommendation 1644 (2004) on Terrorism: A Threat to Democracies (adopted 29.1.2004).

[29] See Tomuschat (2005), p. 292 ff.

attacks against computer systems on the Internet because these attacks range from "online demonstrations" (flooding a server with queries), to denial-of-service (DoS) attacks that make a server inaccessible to its users, to the damage (limited or serious) caused by viruses and worms, and to the serious destruction of world-wide infrastructures. Thus, there are good reasons for countries to address the gradations of damage caused to tangible and intangible property by means of general sentencing rules or sentencing ranges rather than by creating new offences.

As a consequence, there is no strong justification for requesting new instruments on the international level to address aggravated IT-based attacks on computer systems. It is sufficient for countries to evaluate existing domestic statutes that address data and system interference and make sure that they provide sanctions appropriate for cases involving terrorist attacks against computer and other essential infrastructures and other legal interests. However, such "effective, proportionate and dissuasive sanctions" are already required by Article 13 of the Cybercrime Convention, and it can be left to the national legislatures to achieve this result by means of sentencing rules, aggravated offences involving data interference, or infrastructure offences.[30]

Insufficient Signing, Ratification, and Implementation of the Cybercrime Convention

A serious gap is apparent, however, with respect to the signing, ratification, and implementation of the various instruments: the Cybercrime Convention, for example, currently has only 46 signatures and has been ratified by only 23 states (12 of which have filed numerous reservations); full implementation is even rarer.[31] As a result, the goal of preventing computer crime havens by coordinating national rules on substantive, procedural, and cooperation law is still far being achieved. Thus, the signing, ratification, and implementation of the Convention should be a top priority, and care should be taken that additional efforts – both within and beyond the scope of the existing conventions – do not hinder or distract from this important process.

5.2.2 Dissemination of Illegal Content

5.2.2.1 Structural Analysis of the Phenomena With Respect to the Legal Framework

As mentioned above, the second major use of the Internet for terrorist purposes consists in the dissemination of illegal content. In order to spread their messages of fear and terror, perpetrators use all types of media, systems, and content. As a

[30] See, e.g., the specific sentencing rule of sec. 303b subsection 4 no. 3 of the current German draft combating computer crime ("Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität"), BT-Drucksache 16/3656.

[31] See Treaty Office on http://conventions.coe.int/ [last visited: 25 February 2009]; Gercke (2006b), p. 145.

result, websites, video-sharing platforms, and other media have become important tools of an "open university for jihad".[32] Thus, the identification of possible gaps in international instruments with respect to illegal content requires the identification of the various acts that correspond to the categories of conduct prohibited by the relevant national and international provisions.

In most national legal systems and in the international instruments under study, the applicability of these legal provisions no longer depends on the type of carrier used to disseminate the illegal content. In other words, the relevant criminal provisions found in international instruments and in most domestic legal orders do not distinguish between data that are distributed by means of traditional carriers (e.g. paper documents for traditional writing), data that are distributed by corporeal electronic data carriers (e.g. CDs), and data that are distributed by incorporeal transmitters such as the Internet, radio, or television.[33]

Instead, domestic legal orders and international instruments differentiate with respect to the various kinds of illegal content and the types of harm they may cause to different legal interests. An analysis of terrorist communication leads to the identification of the following typologies and kinds of content:

- Threatening to commit terrorist offences,
- Inciting, advertising, glorifying, and justifying terrorism,
- Training for terrorism,
- Recruiting for terrorism,
- Fundraising for and financing of terrorism,
- Disseminating racist and xenophobic material and denying, approving, or justifying genocide.[34]

A legal assessment of most of these phenomena exposes the difficulty in pinpointing the transition between illegality and legality while balancing underlying interests in security and freedom (especially freedom of the press[35]). This can be seen, for

[32] See Coll and Glasser (2005).

[33] See the comparative legal analysis by Sieber (1999), p. 27.

[34] For general threats against Germany and Austria via a video message sent to a website called "Global Islamic Mediafront" (GIMF), see Ramelsberger (2007), p. 5. For terrorist webpages, other forms of propaganda, and psychological warfare, as well as inciting, advertising, glorifying, and justifying terrorism, see Brunst/Sieber in: *Council of Europe* (2007), pp. 25–29; Denning in: Arquilla (2001), pp. 239–288; Sieber in: *Council of Europe* (2005b), pp. 173–178; Thomas (2003), p. 117; U.S. Army Training and Doctrine Command (2006), pp. 1–3; Weimann (2004a), pp. 1–12. For fundraising by selling books, videos, and CDs in online stores and by giving instructions for online donations, see Brunst/Sieber in: *Council of Europe* (2007), p. 29; Gercke (2006a), p. 65; Thomas (2003), p. 116; Sieber in: *Council of Europe* (2005b), p. 178; Weimann (2004a), pp. 5–7. For teaching and training manuals, such as the "Terrorist's Handbook", the "Anarchist Cookbook", the "Mujahadeen Poisons Handbook", the "Encyclopedia of Jihad", the "Sabotage Handbook", and the pamphlet "How to Make Bombs", see Brunst/Sieber in: *Council of Europe* (2007), pp. 28–29; Coll and Glasser (2005); Sieber in: *Council of Europe* (2005b), pp. 173–178, 179–180; Weimann (2004a), p. 9. For recruiting for terrorism, see Brunst/Sieber in: *Council of Europe* (2007), pp. 28–29; Sieber in: *Council of Europe* (2005b), p. 178.

[35] See 5.2.2.6, infra.

example, in the gradual transition between inciting, advertising, glorifying, justifying, explaining, and merely reporting terrorist offences (as illustrated by the publication of assassination videos set to music). The same applies to the publication of information on special weaponry: information that could be useful to terrorists but might also be found in common chemistry or physics textbooks. Similar difficulties also arise with respect to fundraising for charitable organisations that are connected to terrorist groups. Thus, it is obvious that not all of the above-mentioned phenomena are or should be fully covered by the substantive criminal law provisions in international conventions.

Due to the difficulty of balancing security and human rights in the context of each of the aforementioned types of content, this analysis cannot judge in detail whether the balancing approach undertaken in international conventions with respect to each of these categories should be approved or reconsidered. Instead, the following sections examine whether the issue was recognised and whether it was taken into account in a reasonable way during the development of the various international instruments. Also, with respect to the competent international institutions' possible chances to reconsider and change existing conventions, the aim of this analysis is not to judge the approach to the balancing of interests taken in the many specific solutions found in the various instruments but to identify gaps – or deficiencies – in the treatment of serious issues (both with respect to criminalisation and with respect to the protection of human rights).

Based on these considerations, the following analysis will be undertaken with respect to threats to commit terrorist offences; incitement, recruitment, and training for terrorism; fundraising for and financing of terrorism; as well as dissemination of racist and xenophobic material. In addition, the relationship between these types of content and the liability of media representatives and Internet providers will be addressed.

5.2.2.2 Threatening to Commit Terrorist Offences

UN Conventions and Protocols Against Specific Acts of Terrorism of 1970 et seq

Some of the UN conventions against specific terrorist acts described above[36] contain provisions against terrorist threats that are also applicable to terrorist threats disseminated on the Internet: The Convention on the Prevention and Punishment of *Crimes Against Internationally Protected Persons* covers a threat to commit any of the listed acts against senior representatives of a State (Article 2). The Convention on the Physical Protection of *Nuclear Material* refers to a threat "to use nuclear material to cause death or serious injury to any person or substantial property damage" or "to commit an offence described in sub-paragraph (b) in order to compel a natural or legal person, international organisation or State to do or to

[36] See 5.2.1.2, supra.

refrain from doing any act" (Article 7). The Convention for the Suppression of Unlawful Acts Against the *Safety of Maritime Navigation* explicitly includes as separate offences certain threats related to the commission of some (but not all) listed offences against the safety of ships (Article 3). The Protocol for the Suppression of Unlawful Acts Against the Safety of *Fixed Platforms Located on the Continental Shelf* similarly contains as separate offences certain threats related to the commission of some (but not all) listed offences against the safety of fixed platforms (Article 2). The International Convention for the Suppression of *Acts of Nuclear Terrorism* (not yet in force) also similarly mentions as an independent offence certain threats related to the commission of some (but not all) of its listed offences (Article 2).[37]

In contrast, the Convention for the Suppression of *Unlawful Seizure of Aircraft*, the Convention for the Suppression of *Unlawful Acts Against the Safety of Civil Aviation*, the International Convention Against the *Taking of Hostages*, and the International Convention for the Suppression of *Terrorist Bombings* do not have such threat provisions.[38] Thus, there is no common systematic approach to this issue in the various conventions.

EU Council Framework Decision on Combating Terrorism of 2002/2008

In contrast to the UN Conventions, the EU Council Framework Decision on combating terrorism[39] goes further with respect to the criminalisation of terrorist threats. Article 1, a comprehensive general provision dealing with terrorist offences based on objective and subjective criteria, contains a list of acts, such as attacks upon a person's life, attacks upon the physical integrity of a person, kidnapping or hostage taking, causing extensive destruction to certain infrastructures, attacks on aircraft, ships, or other means of public or goods transport, use of weapons, release of dangerous substances, etc. Article 1 requires that these acts be deemed terrorist offences under national law if they seriously damage a country or an international organisation were committed with the aim of:

- Seriously intimidating a population, or
- Unduly compelling a government or international organisation to perform or abstain from performing any act, or
- Seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation.

The advantage of this "uniform" approach can be seen with respect to the present question concerning the criminalisation of terrorist threats: Article 1 section 1(i)

[37] See notes 22 and 23.

[38] See notes 19, 21 and 26.

[39] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002), as amended by Council Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

prohibits in a systematic and transparent way "*threatening to commit any of the acts listed*". Thus, all serious terrorist threats within the scope of Article 1 are covered, irrespective of whether they are directed at individual persons, at institutions, or at the public. It also does not matter whether the threat is communicated via traditional media or on the Internet.

5.2.2.3 Incitement, Recruitment, and Training for Terrorism

CoE Convention on the Prevention of Terrorism of 2005

The Council of Europe Convention on the Prevention of Terrorism[40] is the most specific instrument addressing the harmonisation of substantive criminal law in the area of terrorism and, with it related questions of victims, jurisdiction, international cooperation, etc. In the field of substantive criminal law, the Convention requires each state party to adopt such measures as may be necessary to establish as criminal offences the following acts when committed unlawfully: Article 5: Public provocation to commit a terrorist offence, Article 6: Recruitment for terrorism, Article 7: Training for terrorism, and Article 9: Ancillary offences.

Due to these ancillary offences, the limitation of Article 5 to public provocation does not lead to a serious gap in criminalisation because the (non-public) provocation of individual persons to commit a terrorist offence can often be covered by the provisions on participation (instigation, in particular). Glorification and justification of terrorism and terrorist acts are at least partly covered in Article 5 by the vague wording "distribution of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed".[41]

These provisions do not require that the dissemination of the relevant material take place by means of traditional writing or documents (as was the case with some traditional offences involving illegal content in national legislation).[42] Thus, they also apply to the incitement of terrorist offences, to recruitment for terrorism, and to terrorist training on the Internet and in other electronic communication systems.

EU Council Framework Decision on Combating Terrorism of 2002/2008

In a manner similar to the Council of Europe Convention on the Prevention of Terrorism,[43] the newly amended EU Council Framework Decision on combating

[40] Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196).

[41] For details, see the evaluation at 5.2.2.7 infra.

[42] See the comparative legal analysis by Sieber (1999), p. 27.

[43] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002), as amended by Council Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

terrorism requires all EU Member States, in Article 3.2 (a)–(c), to ensure the criminalisation of: (a) "public provocation to commit a terrorist offence", (b) "recruitment for terrorism", and (c) "training for terrorism".

In Article 3.1 (a)–(c), the Council Framework Decision defines the acts of these three categories of so-called "offences linked to terrorist activities", largely following the wording of Articles 5–7 of the CoE Convention on the Prevention of Terrorism.[44] Ancillary offences, as criminalised in Article 9 of the CoE Convention on the Prevention of Terrorism, are covered by Article 4 of the EU Council Framework Decision on combating terrorism.

UN Security Council Resolution 1624 of 2005

UN Security Council Resolution 1624[45] also deals with the prohibition of incitement to terrorism. In number 1(a) of the Resolution, the Security Council "calls upon all States to adopt such measures as may be necessary and appropriate and in accordance with their obligations under international law to … prohibit by law incitement to commit a terrorist act". This provision covers both traditional and IT-based incitement.

5.2.2.4 Fundraising for and Financing of Terrorism

There are various well-known Conventions that address the need to criminalise acts related to fundraising for and the financing of terrorism:

- The UN International Convention for the Suppression of the Financing of Terrorism 1999[46] obligates parties to criminalise the financing of terrorism.[47]
- UN Security Council Resolution 1373, which was adopted on 28 September 2001,[48] shortly after the 9/11 attacks, contains a similar duty. Like the other UN

[44]However, the scope of application of the EU Council Framework Decision on Combating Terrorism and that of the CoE Convention on the Prevention of Terrorism differ: While a "terrorist offence" in terms of Article 1 of the CoE Convention means any of the offences within the scope of and as defined in the major UN conventions against terrorism, the EU Council Framework Decision defines terrorist offences autonomously in Article 1. See 5.2.2.2 and 5.2.2.3, supra.

[45]UN Security Council Resolution 1624 (2005) of 14.9.2005.

[46]The UN International Convention for the Suppression of the Financing of Terrorism, UN Treaty Series Reg. No. 38349, adopted by the General Assembly of the United Nations in Resolution 54/109 of 9.12.1999.

[47] With respect to the financing of terrorism, this Convention is more specific and far-reaching than the above-mentioned UN Convention against Transnational Organized Crime. See United Nations Convention Against Transnational Organized Crime of 8.1.2001 (A/Res/55/25).

[48]UN Security Council Resolution 1373 (2001) of 28.9.2001.

instruments, the resolution is applicable to acts involving terrorist motives committed online.

The CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime[49] also has rules pertaining to the adoption of substantive criminal law provisions. However, in contrast to the above UN instruments, the convention does not cover the financing of crimes with legally obtained funds. The substantive criminal law provisions of the convention as well as of other UN and EU money laundering instruments will not be dealt with in detail here.

5.2.2.5 Dissemination of Racist and Xenophobic Material

Additional Protocol to the CoE Convention on Cybercrime of 2003

During the process of drafting the Convention on Cybercrime, it was difficult to reach an agreement on the criminalisation of acts of a racist and xenophobic nature.[50] Thus, these acts were addressed in a separate additional protocol.[51] According to the Protocol, "each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct":

Article 3: Dissemination of racist and xenophobic material through computer systems,
Article 4: Racist and xenophobic motivated threat, *and*
Article 5: Racist and xenophobic motivated insult.

In addition, Article 6 addresses the denial, gross minimisation, approval, or justification of genocide or crimes against humanity by "distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies specific acts constituting genocide or crimes against humanity".

With respect to terrorism, the provisions of this Protocol are relevant to threats and insults committed with the intent to incite conflicts and violence among groups distinguished by race, colour, or national or ethnic origin. The provisions are directed at IT-based content and are therefore also applicable to the use of the Internet for terrorist purposes.

---

[49] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 16.5.2005 (ETS No. 198).

[50] See Murphy (2002), pp. 973–975; Gercke (2006b), p. 144.

[51] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems of 28.1.2003 (ETS No. 189).

European Union Council Framework Decision on Combating Racism and Xenophobia of 2008

The EU Council Framework Decision of 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law[52] requires, in Article 1 (a)–(d), each Member State to take the measures necessary to ensure the criminalisation of specific offences "directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin".

- Article 1 (a) and (b) of the Framework Decision mandate the criminalisation of publicly inciting to violence or hatred in general and, in particular, of committing such acts by public dissemination or distribution of tracts, pictures, or other material.
- Article 1 (c) and (d) require the criminalisation of the conduct of publicly condoning, denying, or grossly trivialising the crimes of genocide, crimes against humanity, and war crimes when the conduct is carried out in a manner likely to incite to violence or hatred against the above-mentioned individuals.[53]

Neither the mere dissemination of racist and xenophobic material (Article 3 Additional Protocol to the CoE Convention on Cybercrime) nor the racist and xenophobically motivated insult (Article 5 Additional Protocol) nor even the racist and xenophobically motivated threat (Article 4 Additional Protocol) shall as such be punishable according to the EU Framework Decision on combating racism and xenophobia. However, Article 4 of the Framework Decision requires Member States to ensure that racist and xenophobic motivation is considered an aggravating circumstance or taken into consideration in the determination of penalties, for example in the course of determining the penalty for an intentional and unlawful insult or for coercion stemming from racist or xenophobic motivation under the substantive criminal law of an EU Member State. Thus, while the substantive provisions of the Additional Protocol to the CoE Cybercrime Convention and those of the EU Council Framework Decision on combating racism and xenophobia differ, the practical effects of the two instruments are comparable.

As the jurisdiction clause in Article 9.2 clarifies, the Framework Decision also demands the criminalisation of these acts when committed via an information system. Furthermore, Article 2 of the Framework Decision mandates that substantive law provisions must be accompanied by rules concerning instigation, aiding, and abetting.

---

[52] EU Council Framework Decision 2008/913/JHA of 28.11. 2008 (OJ L 328/55 of 6.12.2008).

[53] The content of the latter provision corresponds largely with Article 6 of the Additional Protocol to the CoE Cybercrime Convention. However, unlike Article 6.2 (b) of Additional Protocol, Article 1 (c) and (d) do not allow for the right of the States not to apply this provision.

5.2.2.6 Liability of the Media and of Internet Providers

The Media

As mentioned above, most of the offences that target illegal content have a critical relationship with freedom of expression, which is a basic element of democratic and pluralistic societies. This is especially important in the present context because the free and unhindered dissemination of information and ideas is a most effective means of promoting understanding and tolerance, which can, in turn, help prevent terrorism. These aspects are addressed by a multitude of international declarations that address the tension between fighting terrorism and protecting human rights.

The basic instrument of protection for this aim is the European Convention on Human Rights,[54] which guarantees the right to freedom of expression (Article 10). This guarantee is taken up in the texts of many of the conventions discussed above, and the relevant case law of the European Court of Human Rights is cited in the Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism.[55] Furthermore, there are other instruments besides the European Convention on Human Rights that deal more specifically with the conflict between preventing terrorism and protecting human rights.[56] In addition, there are special instruments that cover the specific aspect of preventing terrorism and protecting the freedom of the press. The CoE Declaration on freedom of expression and information in the media in the context of the fight against terrorism,[57] for example, calls on public authorities in Member States to refrain from adopting measures equating media reporting on terrorism with support for terrorism, but also recommends that the media be aware of their responsibility not to contribute to the aims of terrorists and to adopt self-regulatory measures. Similar recommendations can be found in the Council of Europe Parliamentary Assembly Recommendation 1706 on "Media and Terrorism",[58] in Recommendation 1687 on "Combating terrorism through culture",[59] and in other international declarations.[60]

---

[54]Convention for the Protection of Human Rights and Fundamental Freedoms of 4.11.1950 (ETS No. 5), as amended by Protocol No. 14 of 13.5.2004 (ETS No. 194).

[55]See, e.g., Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196), Article 12, and Explanatory Report, Nos. 30, 88–98, 143–152, 143–152.

[56]See, e.g., Council of Europe (2005b); UN Resolution No. 60/158 of the UN General Assembly and the report of the Secretary-General pursuant to this resolution of 11.9.2006.

[57]CoE Declaration on freedom of expression and information in the media in the context of the fight against terrorism adopted by the CoE Committee of Ministers on 2.3.2005 at the 917th meeting of the Ministers' Deputies.

[58]Council of Europe Parliamentary Assembly, Recommendation 1706 (2005) of 20.6.2005 on "Media and Terrorism".

[59]Council of Europe Plenary Assembly, Recommendation 1687 (2004) on "Combating terrorism through culture".

[60]E.g., Council of Europe Parliamentary Assembly, Media and Terrorism, of 20.5.2005, Doc. 10557, and the corresponding reply from the Committee of Ministers of 18.1.2006, Doc. 10791.

The EU Council Framework Decision on combating terrorism follows the same pattern, clarifying that "[n]othing in this Framework Decision may be interpreted as being intended to reduce or restrict fundamental rights or freedoms such as… the freedom… of expression…".[61] The 2008 EU Council Framework Decision[62] amending the EU Council Framework Decision on combating terrorism[63] is even more specific, stating in Article 2 that "[t]his Framework Decision shall not have the effect of requiring Member States to take measures in contradiction of fundamental principles relating the freedom of expression, in particular freedom of the press and freedom of expression in other media as they result from constitutional traditions or rules governing the rights and responsibilities of, and the procedural guaranties for, the press or other media where these rules relate to the determination or limitation of liability". These legal instruments as well as other declarations, recommendations, and reports[64] show that the complex problem of balancing freedom and security, especially with respect to press publications on terrorism, is discussed on the international level. An assessment of the appropriateness of the approaches taken in all these conventions and instruments is, however, beyond the scope of this report.

Internet Providers

Problems similar to those experienced in the traditional press context arise in the Internet context as well. Internet providers who transmit and store the illegal content of perpetrators – along with huge amounts of legal data – generally do so without knowledge of the data and, in particular, without knowledge of the legality of the data according to the laws of the countries through which the data are being transmitted. Thus, with respect to the dissemination of illegal content fostering terrorism, the question arises regarding the conditions under which host service providers on the Internet (storers of third-party content) as well as access and network providers (transmitters of third-party content) can be held responsible for such data. Similar questions regarding criminal responsibility for third-party content arise with respect to search engines and with respect to liability in general for Internet links.[65] Attempts in many countries to address these problems by means of the general criminal law rules of participation have shown that these rules are

[61] Recital 10 of the EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002), as amended by Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

[62] EU Council Framework Decision 2008/919/JHA of 28.11.2008 amending Framework Decision 2002/475/JHA on combating terrorism (OJ L 330/21 of 9.12.2008).

[63] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002).

[64] See, e.g., Ministerial Council Decision No. 3/04 of 7.12.2004 of the Organization for Security and Co-operation in Europe (OSCE) on combating the use of the Internet for terrorist purposes.

[65] For details, see Sieber in: Hoeren/Sieber (2007), Part 18.1.

inadequate and that special legislation is required in order to ensure legal security. The analysis of the Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism indicates that this central problem was not considered in the drafting process of the Convention.[66]

The EC Directive on electronic commerce[67] addresses these problems. It seeks to contribute to the proper functioning of the European internal market by ensuring the free movement of information society services between Member States: "Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State" (Article 3.2). Only in situations covered by Article 3 Secs. 4–6 are Member States entitled to take measures in derogation of Article 3 Sec. 2 (e.g. when the measures are necessary for reasons of public policy, in particular the prevention, investigation, detection, and prosecution of criminal offences). Thus, the Directive aims to harmonise the liability of natural and legal persons who provide information society services: in certain cases involving the "mere conduit" of data, access providers are broadly exempt from civil and criminal liability (Article 15). In certain cases involving the storing of data, host service providers are only liable if they have actual knowledge of illegal activity or information (Article 14). Similar regulations exist with respect to caching functions of Internet providers (Article 13).

This liability regime is important not only for ensuring the free exchange of information and legal certainty for Internet providers, but it is also important for the prosecution of past crimes and for the prevention of illegal content in the future. It provides the basis for "notice and takedown procedures", by which host service providers storing illegal content can be forced to erase or block illegal information after they have been given notice of the presence of the illegal content on their servers. The existence of "notice and takedown procedures" enables hotlines (services that collect tips from Internet users concerning illegal information from the public) and the police to force host service providers to take down illegal content so that this content can no longer be accessed by the public.[68] Such "notice and takedown procedures", hotlines, awareness raising, industry self-regulation, and codes of conduct are the most important tools for the prevention of illegal content on the Internet.

---

[66] See Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196), Explanatory Report, No. 102 mentioning "hyperlinks" and No. 132 mentioning a "service provider" without considering the limiting function of the rules of participation and respective special provisions.

[67] Directive 2000/31/EC of the European Parliament and the Council of 8.6.2000 on certain legal aspects of information services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1 of 17.7.2000.

[68] See Commission of the European Communities, Communication from the Commission to the Council, Final evaluation of the implementation of the multiannual community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, Brussels 6.11.2006, COM (2006) 663 final.

5.2.2.7 Summary, Evaluation, and Consequences of Legal Policy

General Evaluation

The analysis undertaken here shows that the dissemination of the various types of illegal terrorist content is addressed by international instruments in an extensive and differentiated manner:

- *Threatening to commit a terrorist act* is covered by a number of UN conventions with respect to specific acts of terrorism and is addressed in a more comprehensive way by the EU Council Framework Decision on combating terrorism. However, with the exception of the efforts taken at the EU level, there is no systematic or general approach to the coverage of threats to commit terrorist acts.
- *Inciting, advertising, and glorifying terrorism* is dealt with by the CoE Convention on the Prevention of Terrorism. Although the central aim of Article 5 of the Convention is to criminalise specific cases of distribution of a message to the public with the intent to incite the commission of a terrorist offence, this Article also covers some cases of advertising, glorifying, and justifying terrorism.[69] Article 3.2 (a) of the amended EU Council Framework Decision on combating terrorism equally criminalises the "public provocation to commit a terrorist offence".
- *Training for terrorism* is tackled by Article 7 of the CoE Convention on the Prevention of Terrorism and Article 3.2 (c) of the amended EU Council Framework Decision on combating terrorism.
- *Recruiting potential terrorists* by soliciting "another person" to commit a terrorist offence is central to Article 6 of the CoE Convention on the Prevention of Terrorism and equally addressed by Article 3.2 (b) of the amended EU Council Framework Decision on combating terrorism.
- *Fundraising for and financing of terrorism* is covered extensively, in particular by the UN International Convention for the Suppression of the Financing of Terrorism of 1999 and UN Security Council Resolution 1373.
- *Dissemination of racist and xenophobic material* is dealt with by the CoE Additional Protocol to the Convention on Cybercrime and by the EU Council Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law.

The international instruments also cover general aspects of these contents, especially with respect to the difficult balancing of freedom and security:

- *Freedom of the press with respect to terrorist content* is addressed in various instruments of the Council of Europe, the European Union, and the OSCE.
- *Responsibility of Internet providers* is (only) regulated in the EC Directive on Electronic Commerce of 2000.

[69] For more details, see below.

In all areas covered by these conventions, one might argue either for more far-reaching or for more restrained solutions. However, this is a common situation for an area in which both a difficult balancing of interests and broad international agreement are required. Slightly different policy evaluations alone do not justify a possible revision of the substantive criminal law provisions of international conventions covering illegal content on the Internet. This can be illustrated with respect to glorifying and justifying terrorism and terrorist acts. These acts are only partly covered in Article 5 of the Convention on the Prevention of Terrorism by the vague wording "the distribution of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed". However, a more extensive or a more precise wording with respect to glorifying and justifying terrorist acts might conflict with such rights as freedom of expression and freedom of the press.[70] Thus, in the context of this general overview of possible problems, the current regulation on glorifying and justifying terrorism cannot be considered a clear gap, neither with respect to criminalisation nor with respect to civil liberties. In addition, on the political level, reopening these issues for discussion only a few years after the adoption of the Convention is not a real option because such a discussion would hamper the process of signing and ratifying the Convention.

Gaps With Respect to Threatening to Commit Terrorist Offences

The situation of illegal content, however, is different as far as the special problems associated with threatening to commit terrorist offences are concerned. In some of the UN conventions dealing with specific terrorist offences, threatening to commit the described acts is not criminalised. The EU Council Framework Decision on combating terrorism of 2002[71] goes further than the UN conventions in that it covers "threatening to commit any of the acts listed" in its broad catalogue of terrorist offences (including attacks on infrastructures); however, because the threat must be related to one of the specified acts, the Framework Decision does not cover general unspecified threats. The Council of Europe Convention on the Prevention of Terrorism does not contain a general threat provision with respect to terrorist offences either. The Explanatory Report to the Convention and the underlying expert report do not address the issue of threats to commit terrorist acts.[72] This gap should be a topic for future reform discussions at the CoE or UN level. On the

[70] See also Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196), Explanatory Report, Nos. 30, 88–98.

[71] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002), as amended by Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

[72] See Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196), Explanatory Report, Nos. 17, 26 in connection with No. 49; Ribbelink (2004), p. 11 ff.

Council of Europe level, a general provision could be included in an additional protocol to the Convention on the Prevention of Terrorism. Another – more systematic – solution would be to create a comprehensive CoE Convention on Terrorism in which the various terrorist offences (including ancillary offences and general rules) would be systematised and consolidated.[73] The problem could also be dealt with on the UN level by systematically analysing the need to amend the specific terrorism conventions that currently do not cover the threat to commit the relevant offence. However, such an offence-specific approach could cause problems in the context of unspecified general threats that do not refer to an act enumerated in one of the UN conventions. In any event, the question of the form and content of threats to be covered would have to be carefully considered and limited, with a focus on destructive attacks and not on the "supporting offences" of glorifying terrorism, training for terrorism, recruiting for terrorism, and fundraising.

Lack of Specific Regulations Regarding Responsibility of Internet Providers

An additional problem arising in this context is the fact that the Council of Europe and the UN conventions provide for liability as direct perpetrators and as aiders and abettors. Application of such general rules with respect to the liability of providers does not lead to clear results and legal certainty. In contrast, the EC Directive requires Member States to create provisions that specifically regulate the liability of various types of Internet providers. This is advantageous with respect to legal certainty. In addition, increased specificity and a broader harmonisation of rules establishing the responsibility of Internet providers could serve as the basis – at least for the aforementioned harmonised areas of illegal terrorist content – for specific "notice and takedown procedures"[74] on an international level. Such rules could then be the basis for improved practical cooperation and for international public–private partnerships (e.g. hotlines, codes of conducts for providers, joint international efforts to erase, block, and/or monitor illegal content).[75]

Given the amount of terrorist propaganda on the Internet, this issue is an important one. Open societies should not needlessly leave the Internet and other electronic communication systems vulnerable to abuse at the hands of their adversaries. However, they should also abstain from ineffective control methods of a purely symbolic nature, especially if these methods infringe information rights, contribute to the development of uncontrollable surveillance systems, and create high costs for the Internet industry. Thus, it is essential to investigate the possibilities, dangers, and

[73] For this proposal, see Tomuschat (2005), p. 299 ff.; Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196), Explanatory Report, Nos. 5–23.

[74] "Notice and takedown procedures" are based on liability rules establishing responsibility only if the provider has actual knowledge of illegal content. Thus, by giving notice to the provider, he or she is forced to remove the illegal content in order to avoid responsibility.

[75] See Sieber in: Lederman/Shapira (2001), pp. 231–292; Sieber in: Waltermann/Machill (2000), pp. 319–400, as well as the other contributions in this volume.

limits of international efforts to prevent illegal content on the Internet and in other electronic information systems. The Council of Europe, with its long tradition of the development of criminal law and the protection of civil liberties, would be the ideal institution to coordinate such efforts.

Furthermore, such rules and procedures are important not only in the context of the dissemination of illegal terrorist content but also with regard to the dissemination of other illegal content, such as child pornography.[76] Thus, it would make sense to develop rules and procedures that would apply both to illegal terrorist content as well as to the many other types of illegal material for which an international consensus can be found.

Insufficient Signing, Ratification, and Implementation of the Convention on the Prevention of Terrorism

Finally, a serious gap can again be identified with respect to the signing, ratification, and implementation of the various instruments: the most important international instrument against the illegal dissemination of illegal terrorist content, the Convention on the Prevention of Terrorism, has 43 signatures and 15 ratifications.[77] Thus, the goal of preventing safe terrorist harbours by coordinating national rules on substantive criminal law has not yet been achieved. As a consequence, future efforts should concentrate on the signing, ratification, and implementation of the Convention.

In the European Union, the situation is somewhat different: the amended EU Council Framework Decision on combating terrorism is taking over as far as certain substantive provisions of the CoE Convention on the Prevention of Terrorism – those dealing with public provocation to commit a terrorist offence, recruitment, and terrorism training – are concerned. Because framework decisions are binding upon all EU Member States regarding their results,[78] important aspects of the CoE Convention on the Prevention of Terrorism will have to be applied within EU territory by means of an EU instrument. This will limit, to a certain degree, the effects of the stagnation in the ratification process of the Convention.[79]

---

[76] See Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (A/RES/54/263) of 25.5.2000, which entered into force on 18.1.2002; CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25.10.2007, not yet entered into force, see Treaty Office on http://conventions.coe.int/ [last visited: 25 February 2009].

[77] See Treaty Office on http://conventions.coe.int/ [last visited: 25 February 2009]; Gercke (2006b), p. 145.

[78] As Article 34.2 (b) of the Treaty on European Union defines, "Framework decisions shall be binding upon the Member States as to the result to be achieved but shall leave to the national authorities the choice of form and methods. They shall not entail direct effect". However, in contrast to EU directives, there is no efficient enforcement mechanism for framework decisions.

[79] The EU Member States are to comply with the amendments to the EU Council Framework Decision on combating terrorism by 9 December 2010, pursuant to Article 3 para.1 Council Framework Decision 2008/919/JHA.

5.2.3 Use of the Internet for Other Purposes

5.2.3.1 Relevant Phenomena

Computer systems and the Internet are also used to support communication relating to the planning of terrorist activities as well as to facilitate other preparatory acts for all types of terrorist cases. The perpetrators may send encrypted email or email containing hidden messages; they may acquire information online (e.g. tips on constructing bombs, on hostage taking, or on hijacking). They may use the Internet to analyze targets by means of satellite maps available on the Internet, to gather other types of information, such as reports of security weaknesses in airports, to pursue logistical planning, to engage in money laundering (e.g. by means of Internet banking), or to make money by selling pirated software and by means of other crimes using the Internet. The analysis of seized computer systems has confirmed that such acts already play a considerable role in practice.[80]

5.2.3.2 Analysis of Relevant Conventions

The above-mentioned activities are addressed to a certain degree by the aforementioned conventions. As described, the criminal acts dealt with in these conventions are broadly defined and the definitions do not specifically address the question of (traditional or computer-based) means of commission. Most of the provisions in these conventions include adequate rules on participation as well as rules covering preparatory acts and attempt.

Besides the rules of the general part of criminal law, there are additional statutes in the specific part of criminal law that already cover preparatory acts at an earlier stage and also extend the attribution of these acts to accessories. On the international level, such respective rules on "conspiracy" and "participation in criminal organizations" are addressed in additional instruments. The UN Convention against Transnational Organized Crime[81] aims to criminalise participation in an *organised criminal group* (Article 5), laundering of proceeds of crime (Article 6), corruption (Article 8), and obstruction of justice (Article 23). The EU Council Framework Decision on the fight against organised crime[82] is very

[80]For the communication of terrorists on the Internet, see Brunst/Sieber in: *Council of Europe* (2007), p. 7–34 (30–31); Sieber in: *Council of Europe* (2005b), p. 179; Weimann (2004a), p. 9 f.; Weimann (2004b); Whine (1999), p. 233 ff.; Wilson (2003), p. 18. For the use of the Internet by terrorists for logistical planning see Brunst/Sieber in: *Council of Europe* (2007), pp. 31–33; Sieber in: *Council of Europe* (2005b), p. 180; U.S. Army Training and Doctrine Command (2006), pp. 1–2; Weimann (2004a), p. 2. For other patterns of terrorists seeking financial gains, see Sieber in: *Council of Europe* (2005b), p. 180 f.

[81]United Nations Convention Against Transnational Organized Crime of 8.1.2001, (A/Res/55/25).

[82]EU Council Framework Decision 2008/841/JHA of 24 October 2008 OJ L 300/42 of 11.11.2008.

similar to the UN Convention against Transnational Organized Crime, both in content and in wording.[83] However, both of these instruments are thus only applicable to crimes committed by terrorist groups when these groups act with the intention of obtaining a financial or other material benefit (such as when crimes are committed in order to facilitate or finance the commission of the group's political crimes).

Unlike Article 5.1 (a) of the UN Convention against Transnational Organized Crime and the corresponding Article 1.1. of the EU Framework Decision on the fight against organised crime, Article 2 of the EU Council Framework Decision on combating terrorism[84] contains the more specific "offences relating to a terrorist group". These offences include "participating in the activities of a *terrorist group*, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group". There is no requirement that perpetrators act in pursuit of a financial objective. This wording is not limited to recruiting and training for terrorism but broadly covers all types of IT-based support given to a terrorist group, irrespective of its – political or financial – goals.[85]

5.2.3.3 Summary and Evaluation

The analysis mentioned above shows that no computer-specific problems arise when treating communication activities as participation or when treating advanced planning activities as attempt. Thus, just as *the general rules on attempt and participation* can be applied to traditional acts outside the IT area, they can be used when terrorists communicate with each other online or prepare their attacks with the help of computer systems. As a consequence, there is no computer-specific gap with respect to terrorist use of the Internet.[86]

For this reason, one might only raise the question of whether the criminalisation of preparatory acts in support of *terrorist organisations* should be extended. As shown above,[87] Article 2 of the EU Council Framework Decision on combating

[83] However, in comparison to the UN Convention, the Framework Decision only focuses on criminalizing participation in a criminal organisation or agreements to conduct serious crimes. The UN Convention against Transnational Organized Crime additionally aims at criminalizing corruption, the laundering of proceeds of crime and the obstruction of justice, see 5.2.3.2, supra.

[84] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002), as amended by Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

[85] For the activities of the EU, see also the Communication from the Commission to the European Parliament and the Council concerning terrorist recruitment: addressing the factors contributing to violent radicalisation, 21.9.2005, COM (2005) 313 final.

[86] For an analysis of the various legislative techniques employed to provide for the early onset of criminal liability, see Sieber (2006), pp. 27–40; Sieber (2009), pp. 353–408.

[87] 5.2.2.3.

terrorism[88] covers all acts of "participating in the activities of a *terrorist* group". In contrast, Article 5.1 (a) of the UN Convention against Transnational Organized Crime[89] and Article 2 (a) of the EU Council Framework Decision on combating organised crime[90] prohibit taking an active part in the criminal activities of an *organised criminal group* or *criminal organisation* that – according to Article 2 (a) of the UN Convention and Article 1.2 of the Framework Decision - must have the aim of committing serious crimes in order "to obtain … a financial or other material benefit". This difference between the "terrorist-specific approach" of the EU Council Framework Decision on combating terrorism (specifically directed at politically motivated terrorist groups) and the "organized crime approach" of the UN Convention against Transnational Organized Crime as well as the EU Council Framework Decision on combating organised crime (limited to organised criminal associations with serious financial benefit crimes) illustrates the question of whether the broader approach of criminalising support for a terrorist organisation should also be implemented on a more global level in a convention of the Council of Europe or the UN.[91]

However, this general question goes beyond the scope of the present analysis, with its focus on cyberterrorism and other terrorist use of the Internet. Dealing with the question of a terrorist-specific group offence would cause difficulties relating to defining the respective terrorist act (e.g. by referring to the special UN conventions or by creating a general definition of terrorism) and would have to address the question of how legal uncertainty, over-criminalisation, and abuse of such a broad "material support provision" could be prevented. In addition, one would have to consider that many preparatory acts (such as public provocation of terrorism, recruitment, training, and financing) are already covered by the above-mentioned specific rules in the CoE Convention on the Prevention of Terrorism Convention.

5.3 Developing and Harmonizing National Criminal Procedure and Preventive Measures

New forms of cybercrime as well as the commission of traditional crimes in computer networks pose new, computer-specific problems not only with respect to substantive criminal law but also for the investigation, prosecution, and prevention

[88] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (OJ L 164/3 of 22.6.2002) as amended by Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

[89] With respect to the financing of terrorism, this Convention is more specific and far-reaching than the aforementioned UN International Convention for the Suppression of the Financing of Terrorism. See United Nations Convention Against Transnational Organized Crime of 8.1.2001 (A/Res/55/25).

[90] EU Council Framework Decision 2008/841/JHA of 24.10.2008 on the fight against organised crime (OJ L 300/42 of 11.11.2008).

[91] The same question applies to the "conspiracy approach" of Article 5.1. (a) (i) of the UN Convention against Transnational Organized Crime and Article 2 (b) of the EU Council Framework Decision on the fight against organized crime.

of crime. These problems stem from a variety of sources: the complex technical environment of computer systems; the multitude and invisibility of computer data; the techniques of encryption and steganography; the difficulty of identifying perpetrators on the Internet; the fact that computer systems can be attacked from a distance; and the global nature of the Internet, which cannot be controlled by purely national measures. Thus, special procedures are essential for investigations of criminal activity on the Internet and in other IT environments.

Legal rules for these computer-specific investigations can be found on the international level in the CoE Cybercrime Convention. In addition, there are other instruments with special procedural rules addressing problems of international cooperation, namely: (1) computer-specific investigations, (2) financial investigations, and (3) investigations in terrorist and other cases. These are briefly analysed next.

5.3.1 Computer-Specific Investigations

CoE Convention on Cybercrime of 2001

The development of the CoE Convention on Cybercrime[92] was not only a success with respect to substantive criminal law but also a breakthrough in the international development of computer-specific investigations in computerised environments. In addition to dealing with substantive criminal law, the Cybercrime Convention obliges parties to adopt a variety of legislative measures for computer-specific investigations. These measures are laid down in Articles 14–22 of the Convention. They cover, among other things, the expedited preservation of stored computer data, the expedited preservation and partial disclosure of traffic data (necessary for tracing attacks back to their origin), production orders to submit specified computer data, search and seizure of stored computer data, real-time collection of traffic data, interception of content data, conditions and safeguards for these measures, as well as jurisdictional rules.[93]

These specific investigation methods are key for successful Internet investigations, both in general and specifically in terrorist cases. This is obvious, for example, if the perpetrators do not attack other computers directly but "jump" via a number of third-party computer systems that they hijack, control, and abuse as intermediaries in order to shield the identity of their own system. Using this technique, an attack from country A on country B can proceed via numerous computer systems in many jurisdictions. Because the victim can – at best – identify only the "direct" attacker, the process of tracing and identifying the perpetrator often depends on the analysis of the traffic data of many computer systems in numerous countries. Because these traffic data are often not stored by Internet providers – or not stored for a long period of time – the implementation of common traceback procedures requires rules for "quick freeze procedures" of data that would otherwise be erased

[92]Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185).

[93]For details, see Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, Nos. 131–239.

and/or obligations for providers to retain traffic data for a certain period of time. The Council of Europe's Cybercrime Convention concentrates on such specific "quick freeze" provisions (differentiating between a fast "quick freeze" and the later transfer procedure). The corresponding procedure of expedited preservation of data is a completely new measure of criminal law.

Additional specific rules concern other specialised instruments, for example, with respect to search and seizure in connected computer systems (which might be located in different countries), or production orders to submit specified computer data (which are often difficult for the prosecution to access either due to the encryption of data or due to the technical problems of dealing with IT applications unfamiliar to the investigators). These examples show that the Cybercrime Convention is designed to address the special problems of investigations in the IT environment and is the central instrument for procedural measures and for international cooperation in the area of cybercrime.

Consequently, it is necessary to ensure that the specialised procedural provisions of the Cybercrime Convention are applicable in cases involving the use of the Internet for terrorist purposes. The relevant scope of the procedural provisions of the Cybercrime Convention is regulated in Article 14: "Each Party shall apply the powers and procedures" of section 2 of the Convention (Articles 14–21) to "(a) the criminal offences established in accordance with Articles 2–11 of this Convention; (b) other criminal offences committed by means of a computer system; and (c) the collection of evidence in electronic form of a criminal offence".

This leads to a clear result: Subsections (b) and (c) guarantee that – subject to the two exceptions in Article 14 paragraph 3 subsections (a) and (b) – the special investigation methods of the Cybercrime Convention can be applied to all kinds of criminal activities on the Internet.[94] As a consequence, it is safe to say that there are no gaps in coverage regarding the use of existing computer-specific procedural provisions of the Cybercrime Convention to investigate cyberterrorism and other forms of terrorist use of the Internet. Thus, the only question that arises is whether the instruments of the Convention are adequate and up-to-date (see infra 5.3.4.2).

EC Directive on Data Retention of 2006

Whereas the goal of the Cybercrime Convention is to address all procedural problems in a computerised environment, the EC Directive on the retention of data of publicly available electronic communication services[95] only deals with a specific

[94] For details, see Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, Nos. 140–148. See also Article 8 of the "Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems" of 28.1.2003 (ETS No. 189) confirming that the relevant articles of the Cybercrime Convention are applied to the crimes defined in the Additional Protocol.

[95] Directive 2006/24/EC of the European Parliament and the Council of 15.3.2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services of public communication networks and amending Directive 2002/58/EC (OJ L 105, 13.4.2006), pp. 54–63.

issue that could not be agreed on during the drafting of the Cybercrime Convention: as explained above, successful investigation on the Internet and in other electronic networks depends to a large degree on the ability to trace back perpetrators to their original computer system. Ordinary traceback procedures require that certain traffic data be stored so that they can be used in an investigation that in many cases may not take place until some time after the crime has occurred. Thus, the EC Directive on the retention of data of publicly available electronic communication services obligates Member States to adopt measures providing that certain traffic data and location communication services be retained for periods of not less than 6 months and not more than 2 years from the date of the communication (with exceptions in Article 12 of the Directive).

Such retention of data could be especially useful for the investigation of terrorist activity. It cannot fully be replaced by the "quick freezing" of traffic data provided for by the Cybercrime Convention because quick freezing of traffic data cannot take place if the data have not been stored. However it could allow for a shortening of the retention period, thus reducing the impact on the data protection interests of Internet users.

5.3.2 Financial Investigations

Specific investigative mechanisms and other measures beyond those contained in the Cybercrime Convention can be found in the context of special financial investigations with respect to money laundering and the financing of terrorism. Such measures are regulated in the instruments against the laundering of the proceeds from crime and against the financing of terrorism.

The CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime[96] contains specific measures on confiscation, investigation, freezing, seizure and confiscation, preventive measures, as well as provisions establishing financial intelligence units (FIUs). According to Article 2 of the Convention, parties must ensure that the provisions are applicable to search, trace, identify, freeze, seize, and confiscate property used for the financing of terrorism or the proceeds of this offence.[97]

Similar measures are found in the UN International Convention for the Suppression of the Financing of Terrorism[98] or – with respect to organised crime – in the UN

[96]Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 16.5.2005 (ETS No. 198).

[97]"Financing of terrorism" means the acts set out in Article 2 of the UN International Convention for the Suppression of the Financing of Terrorism of 1999, UN Treaty Series Reg. No. 38349, adopted by the General Assembly of the United Nations in Resolution 54/109 on 9.12.1999.

[98]UN International Convention for the Suppression of the Financing of Terrorism of 1999, UN Treaty Series Reg. No. 38349, adopted by the General Assembly of the United Nations in resolution 54/109 on 9.12.1999.

Convention against Transnational Organized Crime.[99] The same is true of UN Security Council Resolution 1373,[100] according to which all States must implement a variety of measures against terrorism, such as preventing and suppressing the financing of terrorist acts, freezing financial assets of terrorists, preventing acts of terrorism, affording measures of assistance, providing effective border controls, creating provisions of early warning, exchanging information, identifying the whereabouts and activities of persons, and conducting inquiries with respect to the movement of funds relating to the commission of such offences.

None of these instruments depends on whether the offences are committed with the assistance of IT systems. Thus, there are no gaps in these instruments with respect to their applicability in an IT environment.

5.3.3 Terrorist-Specific Investigations

Other conventions on terrorism include either specific or general rules on investigation. For example, the Council of Europe Convention on the Prevention of Terrorism[101] not only creates obligations to criminalise illegal content but also contains general procedural provisions with respect to these offences. The same is true for the UN Convention against Transnational Organized Crime.[102] As far as national procedural law is concerned, these obligations include the establishment of certain conditions and safeguards, the protection of victims, the establishment of jurisdiction, and the duty to investigate.

Additional regulations are contained in general instruments on mutual assistance and extradition, such as the European Convention on Mutual Assistance in Criminal Matters and its two additional protocol,[103] as well as in the European Convention on Extradition and its two additional protocols.[104] Because these general rules on investigation have been drafted broadly, it is not a problem to apply the provisions to cyberterrorism and to other use of the Internet for terrorist purposes.

---

[99] United Nations Convention against Transnational Organized Crime of 8.1.2001 (A/Res/55/25).

[100] UN Security Council Resolution 1373 (2001) of 28.9.2001.

[101] Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196).

[102] United Nations Convention against Transnational Organized Crime of 8.1.2001 (A/Res/55/25).

[103] European Convention on Mutual Assistance in Criminal Matters of 20.4.1959 (ETS No. 30); Additional Protocol on the European Convention on Mutual Assistance in Criminal Matters of 17.3.1978 (ETS No. 99); Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8.11.2001 (ETS No. 182).

[104] European Convention on Extradition of 13.12.1957 (ETS No. 24) and its additional protocols of 15.10.1975 (ETS No. 86) and of 17.3.1978 (ETS No. 98).

5.3.4 Evaluation and Consequences for Legal Policy

5.3.4.1 General Evaluation

The analysis shows that – like the *rules of substantive criminal law* – the procedural rules of the Cybercrime Convention are also applicable with respect to all use of the Internet for terrorist purposes and that the main problems of national procedural law with respect to terrorist use of the Internet are addressed by the Cybercrime Convention. This is primarily due to the fact that the computer-specific investigation measures contained in Article 14 of the Cybercrime Convention apply not only to computer-specific offences defined in the Convention but to all "other criminal offences committed by means of a computer system" and to the "collection of evidence in electronic form of a criminal offence" as well. This includes all types of terrorist use of the Internet and other computer systems. Furthermore, it is not a problem to apply the special investigation methods of the international instruments for financial and terrorist cases to the IT environment. As a consequence, there are no gaps in the application of the existing international rules on national criminal procedure to cyberterrorism or to other terrorist use of the Internet.

5.3.4.2 Checking the Contemporariness of the Cybercrime Convention

The only questions that remain open are whether the procedural instruments of the Cybercrime Convention are adequate for the investigation of cases of suspected terrorism and whether they are up-to-date. Despite some criticism concerning the lack of transparency in the historical development of its provisions and a resulting lack of concrete safeguards for the protection of civil liberties,[105] it is widely acknowledged that the investigation methods described in the Cybercrime Convention are well-designed and essential for the efficient investigation of computer systems. In addition, special procedural conditions and safeguards are taken into account by Article 15, which refers to the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.[106] As a consequence, and especially with a view to the difficult process of drafting international conventions, there are no grounds for jeopardizing the signing and ratification of the Convention by reconsidering the regulated issues. Thus, in order to avoid safe havens for cybercriminals and terrorists, the message should be clear to sign and ratify the *Cybercrime Convention*.

---

[105] See Article 15 of the Convention and Breyer (2001), p. 594; Dix (2001), p. 588 f.; Gercke (2004), p. 783; Taylor (2002). See also the comments of the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International on Draft 27 of the CoE Convention on Cybercrime at http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm [last visited: 25 February 2009].

[106] For details, see Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, Nos. 145–148.

However, because the Cybercrime Convention was drafted between 1997 and 2000, because the technical environment and the available forensic investigation tools change rapidly, and because terrorism creates special risks, the necessity and possibility of updating the procedural tools in an *additional protocol* to the Cybercrime Convention should be explored. Such a protocol might address, for example, the clandestine use of hacking techniques employed by the police when searching computer systems online (so-called "clandestine online searches"): An effective international cooperation under traditional mutual assistance rules requires that *all* parties have similar provisions in these areas and that these measures also be taken up in the rules on international cooperation. If, for example, state A requests another state to conduct online searches, such measures must be possible in both state A and in the requested state. Similar problems arise with other types of forensic software, for example the clandestine installation of a key logger program on the computer system of a suspect in order to circumvent his or her encryption (which should be discussed as an alternative to highly problematic solutions such as limitations on encryption or encryption key escrow procedures). Another controversial issue has to do with the period of time during which traffic data should be stored.[107] Even if these questions were discussed by the drafters of the Cybercrime Convention, they should be reconsidered in light of the new criminological, technical, and forensic developments and of the new risks posed by terrorism. In addition, if specific solutions are rejected, this should be communicated to Member States so that they can avoid adopting the rejected approaches.

5.3.4.3 Preventive Procedures with Respect to Illegal Content

An additional protocol to the Cybercrime Convention would also be a possibility with respect to preventive measures dealing with the deletion or blocking of illegal content. In the context of search and seizure, Article 19 of the Cybercrime Convention not only empowers competent authorities to seize or similarly secure a computer system but also permits the authorities to "render inaccessible or remove those computer data in the accessed computer system". However, the Convention does not say how this should be done with respect, for example, to data on the Internet, and the search and seizure provision of Article 19 cannot replace a general regulation for blocking Internet data.[108] Moreover, the legal, procedural, and technical questions of blocking illegal content on the Internet are highly complex and controversially discussed all over the world. Resolution of these questions would require not only the participation of lawyers but also that of specialists in the field of computer systems and networks. Furthermore, the technical problems in this area are exacerbated because a possible

[107] Abuses of third-party computers for attacks involving mass queries raise the additional question of the necessity of creating obligatory security measures.

[108] For the interpretation of this clause, see Council of Europe, Convention on Cybercrime, Explanatory Report (ETS No. 185), Nos. 196–199 (especially the indication in No. 199: "seize or similarly secure data has two functions").

control of illegal content cannot be limited to illegal websites on the Internet but should also be extended to content disseminated by other Internet services (such as Internet relay chat) or to media disseminated via mobile phones (such as video uploading). Any approach to illegal content on the Internet will also require a difficult balancing of security interests and human rights, a task for which the Council of Europe, as an international institution, would be ideally suited.

As far as practical results are concerned, there is the risk that no perfect or even adequate solution can be found for blocking access to illegal content on the Internet in the future because of the extreme difficulty of controlling the Internet and global cyberspace. However, in this case, even a rejection of possible solutions would be extremely helpful for reasons of legal certainty. Rejection could also help prevent a situation in which states enact control mechanisms that are ineffective and doomed to failure and that create risks for the free flow of information and privacy rights. Thus, working on global solutions for the prevention of illegal content on the Internet could be a promising task for the Council of Europe, an institution dedicated both to the prevention of crime and to the protection of freedom.

However, an evaluation of the up-to-dateness of the procedural measures of the Cybercrime Convention as well as the development of preventive measures for illegal content is not a problem specific to cyberterrorism and other uses of the Internet by terrorists but rather is an issue that arises in the context of organised crime, economic crime, and all other forms of crime as well. Thus, as indicated above, a broader approach that would go beyond the scope of cyberterrorism and the use of the Internet for terrorist purposes should be considered.[109]

5.4 Improving International Cooperation

5.4.1 Cooperation in Computer-Specific Cases

CoE Cybercrime Convention of 2001

The special investigation problems encountered in computerised environments, especially in global cyberspace, require not only computer-specific investigation measures but also corresponding rules for international legal cooperation when dealing with these measures. Again, the most highly developed regime of rules of international legal cooperation is found in the Cybercrime Convention of the Council of Europe of 2001, specifically in Chapter III of the Convention.[110] Article 24, for example, consists of an extradition provision applicable in cases involving the computer-specific offences established in accordance with Articles 2–11, provided that they are punishable under the laws of both parties concerned (double criminality requirement). Chapter III also contains detailed computer-specific provisions

[109] See Sieber in: Waltermann/Machill (2000), p. 319 ff. See also Sieber (2009), p. 653 ff.

[110] Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185).

for mutual assistance, including cooperation in the areas of expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing of stored computer data, real-time collection of traffic data, and interception of content data. It also provides general principles relating to mutual assistance, confidentiality, and limitation of use, and it addresses the issue of spontaneous information.[111] Article 27 subsection 4 allows a requested party to refuse assistance if the request concerns an offence that the requested party considers a political offence or if it considers it likely that execution of the request will prejudice its sovereignty, security, *ordre public*, or other essential interests.

According to Article 22.1 (a)–(d) of the Cybercrime Convention, a state party shall establish jurisdiction over any of the offences laid down in Articles 2–11 when the offence is committed (a) in its territory, (b) on board a ship flying the flag of that Party, (c) on board an aircraft registered under the laws of that Party, or (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. In case of conflict of jurisdiction, Article 22.5 provides that "the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution". However, Article 22.2 grants state parties the right not to apply or to apply only in part the rules of Article 22.1 (b)–(d).

The Cybercrime Convention also puts great emphasis on practical cooperation. Article 35 requires each party to designate "a point of contact available on a 24-h, 7-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence". Such assistance includes the provision of technical advice, the preservation of data pursuant to Articles 29 and 30, the collection of evidence, the provision of legal information, and the locating of suspects.[112]

As in the case of procedural rules, the scope of the provisions on cooperation is broad, covering not only the specific offences of the Convention but all "criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence" (Article 23). The obligation to cooperate regarding this broad class of crimes was agreed upon because there is the same need for close international cooperation in all these cases. Only Articles 24 (extradition), 33 (mutual assistance regarding the real-time collection of traffic data), and 34 (mutual assistance regarding the interception of content data) permit the parties to provide for a different scope of application of these measures.[113] Thus, the special cooperation proceedings of the Cybercrime Convention can also be used for cyberterrorism and for all other types of terrorist activity on the Internet.

---

[111] For details, see Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, Nos. 240–302.

[112] For details, see Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, No. 297–302.

[113] For details, see Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185), Explanatory Report, Nos. 243, 245, 253.

EU Council Framework Decision on Attacks against Information Systems of 2005

Following the CoE Cybercrime Convention, the European Union Council Framework Decision on Attacks against Information Systems of 2005[114] also included some concise measures of cooperation, such as the set-up of operational points of contact available around the clock 7 days a week.

As far as jurisdiction is concerned, Article 10 of the Framework Decision contains a clause that is more sophisticated than Article 22 of the Cybercrime Convention. According to Article 10.1, a Member State shall establish jurisdiction when one of the relevant offences has been committed within its territory, by one of its nationals, or for the benefit of a legal person that has its head office in the territory of that Member State. Article 10.2 further clarifies that jurisdiction shall include both cases in which the offender commits the offence when physically present on the Member State's territory (regardless of where the information system is located) and cases in which the offence is directed against an information system on the Member State's territory (regardless of where the offender is at the time of commission). Article 10.4 finally lays out a complex conflict rule: in case of conflict of jurisdiction, the Member States concerned shall cooperate in order to resolve their conflict; they shall do so if necessary under the auspices of any possible body or mechanism established within the EU; and they may finally consider, as a rule of preference, that jurisdiction is established sequentially in the Member State's territory in which the offence has been committed, in the Member State of which the perpetrator is a national, and in the Member State in which the perpetrator has been found.[115]

5.4.2 Cooperation in Cases of Money Laundering and the Financing of Terrorism

The special international instruments against money laundering and the financing of terrorism described above also provide for specific cooperation rules:

- The CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.[116]
- The UN International Convention for the Suppression of the Financing of Terrorism.[117]

---

[114] EU Union Council Framework Decision 2005/222/JHA of 24.2.2005 on attacks against information systems (OJ L 69/67 of 16.3.2005).

[115] However, judging by the wording of Article 10.4, it remains unclear whether this rule of precedence is optional or obligatory and what is meant by the wording "sequentially".

[116] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism of 16.5.2005 (ETS No. 198).

[117] UN International Convention for the Suppression of the Financing of Terrorism of 1999, UN Treaty Series Reg. No. 38349, adopted by the General Assembly of the United Nations in Resolution 54/109 on 9.12.1999.

- UN Security Council Resolution 1373 of 2001.[118]
- UN Security Council Resolution 1535.[119]

The rules in these financial investigation instruments on cooperation apply regardless of whether or not the perpetrators made use of computer systems.

5.4.3 Cooperation in Terrorist Cases

Rules on cooperation are also provided in the various conventions, protocols, and decisions that address terrorism:

- The Council of Europe Convention on the Suppression of Terrorism as amended by the Protocol of 2003[120] focuses on issues of extradition and specifically deals with extradition in "political cases". For the purpose of extradition, Article 1 excludes the political offence exception for a list of offences including, for example, the unlawful seizure of an aircraft, offences against internationally protected persons, kidnapping, and offences involving bombs. According to Article 2, the decision not to regard an offence as a political offence can be extended to other acts of violence and acts against property if the act created a collective danger for persons. According to Article 8, Contracting States may not refuse requests for mutual assistance based on the fact that the request concerns a political offence.
- The Council of Europe Convention on the Prevention of Terrorism[121] deals with international cooperation in prevention and in criminal matters. Article 20 excludes the political exception clause for extradition and mutual assistance. However, any party may, in a reservation, declare that it reserves the right not to apply this paragraph.
- The European Union has additional, more specific rules on cooperation. For example, the EU Council Decision of 2005 on the exchange of information and cooperation concerning terrorist offences[122] is designed to improve cooperation in cases of terrorist offences by regulating practical measures. Each Member State must designate a specialised service within its police services that will have access to and collect all relevant information resulting from criminal investigation and prosecution with respect to terrorist offences and that will send the informa-

[118] UN Security Council Resolution 1373 (2001) of 28.9.2001.

[119] UN Security Council Resolution 1535 (2004) of 26.3.2004.

[120] The European Convention on the Suppression of Terrorism of 27.1.1977 (ETS No. 90) as amended by the Protocol of 15.5.2003 (ETS No. 190). The Additional Protocol to the Convention on the Suppression of Terrorism of 2003 addresses offences within the scope of the Convention for the Suppression of the Financing of Terrorism with new rules on reservations.

[121] Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (ETS No. 196).

[122] EU Council Decision 2005/671/JHA of 20.9.2005 on the exchange of information and cooperation concerning terrorist offences. OJ L 253, 29.9.2005, pp. 22–24.

tion to Europol or Eurojust, respectively. The Decision also provides for the establishment of joint investigation teams. Furthermore, specific provisions of cooperation, extradition, and surrender stipulated in the EU Council Framework Decision on the European arrest warrant of 2002[123] are applicable to offences of terrorism. According to Article 2.2 of the Framework Decision, the issuing of a European arrest warrant does not require the verification of the double criminality of the act for offences of "terrorism" and "computer-related crime".

- Most other instruments against terrorism also contain general provisions on international cooperation. This is true of the UN conventions and protocols against specific acts of terrorism (such as bombing) discussed above.[124] These conventions each contain a provision according to which the defined offences must be deemed extraditable offences in any existing treaty between State parties.[125] In addition, for purposes of extradition, offences shall be treated as if they had been committed not only in the place where they occurred but also in the territory of the states that have established jurisdiction under such a convention. The conventions also contain special provisions that exclude the political offence exception, for example, Article 11 of the Convention for the Suppression of Terrorist Bombings, Article 15 of the Convention for the Suppression of Acts of Nuclear Terrorism, Article 16 No. 14 of the UN Convention against Transnational Organized Crime, and Article 9 Sec. 1a of the Hostages Convention.

For these provisions, again, it is irrelevant whether the perpetrator committed the defined acts with the support of a computer system. Thus, there are no computer-specific gaps in any of these instruments.

5.4.4 Cooperation in General Cases

Particularly in cases in which there are no applicable specific cooperation agreements for cybercrime, terrorism, or money laundering, mutual assistance in criminal matters and extradition are regulated by general conventions and protocols. These instruments contain broad grounds for refusals to cooperate, such as for

[123] EU Council Framework Decision 2002/584/JHA of 13.06.2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190/1 of 18.7.2002).

[124] See 5.2.1.2, supra.

[125] E.g. Article 8 of the Convention for the Suppression of Unlawful Seizure of Aircraft of 16.12.1970, UN Treaty Series Reg. No. 12325; Article 8 of the Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons of 14.12.1973, UN Treaty Series Reg. No. 15410.; Article 11 of the Convention on the Physical Protection of Nuclear Material of 3.3.1980, UN Treaty Series Reg. No. 37517; Article 11 of the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation of 10.3.1988, UN Treaty Series Reg. No. 29004; Article 9 of the Convention for the Suppression of Terrorist Bombing of 15.12.1997, UN Treaty Series Reg. No. 37517; Extradition Exception Clause Article 9 of the Convention Against the Taking of Hostages of 17.12.1979, UN Treaty Series Reg. No. 21931.

political offences or with respect to the *ordre public*. This is true, e.g., of the European Convention on Mutual Assistance in Criminal Matters and its two additional protocols[126] as well as the European Convention on Extradition and its two additional protocols.[127] These conventions are applicable to both computer-specific and non-computer-specific crimes.

5.4.5 Evaluation and Consequences for Legal Policy

5.4.5.1 General Evaluation

The cooperation agreements that specifically address cybercrime are applicable to all kinds of cyberterrorism and other use of the Internet for terrorist purposes. Thus, the detailed cooperation procedures of the Cybercrime Convention are available to cases of terrorist use of the Internet. These procedures are the most important instruments for the identification and prosecution of terrorism on the Internet. Similarly, the instruments that address international cooperation in financial, terrorist, and other general investigations can be applied in an IT environment, thereby also enabling investigations of all types of terrorist activities involving the use of computer systems.

5.4.5.2 Political Offence Exception Clause

The only question that remains open is whether the existing international instruments of cooperation should be amended or updated. This question is particularly relevant with respect to the fact that – unlike many of the existing conventions on terrorism – the Cybercrime Convention permits a refusal to cooperate for political reasons. Such a result could be changed by the introduction of a special provision on cyberterrorism committed by attacks against computer infrastructures to which the political offence exception would not apply (an option not favoured above). Another option would be to exclude the political offence exception for specific serious acts in the Cybercrime Convention. This would be beneficial to international cooperation. It would also be in accordance with the trend – described above – towards abandoning the political offence exception in serious cases of terrorism. However, even conventions that exclude the political offence exception may allow state parties to opt out of the exclusion by means of a reservation (Article 20 of the CoE Convention on the Prevention of Terrorism, for example). Thus, international efforts

[126] European Convention on Mutual Assistance in Criminal Matters of 20.4.1959 (ETS No. 30); Additional Protocol on the European Convention on Mutual Assistance in Criminal Matters of 17.3.1978 (ETS No. 99); Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 8.11.2001 (ETS No. 182).

[127] European Convention on Extradition of 13.12.1957 (ETS No. 24) and its additional protocols of 15.10.1975 (ETS No. 86) and of 17.3.1978 (ETS No. 98).

with respect to the political offence exception in the Cybercrime Convention and in other conventions are not a priority. However, in the process – recommended above – of evaluating and updating the procedural provisions of the Cybercrime Convention, exclusion of the political offence exception should be considered for certain offences, such as data and system interference, in serious cases.[128]

5.4.5.3 Specific Cooperation With Respect to the Prevention of Illegal Content

A more serious need for improving international cooperation, again, exists with respect to the prevention of illegal content on the Internet. As described above, it is obvious that specific international cooperation mechanisms are necessary for the establishment of the accessory liability of Internet providers, for "notice and takedown" procedures, for the development of new forms of self-regulation, for public–private "co-regulation", as well as for national instruments for removing and blocking illegal content. These efforts include, but are not limited to, improvements in the sharing of information and allocating of tasks in the control of global cyberspace. Because purely national control and blocking mechanisms on the Internet are often doomed to failure, effective solutions depend to a great extent on close international cooperation or action on a supranational level. To the extent that the global cooperation of states is essential for such solutions, soft sanctions applicable to non-complying states would be useful, such as those found in the international system of money laundering of the Financial Action Task Force (FATF) of the OECD. Efforts with respect to these issues might lead to an increase in international cooperation with regard to the Internet. A deeper analysis of the new regulatory questions might even lead to the conclusion that the global cyberspace is a common heritage of mankind that – like the high seas – requires new mechanisms of supranational governance implemented by means of new institutions. Thus, in addition to the support for signing, ratification, and implementation of the Cybercrime Convention, these questions merit further efforts with respect to illegal terrorist content as well as other illegal content in a more general context.

5.5 Summary

5.5.1 Use of the Internet for Terrorist Purposes

Cyberterrorism against or by means of the Internet poses a significant risk because computer systems today are responsible for carrying out many essential functions of society. As a consequence, *attacks via the Internet* could cause damage not only

[128] In this context, it is worth noting that the EU Council Framework Decision 2002/584/JHA of 13.6.2002 on the European arrest warrant and the surrender procedures between Member States does not contain a political offence exception clause.

to the IT infrastructure and essential electronic communication systems but also to other infrastructures, systems, and legal interests, such as nuclear power stations, electrical supply systems, air control systems, medical computer systems, public administrations, and private companies, all of which depend on the functioning of IT. Interference with many of these systems can also cause harm to the life or well-being of persons. Yet, at this time, very few cases involving these kinds of attacks are known to the public.

However, a primary use of the Internet and other electronic communication systems consists in the *public dissemination of illegal content*. The Internet and other communication systems are abused by terrorists in order to threaten the commission of terrorist acts; to incite, advertise, and glorify terrorism; to engage in fundraising for and financing of terrorism; to provide training for terrorism; to recruit for terrorism; and to disseminate racist and xenophobic material. In sum, the Internet has become an important tool by which terrorists send their messages to a broad audience.

In addition, the Internet and other computer systems play a significant role in the *logistical preparation of terrorist offences*, including internal communication, acquisition of information (e.g. on bomb building, hostage taking, or hijacking), analysis of targets, and other forms of information gathering.

5.5.2 Applicability of Existing Conventions

The existing international conventions and other instruments for the harmonisation of national substantive and procedural law and for international cooperation are applicable to the prosecution of cyberterrorism and other use of the Internet for terrorist purposes. The computer-specific provisions of the Council of Europe's Cybercrime Convention on national substantive law, national procedural law, and international cooperation can all be applied to the cases of terrorism analyzed above. For computer-specific reasons, all destructive attacks via the Internet require interference with data, i.e. offences that fall under the substantive law provisions on data and system interference of the Cybercrime Convention. The applicability of the computer-specific procedural rules and the international cooperation law of the Cybercrime Convention to all types of terrorism is due to the fact that the application of the special provisions of the Cybercrime Convention that deal with procedural law and international cooperation law is defined broadly and is not limited to cybercrime. Similarly, the substantive, procedural, and cooperation rules of the international instruments on terrorism, on money laundering, on the financing of terrorism, and on mutual assistance or extradition are also applicable to cyberterrorism because they are worded generally and thus can apply in an IT environment.

Consequently, the primary question posed in this report concerning the existence of "terrorist-specific" gaps in "computer-specific" conventions and "computer-specific gaps" in "terrorist-specific conventions" can be answered in the negative as far as the application of the Cybercrime Convention and other instruments is concerned.

As a result, only the second question posed remains: whether these instruments have *general gaps*, i.e. gaps that are not specific to the use of the Internet for terrorist purposes. As explained above, this analysis cannot provide a general "super-evaluation" of all relevant international instruments on cybercrime and/or terrorism and their possible gaps with respect to the prosecution of crime and the protection of civil liberties. However, the analysis has shown the major problems relevant for both cyberterrorism and for the use of the Internet for terrorist purposes.

5.5.3 General Problems of Existing Conventions

(a) The major problem facing all existing international instruments is the lack of *signatures, ratifications, and implementations*. Broad acceptance is especially important for the Cybercrime Convention as well as for the Convention on the Prevention of Terrorism, which are the most important international instruments for fighting cyberterrorism and other terrorist use of the Internet. The role of the Cybercrime Convention is essential not only for substantive criminal law (with the Convention's important provisions on data interference and system interference) but also for criminal procedure and the law of international cooperation (with the Convention's highly specialised investigation and cooperation tools). The Convention on the Prevention of Terrorism is decisive with respect to the creation of adequate substantive criminal law provisions for illegal content. Thus, in the future, serious efforts should be made to promote the process of signing, ratifying, and implementing the Convention.

(b) As a consequence, all additional efforts both within and beyond the present scope of the Cybercrime Convention should be pursued in such a way so as not to hinder or distract from signature, ratification, and implementation.
Thus, the discussion of possible amendments and updates to the *Cybercrime Convention* in the quickly changing IT environment should be undertaken only with the aim of a possible *additional protocol* to the Convention, which would recognise the Convention as its basic mother convention. In such a process, the *Cybercrime Convention* should be evaluated with regard to its ability to cover newly emerging technical advances, particularly new forensic investigative techniques (such as online searches or the use of key logger software). In the fast-paced, technical environment of cybercrime, such evaluations, which frequently lead to revisions and updates, are an absolutely normal process, especially when dealing with high risks such as those posed by terrorism.

Should a decision be taken to supplement the Cybercrime Convention with a follow-up protocol addressing new investigative techniques, the possibility of excluding the political exception clause for some of its offences – especially in serious cases of data and system interference – could also be considered, thus following the trend of other cooperation instruments, particularly in clearly defined cases of terrorism.

In addition, the option of adopting a new provision prohibiting serious attacks on IT-based or general infrastructures could be discussed. The advantage of such a provision, however, would be limited and such a provision is not recommended by this report. It is sufficient for countries to evaluate existing domestic statutes on data and system interference and to make sure that they provide appropriate sanctions for cases involving terrorist attacks against computer and other essential infrastructures and other legal interests. However, such "effective, proportionate and dissuasive sanctions" are already required by the Cybercrime Convention, and it can be left to the national legislatures to achieve this result by means of sentencing rules, aggravated offences on data interference, or infrastructure offences.

(c) An additional protocol to the *Convention for the Prevention of Terrorism* should also be considered in order to achieve full coverage of illegal terrorist content, particularly threats to commit terrorist acts. Currently, such threats are not adequately covered in the relevant Council of Europe conventions, and this deficit is not fully compensated by instruments of other international organisations. Considering the effects of threats to commit terrorist acts, a response is necessary. It would also be possible to cover this issue in a better and more systematic way in the specific UN conventions. However, such an approach would pose problems with respect to unspecified general threats because it is difficult to deal with such threats by means of the sector-specific approach taken by the UN.[129] Considering possible amendments to the terrorist specific conventions, in a future study, one might also analyse whether the EU approach of "participation in a terrorist organization" should be transferred to a wider CoE or UN level.

5.5.4 New Efforts With Respect to Illegal Content

Due to the frequent use of the Internet for the dissemination of illegal terrorist content, additional efforts should be made to develop repressive and preventive measures that are both effective and respectful of civil liberties. This could be done either with special regard to illegal terrorist content or – which is more advisable – in a more general way that would also cover other types of illegal content.

Effective standards for the prosecution and prevention of illegal content on the Internet could be achieved by means of an additional protocol to the Cybercrime Convention, which could contain new rules for national substantive law, national procedural law, law on international cooperation, soft law, as well as rules establishing public-private partnerships.[130] In the area of substantive law, effective prevention of illegal content not only needs harmonised rules on illegal content in the

[129] See 5.2.1.2, supra.

[130] The need for international action to deal with illegal content has been shown in all three areas dealt with above: national substantive law, national procedural law, and international cooperation law. See 5.2.3.3, 5.3.4, and 5.4.5, supra.

special part of criminal law (as in the Convention for the Prevention of Terrorism or in the Protocol to the Cybercrime Convention),[131] but also harmonised rules on the responsibility of Internet providers, which could be the basis of international notice and takedown procedures (as in the EC Directive on e-commerce).[132] The same is true with respect to rules on blocking illegal content on the Internet.[133] Such rules would require a difficult balancing of security interests and human rights, especially with respect to freedom of information rights. This is also true for the necessary provisions of procedural law and the law on international cooperation, both of which require specific regulations based on research on technical blocking and control mechanisms on the Internet and must take into consideration the consequences of such measures for the freedom of information. These questions are difficult but essential: open societies should not leave the Internet and other electronic communication systems vulnerable to the abuse of their adversaries. They should also refrain from enacting ineffective control methods of a purely symbolic nature that seriously infringe freedom of information rights and can lead to the development of uncontrolled surveillance.

As this chapter has shown, international instruments have provided for the criminalisation of cyberterrorist activities in many forms; the correct balance among regulations to ensure security and mechanisms to ensure that individual rights are adequately protected has yet to be found.

References

Bassiouni, M. C. (2001). *International Terrorism: Multilateral Conventions (1937–2001)*. Transnational Publishers: New York.

Breyer, P. (2001). *Cyber-Crime-Konvention des Europarats*. *Datenschutz und Datensicherheit*. Volume 25, pp. 592–600.

Coll, S., Glasser, S. B. (2005). Terrorists Turn to the Web as Base of Operations. *The Washington Post*. 7 August 2005, Section A01.

Council of Europe (2001). *Council of Convention on Cybercrime of the Council of Europe of 23.11.2001 (ETS No. 185)*. Explanatory Report.

Council of Europe (2005a). *Council of Europe Convention on the Prevention of Terrorism of 16.05.2005 (ETS No. 196)*. Explanatory Report.

Council of Europe (2005b). *Human Rights and the Fight Against Terrorism. The Council of Europe Guidelines*. Council of Europe Publishing: Strasbourg.

Denning, D. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In: Arquilla, J. *The Future of Terror, Crime and Militancy*. Rand: Santa Monica et al., pp. 239–288. Also online available at http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf [last visited: 25 February 2009].

[131] For a comparative analysis of the substantive criminal law provisions in the area of illegal content, see Sieber (1999).

[132] For a comparative analysis of the responsibility regime of Internet providers, see *Sieber* in: *Lederman/Shapira* (2001), pp. 231–292; for the situation in Germany, see *Sieber/Höfinger* in: *Hoeren/Sieber* (2009), Chapter 18.1, pp. 1–72.

[133] See Sieber and Nolde (2008). See also Sieber (2009), p. 653 ff.

Dix, A. (2001). Regelungsdefizite der Cyber-Crime-Konvention und der E-TKÜV. *Datenschutz und Datensicherheit*. Volume 25, pp. 588–591.

Foltz, C. (2004). Cyberterrorism, Computer Crime, and Reality. *Information Management & Computer Security*. Volume 12, No. 2, pp. 154–166.

Gercke, M. (2004). Cybercrime Konvention des Europarates. *Computer und Recht*. Volume 20, pp. 782–791.

Gercke, M. (2006a). "Cyberterrorismus" - Aktivitäten Terroristischer Organisationen im Internet. *Computer & Recht*. pp. 62–68.

Gercke, M. (2006b). The Slow Wake of a Global Approach Against Cybercrime. *Computer Law Review International*. pp. 140–145.

Hoeren, T., Sieber, U. (2007). *Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs*. Loose leaf. Beck: München.

Murphy, S. D. (2002). Contemporary Practice of the United States Relating to International Law. *American Journal of International Law*. Volume 96, pp. 956–983.

Nuotio, K. (2006). Terrorism as a Catalyst for the Emergence, Harmonization and Reform of Law. *Journal of International Criminal Justice*. Volume 4, pp. 998–1016.

Oeter, S. (2002). Terrorismus und Menschenrechte. *Archiv des Völkerrechts*. Volume 40, pp. 422–453.

Ramelsberger, A. (2007). Krieger im Internet. *Süddeutsche Zeitung*, p. 5. Also online available at http://www.sueddeutsche.de/politik/327/396114/text/[last visited: 25 February 2009].

Ribbelink, O. M. (2004). *Apologie du Terrorisme"and "Incitement to Terrorism*. Council of Europe Publishing: Strasbourg.

Secretary-General of the UN (2006). Protecting Human Rights and Fundamental Freedoms While Countering Terrorism. Report pursuant to the UN Resolution No. 60/158 of the UN General Assembly. A/61/353. http://daccessdds.un.org/doc/UNDOC/GEN/N06/526/78/PDF/N0652678.pdf?OpenElement [last visited: 25 February 2009].

Sieber, U. (1999). Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet – Eine strafrechtsvergleichende Untersuchung. Edited by the German Ministry of Justice in the series "recht". Forum Verlag: Mönchengladbach.

Sieber, U. (2000). Legal Regulation, Law Enforcement and Self-Regulation – A New Alliance for Preventing Illegal Contents on the Internet. In: Waltermann, J., Machill, M. *Protecting Our Children on the Internet. Towards a New Culture of Responsibility*. Bertelsmann Foundation Publishing: Gütersloh, pp. 319–400.

Sieber, U. (2001). Responsibility of Internet Providers: Comparative Analysis of a Basic Question of Information Law. In: Lederman, E., Shapira, R. *Law, Information and Information Technology*. Kluwer Law International: The Hague, pp. 231–292.

Sieber, U. (2004). *Punishment of Serious Crimes. A Comparative Analysis of Sentencing Law and Practice*. Ed. Iuscrim: Freiburg im Breisgau.

Sieber, U. (2005). The Threat of Cybercrime. In: Council of Europe (2005b). *Organised Crime in Europe. The Threat of Cybercrime. Situation Report 2004*. Council of Europe Publishing: Strasbourg, pp. 81–218.

Sieber, U. (2006). Grenzen des Strafrechts. *Zeitschrift für die gesamte Strafrechtswissenschaft*. Volume 119, pp. 1–68.

Sieber, U. (2009). Sperrverpflichtungen gegen Kinderpornografie im Internet: Bewertung und Weiterentwicklung des Gesetzentwurfs BT-Drucks. 16/12850 vom 5. 5. 2009. *Juristenzeitung*, Volume 64, pp. 653–662.

Sieber, U., Brunst, P. (2007). Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions. In: Council of Europe (2007). *Cyberterrorism – The Use of the Internet for Terrorist Purposes*. Council of Europe Publishing: Strasbourg, pp. 9–105.

Sieber, U., Höfinger, F. (2009). Allgemeine Grundsätze der Haftung. In: Hoeren, T., Sieber, U. *Handbuch Multimedia Recht. Rechtsfragen des elektronischen Geschäftsverkehrs*. Loose leaf. Beck: München, pp. 1–72.

Sieber, U., Nolde, M. (2008). *Sperrverfügungen im Internet. Nationale Rechtsdurchsetzung im globalen Cyberspace*. Duncker & Humblot: Berlin.

Sieber, U. (2009), Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt - Eine Analyse der Vorfeldtatbestände im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten". *Neue Zeitschrift für Strafrecht*. Vol. 29 (2009), pp. 353–408.

Taylor, G. (2002). *The Council of Europe Cybercrime Convention - A Civil Liberties Perspective*. http://www.crime-research.org/library/CoE_Cybercrime.html [last visited: 25 February 2009].

Thomas, T. L. (2003). Cyberplanning, Al Qaeda and the Internet: The Danger of "Cyberplanning". *Parameters*. Volume 33, No. 1, pp. 112–123. Also online available at http://www.iwar.org.uk/cyberterror/resources/cyberplanning/al-qaeda.htm [last visited: 25 February 2009].

Tomuschat, C. (2005). Council of Europe Committee of Experts on Terrorism (CODEXTER), Strasbourg. on the Possible "Added Value" of a Comprehensive Convention on Terrorism. *Human Rights Law Journal*. Volume 26, pp. 287–306.

U.S. Army Training and Doctrine Command (2006). *Cyber Operations and Cyber Terrorism*. DCSINT Handbook No. 1.02. http://www.fas.org/irp/threat/terrorism/sup2.pdf [last visited: 25 February 2009].

Weimann, G. (2004a). www.terror.net. How Modern Terrorism Uses the Internet. *United States Institute of Peace*. Special Report No. 116. http://www.usip.org/pubs/specialreports/sr116.pdf [last visited: 25 February 2009].

Weimann, G. (2004b). Terrorists and Their Tools – Part II. Using the Internet to Recruit, Raise Funds, and Plan Attacks. *YaleGlobal Online*. http://yaleglobal.yale.edu/article.print?id=3768 [last visited: 25 February 2009].

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*. Volume 28, pp. 129–149.

Whine, M. (1999). Cyberspace – A New Medium for Communication, Command, and Control by Extremists. *Studies in Conflict & Terrorism*. Volume 22, pp. 231–245.

Wilson, C. (2003). Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. *Congressional Research Service Report for Congress* (RL32114). Updated 1 April 2005, http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf [last visited: 25 February 2009].

Chapter 6
Victims of Terrorism Policies: Should Victims of Terrorism Be Treated Differently?[1]

Hans-Jörg Albrecht and Michael Kilchling

6.1 Introduction: Anti-Terrorism Policies and the Victim

6.1.1 Key Issues

When discussing victims of terrorism policies, two (and originally separate) lines of policymaking have to be included. First, the general line of policymaking with respect to victims of crime and second, the line that is drawn by counterterrorism policies. From the 1980s on, the crime victim received particular attention in criminal policy and subsequently also in criminal legislation.[2] This has led to legislation that is protective as regards possible averse impacts of criminal proceedings and supportive as regards compensation of material and immaterial losses caused by the victimizing event. National legislation and policies generated amendments of criminal procedural codes and victim support schemes. The Council of Europe and the European Union (EU) developed standards and instruments backing up the movement for a better treatment of crime victims. From the 1970s on, terrorism, back then mostly in the form of national, separatist, and political terrorism, started to trouble European countries. The policy response was more or less restricted to tailoring police and criminal procedural laws to new demands of law enforcement in face of organized violence exerted against individual exponents of the economic and political system to strongarm legitimate governments. A few exceptions can be observed with France and Italy introducing specific legislation for victims of terrorism after experiencing terrorist violence in the

H. Albrecht (✉) and M. Kilchling
Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: h.j.albrecht@mpicc.de

[1] Updated version of article originally published by Springer Science+Business Media in the *European Journal on Criminal Policy and Research*, issue 13:1–2 (April 2007), pg. 13–31.

[2] Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, adopted by the General Assembly of the United Nations November 1985; UN General Assembly Resolution 40/34, 1985.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_6,

1970s and 1980s. However, it was only after the 9/11 attack on the World Trade Center with its devastating consequences for civil society and the extreme toll of human life that more attention has been devoted to the question of how victims of terrorist attacks can be accommodated better. This process has been accelerated by the terrorist acts of Madrid in 2004 that claimed almost 200 lives and the London underground bombings of 2005. The policies developing since can be placed alongside such policies that have been adopted in order to respond to the aftermath of mass violence such as state wars or civil wars. Such developments may also be considered to be part of general crime victim policies that recently tend to branch out into special policies devised to meet the needs of particular groups of victims such as victims of trafficking, victims of sexual violence and abuse, or victims of traffic accidents. But, the phenomenon of terrorist violence and its impact on civil society and individuals also exhibit a close relationship to racist or hate violence and ethnic hatred. The latter may be understood as the little brother of international terrorism that feeds on the vulnerability of modern societies and seeks to destroy the very basis of social integration, that is social solidarity.

Solidarity with victims (in terms of individual, symbolic and collective victims, and the victimized states) is, in fact, regularly mentioned in official statements addressing terrorism and the fight against terrorism.[3]

6.1.2 Terrorism: Post-9/11 Legislation and the Victim

Anti-terrorism legislation drafted and enacted after 9/11 certainly carries clear signs of coordination and convergence. Coordination and convergence have been pushed by precise demands voiced by the United Nations (UN), the security council as well as other international and supra national bodies. Moreover, post-9/11 anti-terrorism legislation implements a programme developed in the context of controlling transnational organized crime, money laundering, as well as illegal immigration throughout the 1980s and 1990s. The Madrid bombing again accelerated the pace of actions against terrorism, in particular in Europe and within the framework of the EU. Anti-terrorism legislation is of a cross-sectional nature as it is headed towards amendment, not only of criminal law but also towards amending telecommunication law, immigration law, police law etc. In material criminal law, we find new offence statutes that penalize support of terrorist organizations and financing terrorism, in procedural law police powers have been widened, while telecommunication providers are subject to prolonged periods of data retention. Cooperation between police and intelligence agencies has been facilitated; the emergence of task force approaches that combine police, intelligence agencies, customs, immigration authorities etc. points also to the convergence of policies of prevention and repression. At large, anti-terrorism legislation demonstrates the transformation of the formerly privileged status of politically and ideologically motivated violence into behaviour deemed to be particularly dangerous and therefore eligible for increased penalties

[3] United Nations General Assembly Resolution 52/133, "Human Rights and Terrorism." December 1997.

and incapacitation. Such transformation can be also understood as the emergence of an "enemy"-type criminal law which is opposed to the version of criminal law which addresses citizens and with that treasures the salience of civil liberties. The focus of terrorism legislation so far has been and still is on ways to improve prevention and repression of terrorist acts.[4]

The issue of victims of terrorism, however, did not play a significant role in international and national anti-terrorism policies, although the US Department of State accounts of global patterns of terrorism show clearly that civilians bear the main toll of terrorist violence. Up to 90% of deaths linked to terrorist violence worldwide are suffered by the civilian population.[5]

The Security Council in its resolution 1566 (2004)[6] requests the elaboration of recommendations by a working group to establish a fund to compensate victims of terrorism and their families. Funds should be raised by voluntary contributions and through assets seized and forfeited from terrorists and terrorist groups. In his key note address to the International Summit on "Democracy, Terrorism, and Security – "A Global Strategy for Fighting Terrorism" (Madrid 2005), the Secretary General underlined the salience of such a fund.[7] In its resolution on the UN Global Counter-Terrorism Strategy 2006, the General Assembly has stressed the relevance of national systems of assistance to victims of terrorism and their families.[8] However, despite a frequently voiced need for urgent action implementation, this has failed until now. The UN, moreover, did not go beyond recommending voluntary action of member countries and did not move towards a mandatory scheme of victim of terrorism support.

6.2 European Developments in the Field of Support of Victims of Terrorism

6.2.1 The Council of Europe and Victims of Terrorism

The Council of Europe addressed the issue of compensation to crime victims from public funds already in the early 1970s, eventually leading to the establishment of the European Convention on the Compensation of Victims of Violent Crimes in 1983.[9] The Convention entered into force in 1988. The aims of the Convention

---

[4] Albrecht, H.-J.: Antworten der Gesetzgeber auf den 11. September – eine Analyse internationaler Entwicklungen. Journal für Konflikt- und Gewaltforschung 4, 46–76 (2002); *see also* Irune Aguirrezábal Quijera, I.: The United Nations' Responsibility towards Victims of Terrorist Acts. FRIDE, Madrid 2005.

[5] US Department of State: Global Patterns of Terrorism 2003. Washington, April 2004.

[6] Adopted by the Security Council at its 5053rd meeting on 8 October 2004.

[7] *See also* Commission on Human Rights resolution 2003/37 "Human rights and terrorism."

[8] A/RES/60/288, 8 September 2006.

[9] European Convention on the Compensation of Victims of Violent Crimes of 24 November 1983, ETS No. 116.

are to introduce or develop schemes for compensation of crime victims and to establish minimum provisions for compensation of material and immaterial losses. The Convention states that compensation shall be paid by the state on whose territory the crime was committed to nationals of the states party to the Convention as well as to nationals of all Member States of the Council of Europe who are permanent residents in the state on whose territory the crime was committed. Regarding eligibility, those who have sustained serious bodily injury or impairment of health directly attributable to an intentional crime of violence, as well as the dependents of persons who have died as a result of such a crime, shall be eligible for compensation. This shall apply also if the offender cannot be prosecuted or punished. Compensation shall cover, at least, loss of earnings, medical and hospitalization, and funeral expenses and, as regards dependants, loss of maintenance. Compensation may be made subsidiary to compensation obtained by the victim from any other source. The Convention obliges the Contracting States to designate a central authority to receive and take action on requests for assistance from any other Party in connection with the matters covered by the Convention. The Council of Europe then issued Recommendations on Assistance to Victims and the Prevention of Victimization on 17 September 1987.[10,11]

Recently, the Council of Europe drafted guidelines on the Protection of Victims of Terrorist Acts.[12] Herewith, it was recognized that the suffering of victims of terrorist acts deserves national and international solidarity and support. The guidelines underline the states' obligation to take the measures needed to protect the fundamental rights of everyone within their jurisdiction against terrorist violence, in particular the right to life and thus points also to the European Convention on Human Rights as well as decisions of the European Court on Human Rights holding that states are under a strict duty to implement policies devised to provide for effective protection of human life.[13] According to the guidelines, states should ensure that persons who have suffered physical or psychological harm as a result of terrorist violence, as well as, under certain circumstances, close relatives are in a position to benefit from the services and measures prescribed by these guidelines. A couple of principles are elaborated in the guidelines that reflect fairly well and consistently the principles developed for "ordinary" victims (of violence). When looking into the victim of terrorist approach, we find the principle that the granting of services and support

[10] Recommendation R (87) 21 on the Assistance to Victims and the Prevention of Victimization, adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies.

[11] For a compilation of the most relevant victim-related Council of Europe documents, *see* Council of Europe (ed.), Victims – Support and assistance, Strasbourg 2006.

[12] Adopted by the Committee of Ministers on 2 March 2005 at the 917th meeting of the Ministers' Deputies.

[13] Guidelines on the Protection of Victims of Terrorist Acts, adopted by the Committee of Ministers on 2 March 2005 at the 917th meeting of the Ministers' Deputies. The guidelines are available on the website of the Council of Europe at www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Fight_against_terrorism/2_Adopted_Texts

should not depend on the identification, arrest, prosecution, or conviction of the perpetrator of the terrorist act but also on the principle of respect for the dignity, private, and family life of victims of terrorism, which should be also protected against intrusive media practices. The importance of emergency assistance is stressed as well as that of long-term medical, psychological, social, and material assistance. Then, the duty of effective investigation of terrorist acts is highlighted, a duty which is in line with decisions of the European Court on Human Rights as regards protection of human life.[14] In case of decisions not to prosecute, it is recommended that states give victims the right to have this decision re-examined. Effective access to the law and to justice for victims of terrorist acts should be provided and the position of victims of terrorist acts adequately recognized in criminal proceedings. Fair, appropriate, and timely compensation for the damages is mentioned not to be affected by national borders. Material compensation should come with support to provide for relief as regards other impacts of terrorist acts. Protection of the right to privacy and family life against overly intrusive media practices is demanded, as is protection of witnesses against risks for life and health that can come with testifying in terrorist trials. The latter evidently refers to organized crime legislation where victim and witness protection has been recognized as a key (procedural) issue. The guidelines then address the need for information to be delivered to victims of terrorist activities and which – along the well-known information standards of general victim policies – refer to information on criminal proceedings, victim rights, and victim support. The guidelines conclude with urging member states to establish specific training programmes for officials dealing with victims of terrorism.

The victims of terrorism guidelines insofar reflect general standards of delivering support and granting compensation to crime victims. With focussing on protection in criminal proceedings, safeguarding privacy, fair and effective compensation (including advance payments), adequate training of law enforcement staff, those focal concerns are raised that have been dealt with by advocates of crime victims for the last three decades.

Summarizing the activities of the Council of Europe regarding victims of terrorism, one has to come to the conclusion that these activities are more part of general victim policy than part of particular counterterrorism activities. It is striking that no particular reference to victims is made in the anti-terrorism conventions, neither in the 1997 Strasburg Convention[15] nor in the 2005 Warsaw Convention.[16] This general line is reflected once again in the new 2006 Recommendation on Assistance to Crime Victims,[17]

---

[14] European Court on Human Rights 28 March 2000, Kiliç vs Turkey; 18 May 2000, Velikova vs Bulgaria.

[15] European Convention on the Suppression of Terrorism of 27 January 1977, ETS No. 090.

[16] European Convention on the Prevention of Terrorism of 16 May 2005, ETS No. 196.

[17] Recommendation Rec(2006)8 on Assistance to crime victims, adopted by the Committee of Ministers on 14 June 206 at the 967th meeting of the Ministers' Deputies. The new recommendation is intended to update and amend the earlier recommendations R (87) 21 (*see* above) and R (85) 11 on the Position of the Victim in the Framework of Criminal Law and Procedure.

which has its focus on victims of all types of serious and intentional violent crimes. The text promotes fair and appropriate compensation to be delivered without undue delay for victims and dependants within their immediate family. Compensation shall cover not only the expenses for treatment of physical and psychological injuries. In addition, compensation for pain and suffering, for the first time, is recommended as well, although in a rather weak form.[18] Further attention is on the significance of legal aid and effective access to all civil remedies and to the competent authorities and courts. And once again, the importance of the protection of the physical and psychological integrity of victims is pointed out, as well as the states' responsibility for the protection of privacy of the victims and their families.

6.2.2 European Union

The EU has dealt with victims of crime and victims of terrorism in various Green Papers,[19] declarations, framework decisions issued by the European Council and the European Parliament. The attention paid to victims of crime became visible in a Council Joint Action (97/154/JHA) that aims at combating trafficking in human beings and sexual exploitation of children[20]; in the Vienna Action Plan of the Council and the Commission of 1998 which deals with how to most effectively implement the provisions of the Treaty of Amsterdam on the "area of freedom, security, and justice" (pointing in particular to art. 19 and 51(c) thereof)[21]; in the Commission's communication to the Council, the European Parliament and the Economic and Social Committee which carries the title "Crime Victims in the EU Reflections on Standards and Action"[22]; in the resolution of 12 December 2000 on the initiative concerning the Council Framework Decision on the standing of victims in criminal procedure,[23] as well as in the final Council Framework Decision of 15 March 2001 on the standing of victims in criminal proceedings.[24] However, combating of terrorism became a focus of EU attention just days before the terror attacks in New York and Washington in the Parliamentary resolution of the 5 September 2001 (concerning the role of the EU in combating terrorism),[25] followed by the resolution of 6 February 2002[26] on the proposal

[18] *See* recommendation no. 8.8: "states may consider."

[19] Commission of the European Communities: Green Paper. Compensation to crime victims (presented by the Commission) Brussels, COM(2001) 536 final, 28.9.2001.

[20] OJ L 63, 4.3.1997, p. 2.

[21] OJ C 19, 23.1.1999, p. 1.

[22] OJ C 59E, 23.2.2001, p. 5.

[23] OJ C 232, 17.8.2001, p. 36.

[24] OJ L 82, 22.3.2001, p. 1.

[25] OJ C 72E, 21.3.2002, p. 135.

[26] OJ C 153E, 27.6.2002, p. 275.

for a Council Framework Decision on combating terrorism[27] and the actual Council Framework Decision of 13 June 2002[28] with its definition of terrorist offences. When dealing with terrorism, EU statements also recognize that victims of terrorism must be taken care of in order to respond effectively to terrorist goals that aim at destroying social solidarity.

According to EU policies, the establishment of an area of freedom, security, and justice must also take account of the needs of crime victims. The Vienna Action Plan[29] of the Council and the Commission, adopted by the Council in 1998, called for the question of victim support to be addressed by conducting a comparative survey of victim compensation schemes and assessing the feasibility of taking action within the EU. The Commission presented a Communication[30] on crime victims in 1999, covering not only compensation aspects but also other issues that could be addressed to improve the position of crime victims in the EU. The conclusions of the 1999 European Council in Tampere called for the drawing up of minimum standards on the protection of the victims of crime, in particular on crime victims' access to justice and on their rights to compensation for damages. It also called for the setting up of national programmes to finance supportive measures and for effective protection of victims. For decades, the European Parliament has firmly supported improvements of crime victim compensation schemes. The Council adopted a framework decision[31] on the standing of the victim in criminal proceedings on 15 March 2001. The framework decision, based on title VI of the EU Treaty, includes an obligation for Member States to ensure that crime victims can obtain a decision on compensation from the offender in the course of criminal proceedings. An in-depth study[32] of the position of crime victims in the EU covered, among other aspects, the possibilities for crime victims to receive compensation from the state under the national laws of the Member States. The results of this study have been published as a Green Paper on Compensation of crime victims.[33] Here, it is stated that recognition of crime victims needs and comparable legal regulation are needed in a common space of free movement, justice and security and referred in particular to the principles of non-discrimination and the right to have a fair hearing as well as decisions by the European Court of Justice that provide for certain basic standards.[34] The study found out that current victim

[27] COM(2001) 521 final, 19.9.2001; *see also* OJ C 332E, 27.11.2001, p. 300.

[28] OJ L 164, 22.6.2002, p. 3.

[29] OJ C 19, 23.1.1999, p. 1. Point 51 (c).

[30] Communication from the Commission to the Council, the European Parliament and the Economic and Social Committee. Crime victims in the European Union – reflections on standards and actions. COM(1999) 349 final, 14.7.1999.

[31] OJ L 82, 22.3.2001, p. 1.

[32] Wergens, A.: Crime victims in the European Union. Brottsoffermyndigheten, Umeå 2000.

[33] Commission of the European Communities: Green Paper. Compensation to crime victims (presented by the Commission) Brussels, COM(2001) 536 final, 28.09.2001.

[34] Case 186/87 Ian William Cowan v. Trésor public [1989] ECR 195; Case of Rolf Gustafson v. Sweden, judgement of 27 May 1997.

compensation rules cover in principle three groups: direct and indirect victims as well as third parties (victimized through helping the victim or by official interventions aimed at helping the victim). Most systems cover all crime victims independent of nationality and residence, some requiring reciprocal victim support in case of non-EU citizens. In general a violent and/or intentional crime is required. The type of losses that can be recovered through compensation schemes concern first of all medical expenses, partially also compensation for property losses. Permanent disability is recognized by all member states as a ground for compensation. Quite significant differences can be observed as regards compensation for immaterial damages (pain and suffering). Differences are found also with respect to how the principle of subsidiarity is to be applied. A formal complaint is mostly required to be brought to the competent authorities within a defined, though varying, period. Almost all member states allow for advance payments. The basic legitimacy for setting up victim compensation legislation throughout the EU is seen – besides criminal policy rationales – in equity and social solidarity, which constitute also the basic principles behind the 1983 European Convention on Compensation of Crime Victims. Other Member States connect the need for state compensation schemes to considerations of criminal policy. While it is recognized that the one primarily responsible for compensation should be the offender, it is argued everywhere that most crime victims cannot in fact get compensation from those responsible for various reasons. From that the Green Paper draws the conclusion that the function of state compensation schemes lies in providing a safety net for victims and it is then not surprising that the general approach adopted optimizes the crime victims' rights to compensation paying no regard at all to costs and problems coming along with such a re-distribution scheme (that are borne after all by civil society through taxes).

The need to adopt a common EU policy is justified specifically with obstacles stemming from cross border situations and related to information on the possibilities to get state compensation, to make an application for state compensation, and to the necessary investigation that must follow the application. Reference is made to judicial cooperation between the Member States for service of documents and for the taking of evidence.[35]

A resolution of the European Parliament[36] welcomes the Green Paper[37] and puts the question of victim compensation and victim support in a perspective that stresses free movement under conditions of security and justice, the heavy toll

[35] Council Regulation (EC) No 1348/2000 of 29 May 2000 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters, OJ L 160, 30. 6. 2000, p. 37 Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States of the European Union in the taking of evidence in civil and commercial matters, OJ L 174, 27.6.2001, p. 1.

[36] European Parliament resolution on the Commission Green Paper on compensation to crime victims (COM(2001) 536) – C5–0016/2002 – 2002/2022(COS).

[37] OJ C 125, 27.5.2002, p. 31.

criminal victimization places on the EU citizens, the need to recognize indirect victimization and the particular damage to victims caused by terrorism. The need to develop a common EU victim of terrorism policy is grounded on equity, solidarity, and a rational crime policy that overcomes differences between the systems of crime victim compensation in the member states.

The Committee on Legal Affairs and the Internal Market for the Committee on Citizens' Freedoms and Rights, Justice, and Home Affairs has also welcomed the Commission's Green Paper on compensation to crime victims with declaring that the EU should adopt binding Community provisions to create a common area of justice for citizens who are the victims of crime. The Committee took the view that to be complete and efficacious, any such compensation must cover both material and non-material damage and called on the Commission to treat as a main priority the issues relating to time limits for submission of claims for compensation, procedural guarantees, and the introduction of harmonized claim forms in all Community languages. Furthermore, minimum requirements for subsidiary application of the state's responsibility are demanded, as well as making compensation independent from nationality. Finally, the declaration voices the opinion that a mutual assistance system must apply that compensates the problems crime victims experience in case of cross border victimization.

In line with the preparatory work, a Council directive relating to compensation of crime victims was adopted on 29 April 2004.[38] This directive is to ensure that by 1 July 2005, each Member State had a national scheme in place, which guarantees fair and appropriate compensation to victims of crime. Then, the directive aims at implementing easy access to compensation in practice and regardless of where in the EU a person becomes the victim of a crime. Implementation of this aim shall be facilitated by creating a system for cooperation between national authorities, which should have been operational by 1 January 2006.

The approach emerging in particular with the EU statements and decisions is certainly in line with the traditional concept of a welfare state that tries hard to compensate all the risks individuals are faced with in modern societies and to compensate fully for damage resulting from such risks. It goes beyond the conventional welfare approach in pushing compensation rights towards those available under tort law and a full compensation approach that is normally justified only by a perpetrator being individually responsible for an act that causes damage to another person. Thus, this approach is hardly consistent with the fact that the welfare systems in all member states are overburdened and that such systems are being cut back in order to allow for new assessments of what should fall within the responsibility of the state and what should fall within the individuals' responsibility. Problems of possible fraud and exploitation of such compensation schemes are also hardly analyzed.

[38] Council Directive 2004/80/EC of 29 April 2004 Relating to Compensation to Crime Victims, OJ L 261, 6 August 2004, p. 15.

The statements and declarations consistently refer to solidarity, solidarity with individual victims of terrorist attacks, as well as states falling prey to terrorism. In a declaration on Combating Terrorism, the European Council, responding to the Madrid massacre, stresses the need to assist victims of terrorist crimes by way of adopting the Council Directive on compensation to crime victims. The Council demands then that the Commission allocates the funds available in the 2004 budget for supporting victims of terrorism. What is also mentioned concerns the need of effective protection of witnesses in terrorist cases and indirect victimization in terms of minority communities that are at risk of falling prey to a backlash after a terrorist attack.[39] In particular, the latter should receive thorough attention as the backlash against minority communities is evidently part of terrorist strategies, devised to destroy social solidarity and establish a climate of fear, and ethnic and religious hate, favourable to the spread of violence.

In the EU Guidelines for a Common Approach to Combating Terrorism, larger concepts of protection of victims are introduced in demanding for the enhancement of the capability of Member States to deal with the consequences of a terrorist attack on the civilian population in the area of vulnerable infrastructure.

6.2.3 Experiences with Victim of Terrorism Compensation and Support Outside Europe

6.2.3.1 Victim of Terrorism Legislation in the USA

Specific victim of terrorism legislation and practice are developing in the USA since the early 1980s. The process is based on the conviction that although victims of terrorism have much in common with other violent crime victims and with disaster victims, they appear to experience higher levels of distress and display also different needs, partially due to the magnitude and scope of specific violent events. Stressed are those particulars which are due to the cross border or trans-national character of both terrorism and victimization leading to new demands for procedure and organization of victim relief and support schemes. In fact, the USA has a rather long history of legislation to the benefit of victims of terrorism. The first law that provided federal assistance to victims of terrorism was the Hostage Relief Act of 1980, which was enacted in response to the Iranian hostage crisis. However, the Bill was enacted also in response of the treaty concluded between the USA and Iran which contained a provision that barred victims from seeking tort damages in US courts against Iran. The benefits included hostages' loss of income, medical expenses due to captivity, tax exemption of compensation, and payments for educational expenses for a partner or a child. In particular, medical compensation was accompanied by a subsidiarity

[39] *See also* Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001, SN 140/01, p. 4.

clause. A second piece of legislation concerns the Victims of Terrorism Compensation Act 1986. This act applies to government employees only but is not restricted to a specific terrorist act. In addition to the benefits described above the Act awards each victim 50 US$ for each day of captivity. Another law responded to the bombing of PanAm flight 103 and provided aid and support to all US citizens (US Response to Terrorism Affecting Americans Abroad, Title 22, Aviation Security Improvement Act of 1990). The Oklahoma City bombing resulted in the Justice for Victims of Terrorism Act (amending Title 42 of the Anti-terrorism and Effective Death Penalty Act). With this Act, federal payments to states, public agencies, and NGOs for relief for terrorism victims are provided besides offering immediate crisis response efforts to the victims. The amendment provided also for the right of victims to participate in trial proceedings arising from the Oklahoma City bombing. The Antiterrorism and Effective Death Penalty Act of 1996 also contained a provision requiring state crime victim compensation programmes to include in their compensation programmes state residents who are victims of terrorism while outside of the USA.

The most recent Bill relates to the 9/11 attacks and their aftermath.[40] The Victims of Terrorism Tax Relief Act provides tax relief to relatives of victims of the 9/11 attacks, the Oklahoma City bombing and the anthrax attacks following 9/11. Income tax liability of a deceased victim is waived for both the year of the attack and the previous year and provides other tax exemptions. The Air Transportation Safety and System Stabilization Act of 2001 has established a Victim Compensation Fund that addresses economic and non-economic losses but seeks also to shield, in particular, airlines from civil litigation.[41] An eligible claimant can receive an immediate advance payment of US$ 50,000 in cases involving death or US$ 25,000 in cases involving serious injury. The Act authorizes the head of the Compensation Fund to examine economic and non-economic harm suffered in light of individual circumstances. The non-economic loss compensation is set for the spouse and each dependent of a deceased victim at US$ 100,000 in addition to a US$ 250,000 payment awarded on behalf of all descendants. Other payments and sources of compensation, however, are to be deducted with the exception of tax relief, Social Security benefits, workers' compensation benefits, and support from charitable donations.

US legislation in the area of victims of terrorism is characterized by responding to specific acts of terrorism. However, US-American law provides also for effective civil legislation that enables victims of terrorism to sue foreign perpetrators in US federal courts and based on US tort law.

In terms of organization and procedure, the Office for Victims of Crime (OVC) plays a decisive role. In 1996, OVC was given the authority to access the Victims

---

[40] Peck, R.S.: The Victim Compensation Fund: Born from a Unique Confluence of Events Not Likely to Be Duplicated. DePaul Law Review 53 (2003), S. 209–30.

[41] Mariani, R.L.: The September 11th Victim Compensation Fund of 2001 and the Protection of the Airline Industry: A Bill for the American People. Journal of Air Law and Commerce 57 (2002), pp. 141–186; the final rules governing the Victim Compensation Fund of 2001 were published on March 6, 2002 (P.L. 107–142).

of Crime Act emergency reserve fund of US$ 50 million to assist victims of terrorism and mass violence.

There are five types of support available from OVC to respond to terrorism and mass violence: (a) Crisis response grants, (b) consequence management grants, (c) criminal justice support grants, (d) compensation grants, and (e) technical assistance/ training services.

The Office created the Terrorism and International Victims Unit; the task of which is to help victims of terrorism, mass violence, and international crimes such as trafficking of women and children and child abduction.[42] Moreover, the administration of the international terrorism victims compensation programme is entrusted to the unit as is the maintenance of an International Crime Victim Compensation Programme Directory in collaboration with the State Department that links victims abroad to available resources and lists crime victim compensation programmes in various foreign countries in an attempt to deal effectively with international terrorism affecting citizens at home and abroad. The OVC has issued guidelines to provide compensation and assistance to victims of acts of terrorism or mass violence within the USA and assistance to US citizens and government employees who are victims of terrorism and mass violence abroad.

The specific victim of terrorism programmes are built on federal and state law – emerging parallel to European developments since the early 1980s – that assigns certain responsibilities and duties to agencies involved in investigating and prosecuting crime with respect to crime victims. The rights to be respected and services to be provided concern identifying the victims, providing them with information on the availability of medical, psychological counselling, compensation and restitution, providing information about the status of the criminal investigation and later the prosecution of the criminal case against the suspects, facilitating victim participation in the criminal case through trial attendance, and presenting impact information (victim impact statements) during the sentencing part of the trial.

The USA has thus adopted an individualized approach that is focussed on specific terrorist attacks. With that, flexibility is implemented as is the possibility to consider various and differing (political and economic) goals when deciding whether and to what extent victim of terrorism legislation should be enacted to respond to terrorist attacks. The basic problem then concerns control of discretion and implementation of equal treatment.[43]

The US approach to providing compensation to victims of terrorism has been criticized because of problems of equal treatment. Equality issues are clearly raised with respect to compensation practice after 9/11. While the overall amount of compensation paid to victims of 9/11 (approximately 38 billion US$) certainly demonstrates effectiveness of major players such as insurance companies, the Federal Government,

[42] U.S. Department of Justice, Office of Justice Programs: International Terrorism Victim Expense Reimbursement Program. Report to Congress. Washington, February 2006.

[43] *See*, e.g., Shapo, M.S.: Compensation for Victims of Terror: A Specialized Jurisprudence of Injuries. Indiana Law Review 36 (2003), pp. 237–249.

charitable organizations, and the tort system, it demonstrates also the disparate treatment of 9/11 victims compared with victims of other terrorist incidents as well as disparate treatment among 9/11 victims.[44] Critique has also been voiced as regards the guiding principles of victims of terrorism compensation that tend to be rather close to tort law principles and move away from a support and social welfare approach.[45]

6.2.3.2 Israel

Israel certainly is a country that has experienced mass violence, terrorism, and war in abundance over the last four decades. Insofar it does not come as surprise that Israel has also gained vast experience in legislative and practical efforts to cope with problems of victimization through terrorism and various forms of collective violence. The Israeli legislator has, in fact, devised comprehensive legislative responses to two of the primary issues arising in the context of compensation for harm caused by terrorism: first, the Victims of Hostile Action (Pensions) Law of 1970 provides compensation for bodily injuries suffered in terrorist attacks, as well as compensation for family members of deceased victims. Second, the Property Tax and Compensation Fund Law of 1961 provides compensation for property damage caused by terrorism.[46] The Israeli system is a permanent compensation system emerging from the political will that damages caused by war shall be borne by the public as a whole or rather by public funds and not by individuals suffering such damages. This approach was then expanded to cover victims of terrorism. The compensation system therefore is justified with the principle of solidarity and the recognition that general risks such as war, collective violence, and terrorism must be borne by the general public. While historically risks stemming from war were considered to be restricted to members of military forces or warring factions, such differences cannot play a role since Second World War and subsequent wars, which have shown drastically that the main toll of losses in human life and property will be borne by civil society and not by the military. Terrorism – when drawing a parallel to war – targets and drags random civilians into violence and makes them (and the whole of civil society) involuntary draftees in a war that has been called a small or private war. Israeli law makes no distinction between civilians harmed by war and civilians harmed by terrorism. Both are addressed as suffering from "enemy-inflicted injury" (which also encompasses losses due to "friendly fire").

As do specific US laws, Israeli law covers Israeli citizens falling prey to terrorism at home and abroad. Foreign nationals (having entered Israeli territory legally)

---

[44] Dixon, L., Kaganoff Stern, R.: Compensation for Losses from the 9/11 Attacks. RAND Institute for Civil Justice, Santa Monica 2004.

[45] Diller, M.: Tort and Social Welfare Principles in the Victim Compensation Fund. DePaul Law Review 53 (2003), pp. 719–768.

[46] Sommer, H.: Providing Compensation for Harm Caused by Terrorism: Lessons Learned in the Israeli Experience. Indiana Law Review 335 (2003), pp. 335–365.

are covered when victimized on Israel territory. Providing evidence is facilitated through a presumption of a hostile act given a reasonable basis to assume such an act. Benefits drawn from compensation and support schemes are administered by the National Insurance Institute. Compensation includes costs incurred for medical care as well as living stipends while in medical treatment. Financial support is calculated on the basis of the victims' pre-victimization income. Besides medical expenses, the law compensates a range of other family members of victims who are treated, as are family members of military personnel who died in the line of duty. In case several options for compensation are available the victim has the choice. The compensation for property loss is also seen as an extension to compensation schemes established for losses due to war. The system applicable to property damage underwent changes from an insurance model to a social support system. The law covers direct and indirect damages to property (excluding, however, such damage that is a general consequence of an economy deteriorating after a major terrorist attack). Difficulties may arise out of distinctions to be made between hostile acts and mere acts of violence (or property crime). The applicant has to provide for evidence as regards a hostile motive.

6.3 Varying Models and Practices of Compensation of Victims of Violence and Victims of Terrorism Across Europe

Also in the European states, legislation varies to a significant degree, particularly in the area of victim of violence compensation. In a comparison considering the broader reach of Council of Europe membership, the national models can roughly be divided into three groups[47]:

First, States that have enacted specific victim of terrorism legislation and specific programmes. Such specific legislation is modelled along the precursor of compensating military and civil victims of war. The German law on compensating victims of violence similarly refers to a structure for compensation which is derived from a statute that organizes support for losses due to war. With the reference to war, an analogy is created between victimization through terrorist acts and victimization through war. This becomes evident, for example, when civil victims of terrorist violence are conceptualized as "soldiers" drawn involuntarily into a violent conflict between terrorist groups and the state.[48] The analogy is also driven by the

[47] For more detailed information on the situation in the CoE Member States, *see* Kilchling, M., Albrecht, H.-J.: Victims of Terrorism Policies and Legislation in Europe. An Overview on Victim Related Assistance and Support, forschung aktuell – research in brief, No. 30. Freiburg i. Br. 2005, pp. 18 et seq.; the report is also available in Council of Europe (ed.), Victims – Support and assistance, Strasbourg 2006, pp. 199 et seq. (pp. 211 et seq.) or as document no. PC-S-AV (2005) 04 at www.coe.int

[48] Sommer, H.: Providing Compensation for Harm Caused by Terrorism: Lessons Learned in the Israeli Experience. Indiana Law Review 335 (2003), pp. 335–365.

understanding of modern terrorism as small or private wars (and, of course, by declaring war on terrorism). Specific victims of terrorism legislation can be found in France, Italy, Greece, Spain and Russia. The outcomes of the systems are evidently quite different. While France and Spain have set up separate administrative bodies of victim of terrorism support, Russia responds by ordinary courts assessing applications on the basis of rules that evidently leave much discretion in deciding on whom and what to compensate. Most of the countries that have created specific victims of terrorism legislation have suffered during the last forty years under extended periods of terrorist attacks which had or have either separatist or ideologist, but mostly local, roots.

Second, states that have elaborated crime victim compensation and protection programmes that also cover victims of terrorism but do not mention victims of terrorism specifically.

And finally, states that have, until now, not at all or only created legislation to a very limited extent in the area of compensation of victims of crime and/or have, due to various reasons, not implemented compensation laws or victim assistance and support schemes. These reasons are found in restricted public funds that can be made available for victim compensation and/or the adoption of the view that other areas of social policy require a higher priority when deciding on where public investments should be made.

The compensation legislation can then be subdivided into models that

1. tend to provide full compensation (in particular, for pain and suffering and with that adopt tort law as a basic approach),
2. find basic legitimation in a social welfare approach that responds to a financial crisis and special psychological and other support needs as a consequence of violence (or other damaging behaviour), is subject fully to the principle of subsidiarity, and prevents the state and society from stepping in to replace an offender who is either not identified, dead, or financially not capable of fully compensating the victim.

Further differences can be identified with regard to the extent to which, and the circumstances under which, victims are being subsidized. On the one hand, there are states which grant compensation on the basis of "*one-off*" *payments* which more or less are of a symbolic character only, whereas some states, on the other hand, provide for regular monthly or annual payments. The most significant example for a well-endowed regular subsidy system can be found in Italy, where victims and their relatives receive the highest payments in terms of pensions and further additional subsidies. Greece provides for another remarkable particularity: although the level of direct financial payments granted is much lower there, family members, in particular descendants of victims who were a member of the public service receive a kind of "remuneration in kind" in terms of priority access to the public service. With regard to the widespread public service in the country, such an effective guarantee for employment in this sector is of high value, both in practical and financial terms. Further added value comes from the fact that in countries such as Italy,

Greece, and Spain, the beneficiaries of compensation enjoy partial reduction or even total exemption from income tax and/or other administrative fees.

6.4 What Is Particular to the Compensation of Victims of Terrorism?

Should states provide for special rules or programmes for victims of terrorism? Or should victims of crime, in accordance with the principles of solidarity and non-discrimination, be treated all equally? And what is just and equal treatment in those cases? Large-scale terrorist violence and its consequences for victims in the last decades provide for some lessons about the particulars that have to be considered when discussing whether victims of terrorist violence should be dealt with separately and how compensation of victims of terrorism should be regulated.

International texts show different notions in this respect. The EU, on the one hand, seems to be in favour of explicit programmes focusing on victim of terrorism. According to its 2002 Framework Decision on Combating Terrorism, "specific measures are necessary," in particular with regard to the vulnerability of victims of terrorist offences.[49] The position in the Council of Europe, on the other hand, tends to the opposite position. Notwithstanding the fact that the preamble of the 2005 Council of Europe Guidelines clearly points out the consideration that victims of terrorist acts must receive national and international solidarity,[50] the explanatory memorandum to the 2006 Recommendation on Assistance to Crime Victims stresses victims of terrorism – "although prioritized by some countries" – having essentially the same needs as victims of other crimes.[51] Quite obviously, by adopting the recommendation in its final version, the Committee of Ministers has left behind their original idea of giving priority to victims of terrorism.[52]

Research has shown that victims of violent crime experience a wide range of needs – physical, financial, emotional, and legal – which include also long-term mental health services for post-traumatic responses to the criminal event. Insofar victims of terrorism, in general, are not different as regards the impact of violence and the needs following the victimizing event when comparing them to victims of serious (individual) violence. The impact of terrorist acts creates a sense of vulner-

[49] Cf. EU Council Framework Decision (2002/475/JHA) of 13 June 2002 on Combating Terrorism, recital no. 8.

[50] *See* footnote 12.

[51] Cf. Explanatory Memorandum to the CoE Recommendation (2006)8 on Assistance to Crime Victims, para 21.

[52] Cf. Reply by the Committee of Ministers to Recommendation 1677 (2004) "Challenge of terrorism in Council of Europe member states," adopted at the 912th meeting of the Ministers' Deputies on 19 January 2005: Parliamentary Assembly of the Council of Europe Doc. 1041122 of January 2005, item no. 19.

ability, trauma, disruption of everyday life, destruction of the future, and financial problems that come with loosing parents, being disabled etc. This kind of impact is comparable to that of ordinary violence.

There are differences, though. However, such differences are rather located in the areas of planning, organization, and co-ordination of the response to victimization, for example, USA experiences illustrate.[53] Such differences will also be dependent on the type of administrative system that is in place to respond in particular to situations of mass victimization. The preference of terrorists for soft and symbolic targets and the aim to provoke a maximum of public attention will most likely lead to many casualties (in few cases) in a single act of violence and will also result in the need to accommodate for more victims of foreign nationalities – as became visible, for example, in the 9/11 attacks or in the Moscow theatre siege. This calls for systems that are capable to deliver in a short period a maximum of integrated assistance and to avoid problems of delivering support and assistance across national borders and under differing systems of support and compensation.[54] The victim-related responses to the 9/11 attacks have been summarized as indicating that it is of utmost importance to provide for emergency training for staff involved in victim support and assistance, to integrate compensation and assistance personnel in emergency centres, to integrate compensation and mental health with legal assistance and support with financial and daily concerns of victims, and to prepare for a high volume of claimants to be dealt with within a short period of time.[55]

What creates differences between victims of ordinary violence and victims of terrorism concerns the particular attention terrorist acts draw upon themselves in the media and in the political system. This, of course, is feeding the perception that there is inequality in the response to ordinary violence when comparing such approaches to the attention received by victims of terrorist violence. Another outcome could be symbolic (and sometimes pathetic) legislation that has as main goal the expression of a state's capacity to act in face of dramatic threats to the safety of its citizens.

When looking at the reasons given for compensation of victims of ordinary violence and victims of terrorist violence, we find the same type of legitimatization. The basic ground to provide state compensation and assistance for victims of violence and victims of terrorism is seen in the need to express social solidarity and to compensate for risks the state could not prevent to turn into damage and injury. It is arguable whether compensation of victims of terrorism is needed because a lack of compensation would lead to a growth of fear of terrorist violence, and thus

[53] US Department of Justice Office of Justice Programs: Responding to Terrorism Victims: Oklahoma City and Beyond. Washington, October 2000.

[54] US Department of Justice: New Directions from the Field: Victims Rights and Services for the 21st Century. Washington 1998; *see also* Dixon, L., Kaganoff Stern, R.: Compensation for Losses from the 9/11 Attacks. RAND Institute for Civil Justice, Santa Monica 2004.

[55] Gonzales, A.R., Henke, T.A., Gillis, J.W.: Responding to September 11 Victims: Lessons Learned from the States. www.ovcttac.org

would contribute significantly to achieving terrorist goals.[56] However, there are competing models of victim compensation, and significant differences as regards the coverage and the extent of benefits. The latter fact can, from the individual perspective of the persons directly affected, be perceived as unequal and unjust treatment, even if those differences might appear justifiable from a theoretical and systematic perspective. This can be of particular relevance for victims from economically higher developed countries occasionally falling prey to a terrorist attack in a country with a lower economic standard. The Moscow law suits following the theatre siege and – unsuccessfully – claiming millions of US dollars as compensation in a country where the average monthly income does not exceed US$ 200 demonstrate the type of problems that come with expectations and promises of broad and full compensation.

Having said that the issue of foreigners victimized abroad, nevertheless, requires some additional reflection. The question must be raised as to what degree compensation by countries such as Russia, where a one-off payment of less than € 3,000 in most cases[57] is the regular standard for the compensation in cases of terrorist victimization, can be sufficient to satisfy the interests and needs of victims who are citizens from countries where such an amount, based on the regular life standard under which those individuals live, is not more than a symbolic gesture. Because of the arbitrary character of the threats of modern international terrorism, its victims suffer not only from the fact of being – an arbitrary – target for terrorist victimization. Additional impact may arise from the sheer fact of being a victim of a terrorist act in a foreign state that, occasionally, is not capable to provide sufficient financial compensation (in particular, not to the extent of the disastrous casualties caused by a major terrorist threat). These problems are an inherent consequence of the territory principle that is the regular, internationally recognized standard for liability of states under all major international instruments in the area of victim assistance and victim compensation.[58] It has been laid down also in other pieces such as, most recently, in the new Council of Europe Convention on the Prevention of Terrorism[59]: in its article 13, the 2005 Warszawa Convention explicitly refers to the territory principle again.

---

[56] Sommer, H.: Providing Compensation for Harm Caused by Terrorism: Lessons Learned in the Israeli Experience. Indiana Law Review 335 (2003), pp. 335–365, p. 364.

[57] According to a fix tariff system relatives of a victim who came to death receive an amount of 500 minimum salaries, persons who become invalid receive compensation equating 50 or 100 minimal salaries. Victims who suffered serious injuries are compensated by an amount of 30 minimal salaries, those who were slightly injured an amount of 15 minimal salaries. Regular pensions solely based on the fact of a terrorist victimization are not paid. Concrete figures can be drawn from several cases that came to public attention in recent years. Families of the victims of the two passenger jet crashes of 2004 received 100,000 Rubles (~€ 2,800) from the federal government. Victims injured by a terrorist bombing in Moscow in 2004 received 50,000 (serious injuries) 3,000 Rubles (light injuries) on the basis of a decree signed by the Moscow mayor. Survivors of the North-East theatre siege received some US$ 2,700, whereas families or relatives of those who died received approximately US$ 9,500.

[58] *See*, e.g., article 2 of the Council Directive 2004/80/EC of 29 April 2004 (*see* footnote 38).

[59] CETS No. 196, *see* footnote 16.

In terrorist cases involving victims of different nationalities, all present models, full compensation on tort law basis as well as compensation schemes according to the principle of social solidarity, seem problematic, though. They all cannot solve the problem of different expectations, and needs, resulting from different life standards. As long as significant economic differences prevail, any attempt of establishing a uniform level must remain fruitless. Such endeavours were unsuccessful and unsolved in totally different contexts as well.[60] A compromise comes close to circle squaring: Orientation on an upper standard clearly cannot be met by countries with a less prosperous economy whereas with offering subsidies based on the lower end would make victims from high price countries feel offended. From a practical perspective, the only feasible solution might be to generally entitle victims to receive additional financial redress in their home countries, based on the actual standards there. So far, some countries in Europe provide such additional compensation voluntarily, either on a – legal or factual (political) – ad hoc basis[61] or, as recently established in the UK,[62] through an extra compensation fund.[63] Only very few states[64] entitle victims with a regular statutory right to claim for compensation at home.[65] The establishment of such a right which could be provided on a subsidiary basis[66] would, however, be in deviation from

[60] The controversies about how to subsidize the members of the European Parliament in a way that can be assessed to be just by the public in all EU member states is a good example. The present model of payment based on the national standards is as controversial as a uniform system providing the same extent for all the representatives would be.

[61] After the 2002 synagogue attack in Djerba/Tunesia the federal government of Germany provided some € 10 million as ad hoc subsidy for the German victims who legally not eligible for compensation according to the State Compensation Act for Victims of Violent Crime (*Opferentschädigungsgesetz – OEG)* which, at that time, was strongly territory-based as well.

[62] The new UK compensation scheme for victims of terrorism abroad, endowed with an initial capital stock of £ 1 million from the 2006 budget, is administered by the British Red Cross.

[63] Such as, e.g., the so-called "*Fonds de Garantie*" of France which, according to article 9 para 1 of Law no. 86–1020 of 9 September 1986 on the Combat of Terrorism, is also available for French citizens who were victims of terrorist acts committed outside French territory.

[64] *See*, in particular, the Austrian Crime Victims Compensation Act (*Verbrechensopfergesetz – VOG*) that, in its article 1, provides that Austrians and EEA citizens with regular residence in Austria who became victim of a violent crime are entitled to claim for compensation under the *VOG*, independent of the place of victimization. For more details, *see* Raschka, W.: Austria, in: Greer, D. (ed), Compensating Crime Victims – A European Survey, Freiburg 1996, pp. 15 et seq.

[65] In Germany, two parliamentary initiatives of the Liberal Party (cf. BT-Drucksache 16/585 of 08.02.2006) and the Green Party (cf. BT-Drucksache 16/1067 of 28.03.2006) for an expansion of the scope of application of the *OEG* (*see* footnote 61) to include German nationals who were victims of terrorism and other forms of violent crime abroad were unsuccessful. A third initiative launched by the government parties (cf. BT-Drucksache 16/12273 of 17.03.2009), finally succeeded. As of 1 july 2009, such victims now receive, besides health care and some funeral costs, a lump sum between € 714 and € 25,632 for bodily injury, according to the actual degree of injury; in case of death, dependants receive a lump sum between € 1,272 and € 4,488; in addition, close relatives can claim for psychotherapeutic treatment (article 3a of the *OEG* (*see* footnote 61), as amended by the *Third OEG Amendment Act* of 25.06.2009, BGBI, I, p. 1580).

[66] *See*, as concrete examples of such a subsidiary clause, article 8 para 3 of the Austrian *VOG* (*see* footnote 64) or article 3a para 4 of the amended German *OEG* that provide that victims are exempt from compensation if they are eligible to receive similar compensation under foreign legislation.

the internationally acknowledged territory principle. But it could in fact be an act of solidarity among the community of states. The wilful targeting of concrete states is an important strategic element of international terrorists. A state can be the victim of such an attack at any time, notwithstanding all viable efforts of prevention. Consequently, failure of states in the field of prevention in no way – and even less than in cases of conventional crime[67] – can provide for justification of an exclusive liability of a targeted state for injuries and damage suffered by individuals.

6.5 Conclusions

Assistance, protection, and compensation for victims of terrorism have significant impact as a political strategy to counter the dehumanizing of victims, which is a significant component of terrorist strategies worldwide.[68] States have developed different models for assistance, protection, and relief for victims of (violent) crimes, and implemented different types of compensation that have been adopted, or sometimes even extended, for application in cases of terrorist victimization.

As regards emergency relief and general support and assistance, it seems preferable to make coordination of support and assistance, emergency relief etc. part of general civil and public disaster response schemes that are in place in most of European countries. Moreover, indirect victimization in terms of minority communities that are at risk of falling prey to a backlash after a terrorist attack should be made part of response plans. A significant backlash against minority communities evidently is part of terrorist strategies devised to destroy social solidarity and establish a climate of fear, and ethnic and religious hate favourable to the spread of violence.

Protection of victims and witnesses during criminal proceedings and trial has been put rather high on legislators agendas since the times when trans-national, organized crime emerged as an eminent criminal problem in the 1990s, and sexual abuse – in particular child victims of sexual abuse – fuelled demands to reduce secondary traumatization by way of providing for introduction of evidence through videotapes or live video links. In many European countries, it is now victims of human trafficking that receive attention in this regard.[69] Victims of terrorism, however, fall under the rules that have been enacted to protect intimidated victims or victims under the threat

[67] There is principal dispute as to what extent failure in criminal policy in general and prevention in particular can be a rationale for state compensation for victims of crime. For more details, *see* Greer, D.: Compensating Crime Victims – A European Survey, Freiburg 1996, p. 695 (with further references); *see also* the explanatory report to the 1983 European Convention on the Compensation of Victims of Violent Crimes (*see* footnote 9), paragraph 9.

[68] Compare also the report of the UN Secretary General of 27 April 2006: Uniting against terrorism: recommendations for a global counter terrorism strategy, U.N. doc. no. A/60/825, p. 5, available at http://www.un.org/unitingagainstterrorism/sg-terrorism-2may06.pdf

[69] *See*, e.g., Council of Europe, Commissioner for Human Rights, Berlin Declaration of November 2004, www.nhri.net/pdf/CommDH-NHRI(2004)1_E.pdf

of violent revenge. Witness protection schemes vary also, in particular as regards the type of crime victims that are eligible for protective measures.

Of particular importance is further the issue of compensation of victims. Notwithstanding manifold international efforts and instruments, variation in legislation and practices is large in Europe. With preference for a principled approach, it seems clear that a full compensation model, following civil tort law, cannot be justified. The full compensation model as it developed in the USA and as it seems to find some support in Europe is based on the concept of punitive damages and with that on blame. Such an approach puts pressure on social solidarity because of evident problems of unequal treatment rather than adding to social integration as the US example today demonstrates clearly.

Then, convincing arguments speak in favour of adopting a statutory basis for compensating victims of violence instead of adopting an event compensation model that responds to specific acts of terrorism (or mass violence). Although event-based compensation and ad hoc programming of compensation and assistance is flexible, it does not meet requirements set by principles of predictability and equal treatment, instead it tends to be influenced by varying political and economic objectives.

Issues to be covered when trying to elaborate a legitimate and just scheme of compensating, victims of terrorism are certainly the problem of rare events. It is clear that full blown terrorist attacks with scores of victims will remain rare events in the core of Europe in the future. An exception is the Russian Federation where the pace of terrorist attacks will continue to be determined by the armed conflict in Chechnya. Insofar it seems reasonable to suggest to make compensation of victims of terrorism part of general victim compensation legislation and to abstain from developing a support and compensation scheme exclusively for terrorist victimization.

The latter example, however, points to a problem that so far remains more or less unsolved. That is, the issue of just compensation in cases of (terrorist) victimization abroad. Different economic standards that, under the international territory principle, determine the level of state compensation that is available in a certain country can confront victims from abroad with serious financial problems. From a European perspective, compensation of victims of violent crime is justified by both social solidarity and equity[70] which in turn justifies a social welfare approach that makes the type and the amount of compensation dependent on the financial needs that are due to falling prey to violence. This should include that individuals who became victims abroad should not be left without additional recourse to financial redress at home, if necessary. For such cases, additional compensation should, on a subsidiary basis, be provided by the home states. National borders should not shield states from the support of their citizens in case of terrorist (and other serious) victimization. Moreover, the sharing of the burden of care for these victims would also be a manifestation of solidarity of the community of states against the threat of international terrorism which targets both individuals and states.

[70] Preamble of the 1983 European Convention on the Compensation of Victims of Violent Crimes (*see* footnote 8).

Part III
The Law Between War and Crime

Chapter 7
Anti-Terrorism Related Criminal Law Reforms and Human Rights in Slovenia

Damjan Korošec and Sabina Zgaga

7.1 Introduction

As known, Slovenia, after being at the same time a victim of disintegrative processes in the former Socialist Federal Republic of Yugoslavia (SFRY) and playing an important active role in its disintegration, reached the international legal status of an independent state in 1991. It was formally recognized by other states under the chosen name *Republika Slovenija* (Republic of Slovenia), and accepted under this name as a full member of the United Nations (UNO) and from 1 May 2004 as a full member of the European Union (EU).[1] After the proclamation of the new constitution (on 23 December 1991[2]), all legal provisions in force at that time stayed in force, except where they were in conflict with human rights and fundamental freedoms.[3]

It is interesting to know that in the field of substantive criminal law, no provisions of the Criminal Code of SFRY or of the Criminal Code of Slovenia, as a federal part of Yugoslavia with relatively important legislative powers, especially in the field of the general part, were formally declared as "in conflict with human rights and fundamental freedoms" in the given sense in the period between the proclamation of the new constitution and the implementation of the new Criminal Code of the Republic of Slovenia in the mid-1990s.

D. Korošec (✉)
Faculty of Law, University of Ljubljana, Ljubljana, Slovenia
e-mail: damjan.korosec@pf.uni-lj.si

[1] In the criminal legal context it is perhaps worth mentioning that Slovenia is a full member of NATO (from April 2004), is using the Euro (€) as the national currency (from January 2007), and is a full member of the so-called Schengen contractual area since 22 December 2007.

[2] OJ RS 33/91-I. The Constitution of the Republic of Slovenia was amended several times since (OJ RS 42/97, 66/00, 24/03).

[3] Slovenia adopted this provision in art. 1 of a special constitutional act, called the Constitutional Act for the Implementation of the Constitution of the Republic of Slovenia (OJ RS I 33/91).

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_7,

The all new Criminal Code and the Criminal Procedure Act ("*Kazenski zakonik Republike Slovenije*" [CC RS] and "*Zakon o kazenskem postopku*" [CP RS]) were, according to the Slovenian legislative tradition, drafted by separate expert groups and proposed by the Ministry of Justice. Both acts were adopted without significant political or legal–theoretical objections in the new Slovenian parliament in September 1994[4] and entered into force according to their own provisions on entry into force on 1 January 1995. Since then, CC RS has been amended several times. In 1999,[5] crucial characteristics of the amendments were the harmonization with the requirements of the EU *acquis communautaire* and the raising of the special maximum sentence of imprisonment from 20 to 30 years, but the changes and amendments in the special part were of a relatively minor and, from all viewpoints, rather unimportant nature; the latest changes so far entered into force on 5 May 2004.[6] These latest changes affected mainly the special part of the CC RS. Several of the changes, especially in the field of so-called international crimes and including some important changes of the general part of the CC RS, are regarded as a step towards the so-called European criminal law area. The CP RS was amended several times, mainly in the form of legislative changes and amendments as reactions to several decisions of the Constitutional Court of Slovenia regarding different provisions of the CP RS (the last amendment of the CP RS, the so called *ZKP-H*[7] entered into force on 18 March 2007 and has been applied in practice since 17 May 2007).

In a rather conspirative manner, hidden from the general Slovenian public as well as from the expert legal public, the Minister of Justice, Dr. Lovro Šturm set up a working group of three persons, one judge of the Supreme Court of Slovenia, Dr. Mitja Deisinger, and two scholars, Dr. Ivan Bele and Dr. Vid Jakulin, with the task of drafting a new Criminal Code. Because no details of the nature, including the intensity and duration of their work, are known to the public, they cannot be reported here. All that is known from these preparations is the existence of the group described and the results of their work: its draft of a new Criminal Code, published from the Slovenian Ministry of Justice on 12 October 2007 under the code KZ-1, EVA 2007–2011.

In this chapter, some of the new solutions of the text mentioned will have to be shown in detail because of their obvious relevance for legal dealing with acts of terrorism. However, here in the introductory notes, the following should be stressed: The Slovenian community of scholars of criminal law and criminology (the later a traditionally active and influential group, concentrated in the Institute for Criminology at the Faculty of Law of the University of Ljubljana) reacted very heavily to the new draft of the Criminal Code. On one hand, they criticized the conspiritual nature of the drafting of such an important act; above all, even for Slovenian circumstances, an unusually small number of experts in the working

[4] OJ RS 63/94 from 13 Ocotber 1994.

[5] OJ RS 23/99 from 8 April 1999.

[6] OJ RS 40/04 from 20 April 2004.

[7] OJ RS 14/07 from 16 February 2007.

group and the criteria of their election. On the other hand, several articles in Slovenian legal periodicals were published revealing severe legal–theoretical dilettantism of many proposed solutions in the general part and pointing to obvious attempts of members of the working group to declare some newly proposed instruments (like lifelong imprisonment) as the fulfilment of Slovenia's international legal obligations by manipulating and falsely interpreting some international treaties (like the Rome Statute). A number of criminologists began to raise political polemics in legal publications and the media about some solutions in the general (especially the introduction of lifelong imprisonment as the new highest punishment according to Slovenian law) and in the special part of the new draft. Some legal practitioners publicly refused the new draft as a degradation of theoretical and legislative-procedural standards. No lawyer, at least no one outside the working group, supported or defended the new draft in legal or other publications. In spite of that fact, the Ministry of Justice proposed the draft, compared with the version of October 2007 with minimal, theoretically insignificant changes, to the Government of the Republic of Slovenia in January 2008 and the Government adopted the draft on 17 January 2008 and sent it to the National Assembly for final adoption. It was adopted at the regular meeting of the Assembly in May 2008 and published in the Official Journal of the Republic of Slovenia Nr. 55/08 on 4 June 2008. According to the provisions on entry into force in the proposed Criminal Code, the act should enter into force on 1 November 2008.

A group of experts set up by the Slovenian Minister of Justice is drafting a new Criminal Procedure Act in the meantime. No complete draft is known to the (legal expert) public to this moment.

7.2 Substantive Criminal Law in Force

7.2.1 Introductory Words

For reasons of transparency and consistency of criminal legal order, Slovenian legislators, since the birth of the Yugoslav state after the Second World War, are making efforts to include all criminal offences in the Criminal Code. Even in the field of international crimes in the CC RS, there are no extra statutes. In the Chapter 35 CC RS, titled *Criminal Offences against Humanity and International Criminal Law*, there is a group of criminal offences that try to follow the definitions of classic war crimes and similar crimes against humanity from different relevant legal instruments of international criminal law. The titles of criminal offences are: *Genocide*, *Crimes Against Civil Population*, *Crimes Against the Wounded and the Sick*, *War Crimes Against Prisoners of War*, *War Crimes of Use of Unlawful Weapons*, *Recruitment of Persons, Younger than Eighteen Years*, *Unlawful Slaughtering and Wounding of the Enemy*, *Unlawful Plundering on the Battlefield*, *Infringement of Parliamentary Rights*, *Maltreatment of the Sick and Wounded and the Prisoners of War*,

Unjustified Postponement of Repatriation of Prisoners of War, *Destruction of Cultural and Historical Monuments and Sights*, *Warmongering*, *Abuse of International Symbols*, *Enslavement*, *International Terrorism*, *Endangering Persons under International Protection*, *Taking of Hostages*, and *Piracy*.

In this chapter, we find some criminal offences that at least partially surpass the current standards of international criminal law, for example *Maltreatment of the Sick and Wounded and the Prisoners of War (art. 382)*, *Destruction of Cultural and Historical Monuments and Sights (art. 384)*, and *Warmongering (art. 385).* All provisions from this chapter of the CC RS are considered to be a classic, historically and traditionally integrated part of Slovenian penal law, although these are not all of the substantive norms concerning humanity and international criminal law that are, according to Slovenian legal order, in force. According to articles 8 and 153 of the Constitution of the Republic of Slovenia, published treaties ratified by the National Assembly shall take immediate effect as supra-statutory positive laws. Laws not conformed to such treaties would be deemed unconstitutional. From the viewpoint of human rights, at least at the first glance, this seems to be a promising strategic legislative solution. However, let us look closer at how human rights are protected through criminal law in Slovenia dealing with terrorism.

7.2.2 Incriminations on Terrorism

Before analyzing in depth the main problems of Slovenian criminal legislation on terrorism from the viewpoint of human rights, let us briefly describe the relevant provisions in Slovenian's CC.

The Slovenian CC includes numerous incriminations on terrorism, the most general being Terrorism (art. 355), which incriminates the act of an explosion or fire, or any other act of violence endangering public safety, or threat of the use of nuclear materials or means of mass slaughter, thereby arousing fright and uncertainty among people, with the intention of jeopardizing the constitutional order or security of the Republic of Slovenia; and International Terrorism (art. 388), which incriminates similar acts against a foreign country or an international organization. While drafting these two incriminations in the early 1990s, the drafters were well aware of the importance of human rights due to the rich history of human rights infringements in the previous regime. Consequently, preparatory acts are incriminated only as a separate and independent criminal act. The current CC also no longer allows the use of the incrimination that incriminates all preparatory acts with an aim or goal to destabilize the country or destroy the constitutional order of the state ("*Unternehmungsdelikt*"). The use of this incrimination would mean the use of unclear incriminations, using the terms "act, pointing towards" and similar. In the current CC, the criminal act of Terrorism is defined as a political offence, which is, by its nature, inclined to abuse. That is why the drafters were very cautious with drafting this criminal act (Bavcon et al. 1995).

The Act Amending the Criminal Code from 2004 introduced a new incrimination, Financing of Terrorist Acts (art. 388.a). This amendment is obviously inspired by the UN International Convention for the Suppression of the Financing of Terrorism,[8] because it incriminates provision or collection of money or property with the intention to partly or wholly use it for the commission of certain criminal offences from CC, or any other violent act whose objective is to destroy the constitutional order of the Republic of Slovenia, cause serious disruption to public life or the economy, causes death or serious physical injury to persons not actively involved in armed conflict, to intimidate people or force the state or an international organization to carry out an act or not to carry out an act, even if the money or property provided or collected was not used for the commission of specified criminal offences. The Slovenian CC includes some more special incriminations, which are adjusted to international conventions for the protection of air and sea traffic and persons under international protection, such as Hijacking of an Airplane or Ship (art. 330), Attack on the Security of Air Traffic (art. 331), Destruction or Removal of Signs and Appliances, Important for the Security of Air Traffic (art. 332), Piracy (art. 391), Endangering Persons under International Protection (art. 389), and Hostage Taking (art. 390). In addition to these criminal acts, other articles are relevant, especially criminal acts related to nuclear and other types of weapons for mass destruction and criminal acts against life and physical integrity.

Although the legislation includes much useful incrimination, in its report on the evaluation of Member States' compliance with the Council Framework Decision of 13 June 2002 on Combating Terrorism,[9] the European Commission emphasized some inconsistencies in Slovenian legislation. A report on the measures taken by all the Member States to comply with the mentioned framework decision, including Slovenia, was written by the European Commission in November 2007 and presented to the Council of the European Union (but was not published in the Official Journal of the European Union).

For the correct understanding of the criticism addressed to Slovenia, it is useful to recall that the framework decision includes two types of offences; terrorist offences and offences linked to terrorist activities. The terrorist offences combine two elements: an objective element, as it refers to a list of instances of serious criminal conduct, as it is defined by the national law of Member States, and a subjective element, a special intent, which makes this conduct a terrorist offence. Slovenian legislation, however, does not include all the specified objective and subjective elements. Regarding the objective elements, the Slovenian CC incriminates all intentional acts, as specified in art. 1, par. 1 of the framework decision, but it does not define all of them as terrorist offences. Both criminal acts together do not cover all three subjective elements, required by the EU act, especially narrowing the intention of seriously destabilizing or destroying the fundamental political,

[8] It was ratified by Slovenia on 15 July 2004 and is enforced from 23 October 2004.

[9] OJ of the European Communities, L 164/2 from 22 July 2002.

constitutional, economic, or social structures of a country or an international organization to the protection of only constitutional order and security of Slovenia, leaving out protection of other countries and international organizations.

Regarding the second part of offences – offences linked to terrorist activities, Slovenia currently completely fails to comply with the framework decision. Aggravated theft, extortion, and drawing up false administrative documents, all with a special view to committing one of the terrorist offences, are incriminated in the current CC, but the special aim of the perpetrator to commit these criminal acts to enable terrorist offences does not change the criminal act into an aggravated offence. In this case, the only difference between "normal" extortion and aggravated extortion would be the existence of a special intent to commit extortion as a preparatory act to terrorist offence. Because the court and other institutions cannot read the intent, it has to be distinguished and proved from the objective act and not just assumed.

As already mentioned, new Criminal Code (entering into force on 1 November 2008) brings many changes in the field of terrorist criminal acts, including completely new incriminations. It abandons the division of internal and international terrorism and introduces new classification. Art. 108–111 regulate the incrimination of Terrorism, which includes terrorist acts against the Slovenian state and against other states and international organizations, Financing of Terrorist Acts, Public Provocation to Commit Terrorist Acts, and Recruitment and Training for Terrorist Acts. These criminal acts are prescribed on the basis of international legal acts.

According to the short explanation to the new CC, the criminal act of Terrorism (art. 108) should cover all the incriminations from the EU framework decision. However, looking closely, it is very unclear and confusing. As already explained, in the EU framework decision, a terrorist offence is defined by combining an objective element of nine acts, which should be prescribed in the national legislation of all Member States, and a subjective element; a special aim to intimidate the population, compel some authority to do or refrain from doing something, or to destabilize some organizational public structure. The new CC includes all of the subjective elements and also all of the objective requirements, but the later are described in a rather unclear and undefined way (Mozetič 2007). It speaks of a perpetrator, who, with the aim to seriously intimidate a population, or to unduly compel a Government or international organization to perform or abstain from performing any act, or to seriously destabilize or destroy the fundamental political, constitutional, economic, or social structures of a country or an international organization, performs one of 12 criminal actions prescribed by the proposed new CC. There are also nine additional objective requirements, which are alternatively prescribed by the EU framework decision.

This causes confusion in interpretation of this paragraph regarding whether these two groups of enumerated requirements are to be interpreted cumulatively or the new CC introduced additional criminal acts that should be considered as terrorist offences when performed with the special aim. The first interpretation leads to double incriminations; an act of assassination of the highest representatives of the state is always an attack on a person's life that may cause death, the new CC has double incrimination of hostage taking, and some criminal acts are just incompatible.

This first interpretation brings nothing but confusion. The second interpretation leads again to double incriminations (kidnapping for example) and to a broader objective element of terrorist offence (Mozetič 2007). The authors of this article feel that this incrimination should be revised towards more clarity of the criminal field. We could just follow the framework decision definition and should not add more elements, which just confuse the definition to the point that it does not fulfil the obligation of *lex certa.*

The second paragraph of art. 108 incriminates nuclear terrorism, and the following paragraphs cover aggravated forms, when a terrorist offence or nuclear terrorism is being committed and the consequence is the death of one or more persons, or when they are being committed in a criminal association.

The criminal act of the financing of terrorist acts remains punishable in the new CC, even if the money or property provided or collected were not used for commission of specified criminal acts, but these specified criminal acts are defined in a new way. They are limited to criminal offences, specified as a terrorist offence in the previous article.

The new CC also includes several special incriminations, already mentioned with the current CC (for example, Hijacking of an Airplane or Ship, Attack on the Security of Air Traffic, piracy, criminal acts related to nuclear and other types of weapons for mass destruction, and criminal acts against life and physical integrity).

7.2.3 Participation in Terrorist Criminal Acts

Regarding participation in terrorist criminal acts, two articles of the framework decision are of special interest: those regulating offences relating to a terrorist group and inciting, aiding, or abetting. Art. 2 defines a terrorist group as a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences, where a structured group shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership, or a developed structure. Many (Slovenian) theoreticians (Bavcon 2006b; Korošec unpublished) argue that the definition of the terrorist group is too broad and that the requirement that a member does not need to have a formally defined role, and that no continuity of its membership or a developed structure of the group are required, contradict the first requirement, that a terrorist group should not be randomly formed and should be a structured group. Notwithstanding these contradictions, the Slovenian legal system does not recognize a special terrorist group, but it does include a more general criminal association. As defined in art. 126 (the meaning of terms in this code), a criminal association is a group of at least three persons who have joined for the commission of criminal offences for which a punishment by imprisonment of more than 3 years may be prescribed. Generally speaking, this group complies with the definition of the terrorist group. Because the Slovenian CC requires at least three persons, the Slovenian criminal association covers fewer asso-

ciations than the terrorist group from the EU framework decision, which requires at least two persons. It remains open whether the description of the criminal association complies with the EU structured group. However, because the description of the structured terrorist group is contradictory and because Slovenian theoreticians (Bavcon & Šelih 2003) emphasize that the term criminal association should be built on a structured group of individuals that divide their work and possess the intent to commit crimes together to comply with the rule of law, prescribed in art. 2 of the Slovenian Constitution, we can conclude that the Slovenian regulation of criminal association complies with the formal EU understanding of the term terrorist group. It must also be added that both criminal acts of terrorism fulfil the requirement that more than 3 years punishment may be imposed. The framework decision incriminates both, directing a terrorist group and participating in activities of a terrorist group, as does also the Slovenian CC in art. 279 (Criminal Association). However, Slovenian theory (Bavcon & Šelih 2003; Deisinger 2002; Bele 2001) stresses that the establisher and participants need to posses direct intent for establishing or participating in criminal association and intent to commit crimes in association. According to the Slovenian CC, when participants and the establisher commit the criminal act intended in the criminal association, the criminal act of solely participating or establishing criminal association looses independence and the rule of merger of offences is used, unless the act of establishing criminal association itself carries enormous criminal content, which cannot be disregarded (Bavcon & Šelih 2003).

Slovenian legislation also complies with the EU requirement that inciting, aiding, and abetting are punishable. According to the Slovenian CC, aiding and abetting are punishable acts (art. 25–27 and art. 287 – Accessory to the Perpetrator after the Commission of Criminal Offence), especially the criminal act of Financing of Terrorist Act (art. 388.a) should be mentioned. It remains questionable, however, whether inciting is punishable in current Slovenian CC, because it is unclear whether inciting is broader than abetting. The Slovenian CC namely does not recognize a special incrimination of inciting, only a provision on abetting in the general part of the CC. Consequently, if inciting is broader in its meaning than abetting, then inciting is not punishable in Slovenian law (Korošec 2003).

The new CC brings new solutions in the field of participation. It incriminates some new criminal acts, which are by their nature acts of aid. One of these is par. 3 of art. 108, which incriminates aiding and preparing of terrorist offence through acquiring necessary funds, compelling another to participate in a terrorist offence, or drawing up false administrative documents. This criminal act is *lex specialis* towards general rules on criminal act participation.

Another new incrimination is the incrimination of public provocation to commit a terrorist offence, which punishes the distribution, or otherwise making available, of a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed. This incrimination was transferred from the Council of Europe's Convention on the Prevention of Terrorism and represents a novelty. In the current CC, only general rules on abetting or maybe the criminal act of Stirring up Hatred, Strife or Intolerance based on

Violation of the Principle of Equality (art. 300) can cover such prohibitions, but they do not cover all aspects of this new incrimination.

The incrimination of Recruitment and Training for Terrorism is also modelled after the Council of Europe convention and it also represents a *lex specialis* form of aiding as well as complicity in terrorist offence. Recruitment is defined as soliciting another person to commit or participate in the commission of a terrorist offence, or to join an association or group for the purpose of contributing to the commission of one or more terrorist offences by the association or the group and, in the current CC, can be covered by general rules on abetting. Training for terrorism is defined as provision of instruction in the making or use of explosives, firearms, or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence. This definition regrettably left out the last part of the Council of Europe's definition: "knowing that the skills provided are intended to be used for this purpose." This crucial last part of the definition demands the perpetrator's knowledge, that the skills are intended to be used for terrorist offence, and that it fulfils the obligation of objective – subjective definition of criminal offence. The act must be recognizable in the physical sense and the perpetrator's knowledge and intent to use these skills for commission of a terrorist offence must be present.

The new CC also deals with new aspects of criminal association and brings new general rules on participation in the criminal act (art. 37–41), which remain relevant for terrorist offences, because the new CC still does not incriminate a special terrorist group. In art. 294, there is the old incrimination of establishing, leading, or participating in a criminal association, but the new art. 41 changes the definition of criminal association (into minimum three persons, of which at least two commit the criminal act as an execution of criminal plan of the criminal association) and introduces the possibility of an aggravated offence, when committed in a criminal association. This aggravated offence must then be prescribed with the criminal act itself, where intended. According to the introductory explanation to the proposed, this article introduces a special form of complicity and regulates when and how a participant or a leader of criminal association is punished. The third paragraph incriminates also the leader of the criminal association, who led the implementation of a criminal plan or profited from the pecuniary gain, won via the criminal act, that was included in criminal plan. It is of no importance whether the leader physically committed the criminal act as a perpetrator or participant.

7.2.4 Phases of the Criminal Act

The current Slovenian CC as well as the new CC in its general part incriminate inter alia the attempt to commit a criminal act, whenever somebody intentionally initiated a criminal offence but did not complete it, provided that such an attempt involved a criminal offence for which the sentence of 3 year's imprisonment or a heavier sentence may be imposed under the statute; attempts involving any other criminal offence

shall be punishable only when expressly stipulated by the statute, that is, in its special part (art. 22). Criminal attempts of Terrorism and International Terrorism are punishable, as well as criminal attempts of aggravated theft, extortion, and drawing up false administrative documents, according to the current CC. According to the CC, preparatory acts to criminal acts are not punishable, except when constituting an independent criminal act (so-called *delictum sui generis*), regulated in the CC. In the case of terrorism, several such criminal acts are relevant: the aforementioned Criminal Association (art. 297), Criminal Conspiracy (art. 298), and Manufacture and Acquisition of Weapons and Instruments Intended for Committing of Criminal Offence (art. 309). If the main criminal act is also committed afterwards, the rule of merger of criminal acts is to be applied and the preparatory act looses its independence, becoming the included offence (Bavcon & Šelih 2003).

7.2.5 Criminal Responsibility

In the current and in the newly adopted CC, the requirement of *dolus directus* is prescribed. The current CC demands direct intent with special aim of jeopardizing the constitutional order or security of the Republic of Slovenia (with terrorism) or the special aim of inflicting damage on a foreign state or an international organization, or compelling a legal person, international organization, or state to perform or to omit a certain act (with international terrorism). That excludes the use of *dolus eventualis* and demands even *dolus coloratus*; direct intention to commit these criminal acts, coloured with special aim.

This is also true for the newly adopted CC. For the criminal act of terrorism, a special aforementioned aim of seriously intimidating a population, unduly compelling a government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organization is demanded and *dolus eventualis* does not suffice.

7.2.6 Liability of Legal Persons

The Slovenian CC introduced the liability of legal persons in 1994 (art. 33). A legal person is liable for criminal act when the perpetrator (a natural person) commits the criminal act in its name, on its account, or in its favour. It is regulated by a special act, the Act on Responsibility of Legal Persons ("*Zakon o odgovornosti pravnih oseb za kazniva dejanja*"),[10] which was introduced in 1999. This act introduced a catalogue of criminal acts for which a legal person can be held responsible. Among

[10] OJ RS 98/04 from 9 September 2004.

these criminal acts are also Criminal Association, Criminal Conspiracy, and Financing of Terrorist Acts, but not Terrorism, International Terrorism, and other more special criminal acts.

The newly adopted CC is keeping the legal basis for liability of legal persons, however, the most important will be the amendment of the Act on Responsibility of Legal Persons, because the criminal acts for which a legal person can be liable are enumerated.

7.3 Criminal Procedural Law

Slovenian theory observes that there are two general consequences in the field of criminal procedure due to an "efficient fight against terrorism" in all criminal legislations: increase of power of authority by repressive authorities and a reduction of judicial control (Bošnjak 2005). This can lead to infringements of human rights, in concrete, the right to judicial protection, defined also by art. 23 of the Slovenian Constitution. According to this article, everyone has the right to have any decision regarding their rights, duties, and any charges brought against them made without undue delay by an independent, impartial court constituted by law.

According to the Criminal Procedure Act, criminal acts of terrorism, international terrorism, and, according to the new CC, terrorism and all accompanying criminal acts fall into the jurisdiction of the district court. Because of the height of the penalty that may be imposed, the defendant is given a compulsory defence counsellor because the indictment is served to him and the defendant is in custody the whole time (art. 70). That provision guarantees the defendant a constitutional right to defend themselves, as defined in art. 29 of the Constitution of the Republic of Slovenia, which guarantees that anyone charged with a criminal offence, among other rights, also has the right to conduct their own defence or to be defended by a legal representative.

In the course of criminal proceedings against defendants charged with a terrorist offence, the police, state attorney, and the judicial branch have numerous additional measures at their disposal, due to the dangerousness of the alleged criminal act. These measures are also the ones that infringe human rights the most (for example, the rights to privacy and to personal liberty defined in art. 35 and 19 of the Slovenian Constitution). The right to privacy is being infringed by concealed investigatory action (secret surveillance, metering, monitoring and production order, monitoring of electronic communications, control of letters and other parcels, control of the computer systems, listening to and recording of conversations with the permission of at least one person participating in the conversation, listening and surveillance in another person's home or in other areas with the use of technical means for documentation and where necessary secret entrance into the aforementioned home or area may exceptionally be ordered against such person, measure of feigned purchase, and feigned acceptance or giving of gifts or feigned acceptance or giving of bribes). These measures are very intrusive and infringe the right to

privacy, especially the right to communication privacy (art. 35 and 37), and the right to inviolability of dwellings (art. 36 of the Constitution). That is why this regulation is of a highly sensitive nature. The Constitutional Court of the Republic of Slovenia has already annulled the whole legislation on concealed investigatory action in the Criminal Procedure Act. Consequently, the Act on Criminal Procedure was amended and this new legislation is very detailed and complex, although some irregularities can still be found (some were missing standard of proof,[11] and some measures are still very broad and lead to very deep privacy intrusions).[12]

Regarding the right to personal liberty, the measure of custody and alternative measures are relevant. In Slovenia, a defendant accused of a criminal act for which the punishment of 5 or more years of imprisonment may be imposed can be held in custody for a maximum of 6 months before the indictment is filed and then 2 more years after that. These deadlines represent a serious problem for the Slovenian judicial system, because the procedures last longer, but after 2 years and a half, the defendant must be released (Fišer 2007), and this represents a threat that the person will flee, especially inside the Schengen system.

The Act amending the Criminal Procedure Act from 2005 introduced the possibility of a joint investigation team according to EU law. Terrorism is one criminal act where international cooperation is necessary and wished for. Slovenian policemen may cooperate with policemen from other member states or other countries in a criminal investigation or in the pre-trial phase. The joint investigation team may also include Europol, Eurojust, or Olaf representatives (according to the EU framework decision (Zgaga & Ambrož 2007)).[13]

Given the nature of the criminal act, witness protection in criminal proceedings against defendants charged with terrorist offences is very useful and common. In Slovenian law, the ample regulation of witness protection is new. The Criminal Procedure Act has had some general provisions on witness protection since its adoption in 1994. A witness was protected when giving testimony during the investigation

[11] For example, for the physical examination of the defendant and other persons, no standard of proof is required (art. 266 of the Criminal Procedure Act), the prosecutor needs only to establish that the physical examination of the defendant is necessary to establish facts material to criminal procedure, or, in the case of other persons, that it is necessary to establish whether a particular trace or consequence of criminal offence has been left on their body. No standard of proof is also required for the production of the documentation on the deposits, statement of account and account transactions or other transactions, and for monitoring order of the financial transactions (art. 156).

[12] Art. 156 can be also used as an example for a broad definition of a measure. Production and monitoring order can be used against the suspect, the accused, and other persons who may reasonably be presumed to have been implicated in the financial transactions or deals of the suspect or the accused. The range of data that can be required through this measure is very broad (information and send documentation on the deposits, statement of account, and account transactions or other transactions), and the data can be used in various way (data might represent evidence in criminal proceedings or may be necessary for the confiscation of objects or the securing of a request for the confiscation of proceeds or property in the value of proceeds).

[13] Council Framework Decision of 13 June 2002 on Joint Investigation Teams, OJ of the European Communities, L 162 from 162, 20 June 2002.

and trial. With an act amending the criminal procedure act from 2004, the circle of endangered persons broadened. The act also more precisely regulated the procedure of deciding whether the person is entitled to witness protection during the phase of judicial investigation and trial. In 2005, a special Witness Protection Act was adopted.[14] It regulates conditions and procedures for witness protection and for protection of other persons who are endangered due to their cooperation in a criminal procedure. The right of a witness to witness protection and special types of witness examination infringes the right to defence from art. 29 of the Slovenian Constitution and the right to examine witnesses against the defendant from the art. 6 of the European Convention of Human Rights. Consequently, this regulation has already been a matter of constitutional debate. The Constitutional Court decided that the mere fact that the court denied the request to directly question the undercover police co-worker who had written the incriminating report about the defendant does not automatically mean that the defendant's right to test witness evidence has been infringed. In disputed criminal procedures, courts did not even think of the possibility to use measures to protect the witness and at the same time question them. They simply refused to question the witnesses at all. When the court uses aggravating testimony as evidence, it should enable the defence to test the evidence.

The proposed new Criminal Procedure Act was partially announced by the Ministry of Justice in December 2007. It does not bring any changes in the field of these measures, because it focuses on the elimination of judicial investigation and of the investigative judge and on the more powerful role of parties in criminal proceedings. Of course there is a general question of balance between defence and prosecution in the pre-trial phase, but the question of custody, concealed investigatory action, and joint investigation team is not regulated any differently than in the current Criminal Procedure Act.

However, already by the year 1999, the Slovenian Police got the authority to perform anti-terrorist control, which combines anti-bomb, chemical, bacteriological, and radiological checks and anti-audio and visual surveillance control (art. 40 of the Police Act, art. 27 and 28 of Rules on Police Powers) [15] as one of police powers.

7.4 Conclusion

Last but not least, it should be emphasized that the EU framework decision on combating terrorism itself demands respect for human rights and claims that it shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in art. 6 of the Treaty on European Union. This article refers to the right to a fair trial, as referred to in art. 6 of the European Convention for Human Rights. Because terrorism is recognized as a threat to modern

[14] OJ RS 91/06 from 31 July 2006.

[15] OJ RS 107/06 from 17 October 2006.

democratic society, authorities get more and more powers, which also infringe human rights, these measures being the concealed investigatory action, custody, or witness protection. Slovenian legislation in these fields has already been amended according to the Constitutional Court case law. Consequently, it is in general compliance with criminal proceedings standards. In addition, in criminal procedure, authorities have not gotten any new special measures solely for the case of criminal acts of terrorism, but general measures for the investigation and prosecution of serious criminal acts should be applied.

The EU Commission in its report also sets up the substantive rights, such as rights to strike, to freedom of assembly, of association or of expression, to form and join trade unions, and to demonstrate. These rights touch the core rule of substantive criminal law: the rule of *lex certa*, as defined in Slovenian Constitution and case law of the Slovenian Constitutional Court. It is recognized that the main problem with incriminating the participation and establishment of a terrorist group is the distinction between benign and malign groups (Bavcon 2006a, b). The only distinction lies in their aim; the aim to commit a terrorist offence or not. Slovenian theory often warns that this distinction in the aim of a group should be recognizable from its action and not only from assumption (Mozetič & Bavcon 2007; Bavcon & Šelih 2003). Here lies also the main problem of substantive criminal law regarding terrorism, when it cannot be objectively defined, which act is punishable and which is not. So the method of incriminating the membership of, joining, or the forming of a terrorist group solely on the basis of aim of the group opens the door to possible abuses of criminal law. In closing, we again emphasize the disturbing new incrimination of Terrorism (art. 108) in the new CC, which defines terrorism half according to the framework decision, but also adds additional elements that make the incrimination very indefinite and unclear, leaving the door open to contradictory interpretations, of which none makes sense. In other words: with the new criminal provisions in Slovenia regarding terrorism, human rights are at least potentially more endangered than they were before.

Last, but not least, we mention the impact of terrorism and the fight against terrorism on politics and criminal policy. We must conclude that adopting amendments on terrorism to the CC and other acts is just a matter of complying with international obligations and standards and not a high-profile issue in Slovenian politics and criminal policy. Terrorism is also neither a feature in broader media discussions nor the in case law of Slovenian courts with an exemption of one case few years ago. A person was convicted of endangering persons under international protection (art. 389/I of CC), because he had written a threatening e-mail to a president of a foreign state. This was the only time in recent time that the issue of terrorism was broadly discussed in the media and Slovenian court.

References

Annex to the Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on Combating Terrorism, 6.11.2007.

Bavcon, L. (2006a). Okvirni sklep Sveta Evropske unije o boju proti terorizmu. *Pravosodni bilten*, *1*.

Bavcon, L. (2006b). Statut kazenskega prava v pravnem redu Evropske unije. In D. Korošec (Ed.), *Izzivi in odzivi* (pp. 299–311). Ljubljana: Uradni list Republike Slovenije.

Bavcon, L. & Šelih, A. (2003). *Kazensko pravo: splošni del*. Ljubljana: Uradni list Republike Slovenije.

Bele, I. (2001). *Kazenski zakonik s komentarjem: splošni del*. Ljubljana: GV Založba.

Bošnjak, M. (2005). S pravom nad terorizem. *Pravna praksa*, *33*, 3.

Council Framework Decision on Combating Terrorism (2002/475/JHA), Official Journal L 164, 22/06/20002.

Criminal Code of the Republic of Slovenia (official consolidated text), UL RS, 95/2004.

Criminal Code of the Republic of Slovenia – 1, UL RS, 55/2008 and 66/2008.

Criminal Procedure Act (official consolidated text), UL RS, 32/2007.

Deisinger, M. (2002). *Kazenski zakonik s komentarjem: posebni del*. Ljubljana: GV Založba.

Fišer, Z. (2007). Omejevalni ukrepi. In K. Šugman (Ed.), *Izhodišča za nov model kazenskega postopka* (pp. 221–255). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

Kazenski zakonik Republike Slovenije z uvodnimi pojasnili Ljuba Bavcona, Ivana Beleta, Mitje Deisingerja, Draga Demšarja, Zvonka Fišerja, Milana Kosterce, Pavla Martonošija, Alenke Šelih in stvarnim kazalom Vida Jakulina (1995). Ljubljana, Uradni list RS.

Korošec, D. (2008) A *Challenge for Contemporary Substantive Criminal Law – How to Efficiently Supress Terrorism While Preserve Fundamendal Human Rights*. Zagreb: Faculty of low.

Korošec, D. (2002). *Terorizem kot izziv za (materialno) kazensko pravo*. Ljubljana: Pravna fakulteta v Ljubljani.

Korošec, D. (2003). *Mednarodno kazensko pravo; Posebni del*. Ljubljana: Pravna fakulteta v Ljubljani.

Mozetič, P. (2007). *Kaznivo dejanje terorizma v osnutku predloga novega kazenskega zakonika (KZ-1).* Article for the conference on draft of new Criminal Code.

Mozetič, P. & Bavcon, L. (2007). K vprašanju o stopnjah uresničevanja kaznivega dejanja – pripravljalna dejanja. In A. Šelih (Ed.), *Sodobne usmeritve kazenskega materialnega prava* (pp. 181–197). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani. <ch editor>

Police Act (official consolidated text), UL RS, 107/2006.

Proposed New Criminal Code, announced October 12th 2007, not yet adopted.

Proposed New Criminal Procedure Act, announced December 2007.

Report from the Commission based on Article 11 of the Council Framework Decision of 13 June 2002 on Combating Terrorism, 6.11.2007.

Šelih, A. (2003). Človekove pravice in terorizem. *Pravna praksa*, *1*, 3.

Zgaga, S. & Ambrož, M. (2007). The Changes of Slovenian Criminal Procedural Legislation in Relation to EU Criminal Legislation. In Đ. Ignjatović (Ed.), *Stanje kriminaliteta u Srbiji I Pravna sredstva reagovanja* (pp. 22–40). Beograd: Pravni fakulteta u Beogradu.

Chapter 8
Extraordinary Renditions – Shadow Proceedings, Human Rights, and "the Algerian six": The War on Terror in Bosnia and Herzegovina

Almir Maljević[1]

8.1 Introduction[2]

The decision of the US Supreme Court of 12 June 2008 in *Boumediene et al. v. Bush et al.* (No. 06–1195) and *Lakhdar Boumediene et al. v. Bush, President of the United States et al. and Khaled A. F. Al Odah, next friend of Fawzikhalid Abdullah Fahad Al Odah et al. v. United States et al.* ruled that denying the petitioners (alleged terrorists imprisoned in Guantanamo Bay in the aftermath of the 9/11 attacks) access to *habeas corpus* had been illegal. Thereby, the US Supreme Court confirmed that "some of the petitioners have been in custody for 6 years with no definitive judicial determination as to the legality of their detention. Their access to the writ is a necessity to determine the lawfulness of their status, even if, in the end, they do not obtain the relief they seek."[3] This practically means that the detainees had been imprisoned based on the decisions of the US Government without adequate legal means being provided to find or present evidence to challenge its decisions.

A. Maljević (✉)
Faculty of Criminal Justice Sciences, University of Sarajevo, Sarajevo, Bosnia and Herzegovina
e-mail: A.Maljevic@mpicc.de

[1] Many thanks to Marianne L. Wade and Erik Luna for their comments and suggestions

[2] This chapter is an updated version of the article published in Derenčinović/Becker 2008: 159.

[3] Supreme Court of the United States, Opinion of the Court in Lakhdar Boumediene et al. V. Bush, President of the United States et al. and Khaled A. F. Al Odah, next friend of Fawzikhalid Abdullah Fahad Al Odah et al. v. United States et al., 12 June 2008, p. 8.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_8, © Springer Science+Business Media, LLC 2010

The process leading to this judgement began when Congress, in order to prevent any further acts of international terrorism against the USA, authorised President Bush "to use all necessary and appropriate force against those nations, organisations, or persons he determines planned, authorised, committed, or aided the terrorist attacks that occurred on 11 September 2001, or harboured such organisations or persons." The measures deployed to get bring suspected terrorists into US custody, the locations created to imprison any such suspects caught (black sites) and the newly developed, so-called "enhanced" methods of interrogation declared suitable to glean information from them, introduced pursuant to this authorisation and swiftly put in practice, quickly displayed that the new approach introduced by the US administration has little to do with the human rights standards developed in the last decades, so far regarded as inviolable categories in Europe and beyond.

Very few persons, if any, could have imagined the implications that the US congressional resolution "Authorisation for use of US Armed Forces" of 14 September 2001, followed by the instructions and powers given to the CIA by President Bush and his administration would have on the European human rights debate. According to the official reports (CLAHR 2006; TCEP 2006; CPT 2007), and contrary to their denial (AI 2006:1), several Council of Europe as well as European Union member states, declared democracies bound by the European Convention on Human Rights, and other conventions that serve as safeguards of human rights have been shown to have played an important role in US' activities to detain persons suspected of involvement in international terrorism and transferring them to other locations (black sites) for interrogation purpose; in other words, to have played an active role or "turned a blind eye" (TCEP 2006) in so-called extraordinary and reverse[4] rendition procedures.

This chapter attempts to give a deeper insight into the rendition practice which played out in Bosnia and Herzegovina in the case known as "The Algerian six," by relating the facts of the case to the relevant domestic and international law. This case, in which Bosnia and Herzegovina handed over its citizens to US forces flying in the face of decisions of the country's competent courts and institutions, raises several issues related to international law as will be shown.

[4]For the purpose of this article, extraordinary rendition is to be understood as the transfer of an individual, with the involvement of US personnel or persons acting as US agents, to a foreign State in circumstances that make it more likely than not that the individual will be subjected to torture or cruel, inhumane, or degrading treatment. Reverse rendition is to be understood as foreign authorities detaining persons in non-combat scenarios and handing them over to US custody using procedures without basic legal protection (*see* Fisher/Satterthwaite, 2005: 6).

8.2 The "Algerian six" Case[5] Unfolds

"The Algerian six"[6] is the case of six men, five of whom[7] are naturalised citizens of Bosnia and Herzegovina and one[8] citizen of Algeria with a permanent residence permit for Bosnia and Herzegovina. All six of them are family men, with all but one (Nechle) married to wives[9] of Bosnian and Herzegovinan nationality. All have children. They were of different professions: some being imams (religious officials), some administrators, some Arab language teachers, mechanics, and they were all (but Bensayah)[10] employed by various humanitarian organisations in the country. The exact time at which they and their reason for entering the country is unclear but they gained citizenship or a permanent residence permit for Bosnia and Herzegovina at different times in the period between 1995 and 1997.

The Algerian six first came into contact with the criminal justice system of Bosnia and Herzegovina on 19 October 2001, when the Federal Prosecutor requested that the Supreme Court of the Federation of Bosnia and Herzegovina (the Supreme Court) open a criminal investigation into allegations of a foiled terrorist plot against the US and UK Embassies[11] in Sarajevo against eight persons: "The Algerian six" and two other persons, namely Khaled El Arbed and Atif Munassura. According to the Federal prosecutor, there was reasonable suspicion that they may have committed a criminal offence as defined by article 168 (1) (International terrorism) of the CCFBH in conjunction with articles 20(1) (Criminal attempt) of the CCFBH,

---

[5] The facts presented here as well as the analysis that follows are predominantly based on the following decisions of the Human Rights Chamber of Bosnia and Herzegovina: Decision on admissibility and merits (11 October 2002) Cases no. CH/02/8679, CH/02/8689, CH/02/8690, and CH/02/8691 (HRC, Decision I); Decision on admissibility and merits (4 April 2003) Case no. CH/02/8961 (HRC, Decision II); and Decision on admissibility and merits (4 April 2003) Case no. CH/02/9499 (HRC, Decision III), as well as on the brief submitted by the United Nations Office of the High Commissioner for Human Rights (UNOHCHR, Brief) (Field Operation in Bosnia and Herzegovina) to the HRC as the *amicus curiae* in Cases no. CH/02/8679, CH/02/8689, CH/02/8690, and CH/02/8691.

[6] Although the case is known as "The Algerian six," it is not known whether all the persons involved were actually citizens of Algeria. According to the HRC (Decision III, Para. 14), Belkasem Bensayah (*see* footnote 7) had two identities; one as Belkasem Bensayah born in Yemen and another as Abdulkarim al-Sabahi born in Yemen.

[7] Hadj Boudellaa, Boumediene Lakhdar, Mohamed Nechle, Mustafa Ait Idir, and Belkasem Bensayah were citizens of Bosnia and Herzegovina.

[8] Saber Lahmar was not a citizen of Bosnia and Herzegovina but had a permanent residence permit.

[9] Interestingly, Hadj Boudellaa claimed before the HRC that he has six children, and one on the way, with two wives. Bigamy, however, is forbidden and prescribed as a criminal offence by the Criminal Code of the Federation of Bosnia and Herzegovina (CCFBH) which was the law in force at the time.

[10] Bensayah claimed never to have worked in Bosnia and Herzegovina and to have been financially supported by his family in Yemen.

[11] The HRC, Decision III mentions both embassies whereas the UNOHCHR, Brief mentions the US Embassy only.

and that Saber Lahmar alone may have committed a criminal offence as defined by article 353(1) (certifying a falsehood in a public document) of the CCFBH. The Federal Prosecutor requested that the suspects be subject to pre-trial detention. Bensayah, individually, was already under investigation as of 8 October for allegedly committing the criminal offence of certifying a falsehood in a public document,[12] Lahmar and Ait Idir were arrested on 18 October, and the remaining members of "the Algerian six" group were arrested and brought into custody of the Supreme Court on 19 (Nechle), 20 (Lakhdar), and 21 (Boudellaa) October 2001. In the following days, the investigative judge of the Supreme Court issued separate orders for 1-month pre-trial detention. These orders were extended on 16 November for an additional 2 months. An investigation was officially initiated by the investigative judge of the Supreme Court on 30 October, by which time all persons were already in pre-trial detention.

In synchrony with the extension of the pre-trial detention order (16 November 2001), the Federal Ministry of the Interior issued a decision revoking the citizenship of the five suspects. According to the ministry, this decision was justified on grounds that criminal charges were brought against the suspects leading to a conclusion that when they applied for citizenship, they had concealed their intentions to violate the Constitution and the laws of the Federation of Bosnia and Herzegovina (*see* HRC, Decision I: Para 43; HRC, Decision II: Para 17; Decision III: Para 38). As soon as these decisions were approved by the Ministry of Civil Affairs and Communications (on 28 December), the Federal Ministry of Interior submitted a request to that ministry that the suspects be expelled from the territory of Bosnia and Herzegovina (*see* HRC, Decision I: Para 48; HRC, Decision II: Para 22; Decision III: Para 42). Lahmar's permanent residence permit was retracted by the Ministry of Human Rights and Refugees of Bosnia and Herzegovina on 23 November. That decision was based on Lahmar's previous sentence to 5 years imprisonment on 9 July 1998 by the Supreme Court.[13] In other words, the ministry claimed that the fact that he was sentenced to imprisonment for longer than 4 years provided grounds for the termination of his residence permit in accordance with article 29 (1b) of the Law on Immigration and Asylum of Bosnia and Herzegovina. All citizens of Bosnia and Herzegovina, on 20 December the members

[12] According to the police, in the course of the search of Bensayah's apartment within the framework of the initial investigation related to the criminal offence of certifying untrue matter in a public document (related to the fact that Bensayah was residing in Bosnia and Herzegovina under two names), a telephone number of a senior liaison officer of Osama bin Laden was found. On that same day, while the search was still underway, the Federal Minister of Interior issued a communiqué stating that the suspect was found in possession of the telephone number so it was broadcasted in the news on that very evening. Bensayah, himself, claims not to have known the person (bin Laden's senior liaison officer) and to have seen that phone number for the very first time on 25 October when he was questioned by the US Federal Bureau of Investigation (FBI). *See* HRC, Decision III, Paras. 18–21.

[13] After serving less than 18 months, his remaining sentence was exchanged for a suspended sentence, conditional upon him not committing a new criminal offence within next 2 years. *See* HRC, Decision I: Para 45.

of "the Algerian six" group (but Bensayah)[14] initiated an administrative dispute before the Supreme Court challenging the decision to revoke their citizenship, whereas Lahmar appealed against the decision that his residence permit be terminated on 11 January 2002.

As the Ministry of Civil Affairs and Communications took no action in response to its request to expel the suspects, on 10 January 2002, the Federal Ministry of the Interior issued a decision refusing entry to the territory of Bosnia and Herzegovina for all six suspects by means of which all the suspects were ordered to leave the country immediately (*see* HRC, Decision I: Para 49; HRC, Decision II: Para 23; Decision III: Para 43).

On the basis of the decisions revoking the suspects citizenship and, respectively, terminating the relevant residence permit (ignoring the fact that an appeal had been lodged against all these decisions or pending deliberation in legal proceedings) as well as on the decision concerning the refusal of entry for all suspects, on 11 January 2002, the Ministry of Foreign Affairs of Bosnia and Herzegovina contacted the People's Democratic Republic of Algeria inquiring about the possibility to deport the suspects to their native country. The Embassy of the People's Democratic Republic of Algeria from Rome responded to that inquiry on 12 January stating that "the unilateral decision on deportation of the six persons… is inadmissible" and "therefore those competent in Algeria call upon the competent institutions in Bosnia and Herzegovina to annul all actions undertaken to enable implementation of these decisions in an operation foreseen for 14 January 2002" (*see* UNOHCHR, Brief: 3).

Given that their pre-trial detention was due to expire and the suspects to be released because of a lack of evidence against them, the suspects feared that, after Algeria refused to accept them, they might be handed over to US forces stationed in Bosnia and Herzegovina. For this reasons, between 11th and 16th of January 2002, their lawyers submitted requests to the HRC that the decisions on the revokation of citizenship and the termination of Lahmar's residence permit be annulled and an order issued provisionally prohibiting deportation, extradition, or any other form of handover of the citizens of Bosnia and Herzegovina to any other state (UNOHCHR, Brief: 3).

On being informed by the Federal Prosecutor that there were no further reasons or circumstances based on which pre-trial detention could be imposed, the investigative judge of the Supreme Court ordered on 17 January 2002 that all six men[15] be released from pre-trial detention immediately. On the same day, the US Embassy sent a diplomatic note to the Ministry of Foreign Affairs of Bosnia and Herzegovina stating that the USA were prepared to assume custody of the six specified Algerian citizens and that, should it be acceptable to the Government of Bosnia and

[14] Bensayah, although in disagreement with the arguments of the decision decided not to appeal against it as he was aware of other reasons that would justify the decision. *See* HRC, Decision III: Para 40.

[15] It should be noted here that their pre-trial detention started at different times so they were due to be released at different times. However, the investigative judge ordered their simultaneous release.

Herzegovina, the USA would arrange to take physical custody at a time and location convenient for both states (*see* UNOHCHR, Brief: 3).

Meanwhile, Amnesty International (AI Index 2002) warned Bosnia and Herzegovina that "Governments cannot just ignore their human rights obligations. These men should only be transferred to US custody following proper extradition proceedings before a court of law and after the Federation authorities have obtained firm guarantees that they will not be tried before the special military commissions or face the death penalty." Amnesty International thus clearly also feared that if transferred into US custody, the suspects might face unfair trials before newly established special military commissions and risk being sentenced to death.

At the same time (17 January 2002), the Human Rights Chamber, by means of a provisional measures order, obliged Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina to take all necessary steps to prevent the suspects' removal from Bosnia and Herzegovina by the use of force (UNOHCHR, Brief: 3). This order was sent not only to the two governments concerned but to all major national and international organisations tasked with promoting the rule of law in the country, including the Office of the High Representative of the International Community, the OSCE, the UNMBiH Human Rights Office, the International Police Task Forces Commissioner's Office, and the Human Rights Ombudsman of Bosnia and Herzegovina.

Following the order of the Supreme Court, the suspects were released from pretrial detention shortly before midnight but, due to unauthorised demonstrations of around 500 citizens, could not leave the area before the early morning of 18 January 2002, at which time police officers of the Federal Ministry of the Interior took them to an, at the time, unknown location. Later that day, it, however, became apparent that the Algerian six were handed over to US forces as the US Embassy issued a press release confirming that the six Algerian nationals whose involvement in international terrorism had been demonstrated and who therefore posed a credible security threat to US personnel and facilities in Bosnia and Herzegovina were in US custody.

Although the location to which the Algerian six were transferred was not known for some time, as of late January 2002[16] Amnesty International assumed (AI Index 2002) that they were in Camp X-Ray at Guantanamo Bay in Cuba. Despite Amnesty International's efforts urging US authorities to inform the Algerian six's families and lawyers of their detention location (AI Index 2002), official confirmation – in form of a letter, stating that they were transported by US forces to Guantanamo Bay on 19 January 2002 and were being held as enemy combatants, thus to be treated

[16] According to the memorandum, based on the official information, the legal representatives of the Algerian six received from the US Government in response to a lawsuit under the US Freedom of Information Act regarding the transportation of the six Bosnian citizens and former residents from the territory of Bosnia and Herzegovina to Guantanamo Bay, Cuba, and written by Stephen H. Oleskey to the Temporary Committee on the Transportation and Illegal Detention of Prisoners of the European Parliament, US forces made use of airports located in Germany (an EU Member State), Turkey (an EU candidate country), and Bosnia and Herzegovina (a potential EU candidate country), and of those countries' airspace, in order to carry out the rendering of citizens and former residents of Bosnia and Herzegovina to Guantanamo Bay (*see* Oleskey, 2006).

in accordance with the Third Geneva Convention,[17] was delivered to their legal representatives in Bosnia and Herzegovina and family members only on 31 December 2002 (*see* HRC, Decision II: Para 32; HRC, Decision III: Para 51). These letters also contained notice from the US Embassy in Sarajevo informing the Algerian six's family members that correspondence with their relative was possible; visits by family members, attorneys, and members of international organisations, and public interest groups, however, prohibited.

On the basis of this brief overview of the proceedings prior to the handover of the "Algerian six" as well as the handover to US authorities itself, it is plausible to assume that Bosnia and Herzegovina went above and beyond what the law allows in trying to comply with the requests of the USA in relation to rendering to them persons suspected of international terrorism. The following paragraphs will shed light on the most relevant provisions of international law that may have been breached in this exemplary case of reverse rendition.

8.3 The "Algerian six" and the European Convention on Human Rights

A case that is as complex as that of the "Algerian six" raises several issues related to relevant domestic and international law. A contribution of this nature is unable to sufficiently address all interesting and relevant questions. It will thus focus on some issues arising from the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (ECHR) and its protocols. More specifically, the discussion will relate to the right not to be arbitrarily expelled, the right to liberty and security of person, and the right not to be subjected to the death penalty and an examination as to whether Bosnia and Herzegovina breached any of these rights in the process of rendering the Algerian six to US forces.

8.3.1 The Algerian six and the Right not to Be Arbitrarily Expelled

It is of particular importance for this question that, as explained above, not all members of the Algerian six had the same status in terms of their citizenship or

[17] This, however, is in contrast with the information provided in the Fact Sheet: Statues of Guantanamo Detainees in which it is stated that the United States is treating and will continue to treat all of the individuals detained at Guantanamo humanely and, *to the extent appropriate and consistent with military necessity* (italics added), in a manner consistent with the principles of the Third Geneva Convention of 1949. It is furthermore stated that the President has determined that the Geneva Convention applies to Taliban detainees, but not to al-Qaida detainees (White House, 2002). This was stressed even more strongly in the Statement by the Press Secretary on the Geneva Convention in 2003.

residence rights in Bosnia and Herzegovina on the critical days of 17 and 18 January 2002. Moreover, not even all those members who were citizens of Bosnia and Herzegovina can be regarded as equal as not all of them had initiated administrative proceedings to dispute the decision to revoke their citizenship in front of the Supreme Court. Therefore, in four cases,[18] the right not to be expelled was protected by article 3 of the fourth Protocol to the ECHR (Prohibition of expulsion of nationals) whereas in two,[19] the procedural safeguards required for their legal expulsion were those defined by article 1 of the seventh Protocol to the ECHR (procedural safeguards relating to the expulsion of aliens).

As stated above, the Ministry of the Interior of the Federation of Bosnia and Herzegovina revoked the citizenship of five men on 16 November 2001 and that decision was immediately confirmed by the Ministry of Civil Affairs of Bosnia and Herzegovina. The decision was based on article 30.2 of the Law on Citizenship of Bosnia and Herzegovina in connection with article 23 of that law, as well as on article 28.3 in connection with article 24 of the Law on Citizenship of Federation of Bosnia and Herzegovina. According to these provisions, citizenship of Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina are to be revoked if it was obtained based on fraud, false information, or by hiding any relevant fact. In this case, the Ministry of the Interior argued that the suspects had hidden their intention to violate the laws and the Constitution of the Federation of Bosnia and Herzegovina.

However, although the HRC did not take a clear stand on this issue when discussing it in October 2002, because of the conflicting laws of the Federation of Bosnia and Herzegovina and Bosnia and Herzegovina, in the Ait Idir case (HRC, Decision II: Paras 99–101), the Supreme Court decided that the purported hiding of an intent to commit a crime could not be considered as "fraud, false information or the hiding any relevant fact" in accordance with the laws on citizenship. A court ruling on 19 December 2002 confirmed this view in revoking the procedural decision to annul the suspects' citizenship as it was based on reasons that violated the presumption of innocence as protected by article 6.2 of the ECHR. It furthermore ruled that the decision is effective *ex tunc*, meaning that the suspects never lost their citizenship of Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina and are, therefore, also to be considered as nationals of Bosnia and Herzegovina at the time of expulsion.

Bearing in mind that article 3 of the fourth Protocol prescribes that no one shall be expelled, by means of either individual or a collective measure, from the territory of the State of which he or she is a national, there can be no doubt that Bosnia and Herzegovina, in handing over its citizens to US forces, violated the right of its citizens not to be expelled.

---

[18] Boudella, Lakhdar, Nechle, Idir who all challenged the decision their citizenship be revoked.

[19] Bensayah, who did not challenge the decision that his citizenship be revoked and Lahmar who only had a permanent residence permit which was revoked.

As far as Bensayah and Lahmar are concerned they cannot be considered to have been nationals of Bosnia and Herzegovina at the time of expulsion. Thus, their right not to be expelled from the country was not regulated by article 3 of the fourth Protocol but rather by article 1 of the seventh Protocol. This article provides for the expulsion of an alien lawfully resident in the territory of a state only in pursuance of a decision reached in accordance with the law. Therefore, the main issue in these two cases is whether the decisions to hand over Bensayah and Lahmar were in accordance with domestic law.

In relation to Bensayah, the former citizen of Bosnia and Herzegovina, article 36 of the Law on Immigration and Asylum of Bosnia and Herzegovina is the relevant provision. This article prescribes that decisions on expulsion are to be taken by the Ministry of Civil Affairs and Communications of Bosnia and Herzegovina. From the facts of the case presented above, it is clear that, although the competent Federal Ministry of the Interior requested that the Ministry of Civil Affairs and Communications issue such a decision, the latter never did so. Therefore, and in spite of the fact that the Federal Ministry of the Interior issued an order that Bensayah was to leave Bosnian and Herzegovinan territory immediately,[20] the absence of an appropriate decision by the competent administrative body leads to a finding that his expulsion was not in accordance with domestic law and thus that his rights, as protected by article 1 of the seventh Protocol, were violated by the authorities of Bosnia and Herzegovina.

Lahmar's permanent residence permit was revoked by the Ministry of Human Rights and Refugees, and he was banned from entering the country for a period of 10 years. He appealed against this decision on 11 January 2002 and at the time of his expulsion, this procedure was still pending. Bearing in mind that, according to article 38.3 of the Law on Immigration and Asylum of Bosnia and Herzegovina, such an appeal has a suspensive effect, the HRC concluded (Decision I: Paras 204–5) that Lahmar's expulsion was not in accordance with domestic law. In other words, article 1 of the seventh Protocol defines a right not to be expelled under such circumstances, and in his case, this right was violated by the authorities of Bosnia and Herzegovina.

8.3.2 The Algerian six and the Right to Liberty and Security of Persons

Because of the complexity of the case, the UNOHCHR suggested (2002, Brief: 7) that the right to liberty and security of persons could be discussed in relation to three periods of detention: (a) the first period of detention from the date of original

[20] The HRC found that the expulsion of Bensayah based on this particular decision of the Federal Ministry of the Interior is "not in accordance with the law" because it was delivered to Bensayah after he was handed over, so he could in fact not exercise his right to appeal. Moreover, the decision itself misleadingly instructed Bensayah that he had no right to appeal against it although the relevant domestic law foresees such a right (*see* HRC, Decision III: Para 125).

arrest to the decision of the Supreme Court ordering release on 17 January; (b) the second period of detention from the decision of the Supreme Court on 17 January concerning the applicants' hand-over to US forces at approximately 6:00 a.m. on 18 January; and (c) the third period of detention beginning with this hand-over and lasting until their subsequent removal from the jurisdiction by the USA. As the HRC decided (2002, Decision I: Paras 207–14; 2003, Decision II: Paras 103–10; 2003, Decision III: Paras 135–40) that the first period of detention was in accordance with the law, it is only the remaining two that will be briefly considered here.

The Supreme Court's order that the Algerian six to be immediately released from detention was delivered to the detention unit on 17 January 2007 at approximately 5 p.m. Not only were they released immediately (they left the detention unit at 11:45 p.m.) on the prison authorities' receipt of the order, they were also immediately taken into custody by the police of the Federation on Bosnia and Herzegovina and remained in their custody until 6:30 a.m. the next morning when they were handed over to US forces. In its deliberation concerning this time period of more than 13 h, the HRC recalled (2002, Decision I, Para 219) the case of Quinn v. France (Eur. Court HR, judgement of 22 March 1995, Series A no. 311) and argued that although a certain delay in the execution of the order might be acceptable, the time elapsing between 5:00 p.m. and 11:45 p.m. can by no means be interpreted as conforming with an order to release "immediately," and the court thus held that the men were held in detention contrary to article 5.1(c) of the ECHR.

When discussing the detention period between 11:45 p.m. and 6:30 a.m. the next day, the HRC recalled that, in accordance with article 5.1(f) of the ECHR, a person can be deprived of liberty in case of a lawful arrest or detention and when the action is being taken with a view to deportation or extradition. In the case under consideration here, however, detention could not be considered lawful after the Supreme Court's order to release the men immediately as no new detention order had been issued. Additionally, the men were not informed of the reason for their new detention and they were not provided with the opportunity to challenge the decision that they be detained (see HRC 2002 Decision I: Paras 223–5; 2003, Decision II: Paras 117–20; 2003, Decision III: Paras 159–62). Simultaneously as representatives of Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina have since admitted, the exchange between authorities administering custody was a mere handing over and not an extradition. The diplomatic note sent to Bosnia and Herzegovina by the US authorities proves this fact beyond any doubt; it can be viewed as anything but a proper extradition request.[21]

With all this in mind, there can be no denying that the Algerian six's detention in the period after the delivery of the Supreme Court's order that the men to be

[21]Appropriate legal procedure in cases of extradition was defined by Chapter XXXI "Extradition of persons who have been charged or convicted" of the Criminal Procedure Code of the Federation of Bosnia and Herzegovina.

released and up until their handover is contrary to domestic law and in violation of the rights prescribed by article 5.1 of the ECHR.

Furthermore, the right to liberty and personal security was given consideration in the Bensayah case. Because he was under criminal investigation since 8 October 2001 for allegedly committing a criminal offence of certifying an untrue matter, his detention was initially based on an order of the municipal court of Zenica. However, as he was considered to be one of the Algerian six, the investigative judge of the Supreme Court ordered one month detention on 25 October 2001, which was supposed to start running from the day of the termination of the detention ordered by the municipal court of Zenica (*see* HRC 2003 Decision III: Para 33). As the municipal court of Zenica ordered Bensayah to be released on 16 January 2002, and since he was immediately transferred to the detention unit in Sarajevo rather than being released the question remains whether his right to liberty was violated in the period between the Zenica municipal court's order to release him (16 January 2002) and the Supreme Court order that he be released (17 January 2002). In other words, the validity of the detention order issued by the investigative judge of the Supreme Court was challenged.

In discussing this issue the HRC discussed (*see* HRC 2003 Decision III: Para 146) article 5 of the ECHR according to which, in the light of the presumption of innocence, pre-trial detention, as an exception to the right to liberty, must be used as restrictively as possible. The court also argued that this article obliges the authorities ordering pre-trial detention to examine, at regular intervals, whether the reasons for detention are still existent or not. Leaving to one side the fact that the Criminal Procedure Code of the Federation of Bosnia and Herzegovina does not prescribe even the possibility of pre-trial detention of a person within criminal investigation beginning first when the pre-trial detention of that person ends in another criminal investigation, the HRC argued that, even if he was empowered to issue such an order, the investigative judge could not have known on 25 October 2001 whether the reasons justifying pre-trial detention of Bensayah would be present at some point in the future (when the pre-trial detention order of the municipal court of Zenica came to an end), that is he was not in a position to have assessed the danger that Bensayah would destroy evidence, commit a crime, or to which extent he would then represent a danger to the public (*see* HRC 2003 Decision III: Para 148–50). Therefore, the HRC concludes that Bensayah's detention between 16 and 17 January 2002 was not in accordance with the requirements prescribed by article 5 of the ECHR, and therewith his right to liberty was violated in that specific period.

In relation to the third detention period, the right to liberty was found to be guaranteed by article 1 of the ECHR which prescribes that the High Contracting Parties shall secure the rights and freedoms defined within section I of the ECHR for everyone within their jurisdiction. This, according to the HRC (*see* HRC 2002 Decision I: Paras 231–7;2003, Decision II: Paras 126–32; 2003, Decision III: Paras 167–73), implies that before handing over the Algerian six, Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina were obliged to obtain and examine the legal basis of US forces' custody of the men. As the authorities did not ask for nor receive any information related to the grounds of detention, the handover of the

men into the illegal custody of US forces, this constituted a violation of their right to liberty as prescribed by article 5.1 ECHR.

8.3.3 The Algerian six and the Right not to Be Subjected to the Death Penalty

Article 1 of the sixth Protocol to the ECHR prescribes that the death penalty shall be abolished and that no one shall be condemned to such penalty or executed. As neither Bosnia and Herzegovina nor the Federation of Bosnia and Herzegovina sought any assurance that the Algerian six would not be condemned to such a penalty or executed, the question whether they were at risk of being so arose in this case.

In discussing this issue the HRC was of the opinion (HRC 2002 Decision I: Para 279; 2003, Decision II: Paras 147–8; 2003, Decision III: Paras 193–4) that, if brought to court, the men would be tried either for the violation of the laws of war or for the violation of federal US law. In case they were tried for violation of the laws of war, they could be sentenced to the death penalty if the procedure were to take place before US military commissions, provided that the military commission finds the offence they were involved in to be serious. Should they, however, be tried under US federal law, the death penalty could be imposed if they were found guilty of conspiracy to wage a terrorist war against the US, resulting inter alia in the 9/11 attacks.

The likeliness of the latter scenario was increased by the fact that Bensayah was allegedly found in possession of the telephone number of a senior liaison officer of Osama bin Laden. However, because of the fact that the Algerian six were transferred to the X-Ray Camp in Guantanamo Bay, it seems more plausible to assume that they will not stand trial before regular US courts but rather before a military commission in accordance with the Military Order of the President of the USA of 13 November 2001 and the Order of the US Secretary of Defence of 21 March 2002. As a result, bearing in mind that these two documents are defining criminal proceedings in such a way that rights, such as the right to trial within a reasonable time period, to a public hearing, to equality of arms, and to counsel of ones own choosing, are severely curtailed, the risk of them being sentenced to the death penalty is significant. Even more so because in this case they would be treated (as was confirmed by the letter of the US Ambassador in Bosnia and Herzegovina to the family members of the Algerian six, *see above*) as enemy combatants, in which case the provisions and the safeguards provided by the Third Geneva Convention from 1949 would not be applicable to them.

The HRC, therefore, concluded (HRC 2002 Decision I: Para 300; 2003, Decision II: Para 153; 2003, Decision III: Para 199) that the uncertainty as to whether, when, and under what circumstances the men would be put on trial and what punishment they might face at the trial's end gave rise to an obligation on the part of Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina to seek assurances that the death penalty would not be imposed. Having failed to do so, the HRC concluded that both Bosnia and Herzegovina

and the Federation of Bosnia and Herzegovina violated article 1 of the sixth Protocol to the ECHR.

8.4 Concluding Remarks

Judging by the time line of the proceedings as well as the time of the handover and the transfer to Guantanamo, it seems that the Algerian six were amongst the very first detainees to arrive at this location.[22] It is therefore of no surprise that five of them (all but Belkacem Bensayah) were released from Guantanamo at the end of 2008.[23] The brief overview of the facts of the rendition proceedings presented here, as well as the views of the HRC presented in relation to the violation of some basic human rights and fundamental freedoms in the so-called "Algerian six" case have clearly demonstrated that both Bosnia and Herzegovina and the Federation of Bosnia and Herzegovina failed to comply with the highest human rights standards as prescribed by international law and embedded in domestic law. Thus, those entities violated guaranteed human rights and fundamental freedoms. Moreover, in doing so, they failed to comply with the Constitution of Bosnia and Herzegovina which obliges them (Dayton Agreement, Annex 4, Article 2.1) to ensure the highest level of internationally recognised human rights and fundamental freedoms.[24] They, as well as the US authorities, furthermore disrespected the legal decisions of the Supreme Court and the Human Rights Chamber and in consequence undermined the rule of law in Bosnia and Herzegovina.

The need to fight terrorism as a legitimate one is not denied in any way. It is as such confirmed in the numerous international legal documents defined on all levels of international and intergovernmental co-operation. Nevertheless, it is not only possible but also necessary[25] to fight terrorism while respecting standards dictated by human rights, the rule of law, and, where applicable, international humanitarian law. This necessity, which would have to be observed in fully formalised legal forms of international co-operation, such as extradition procedures are, would have to be even more meticulously observed in other, less formalised forms of diplomatic co-operation, such as this one between US and Bosnia and Herzegovina was. Bearing in mind that the authorities in Bosnia and Herzegovina managed to breach all three sets of standards mentioned above, the author can

[22] The first group of Al Qaeda and Taliban detainees arrived at the U.S. Navy Base at Guantanamo Bay on 11 January 2002. *See* Borelli, 2004.

[23] Mustafa Ait Idir, Mohamed Nechle i Hadj Boudellaa arrived back to Sarajevo on December 16 2008.

[24] Compare the Decision of the European Court of Human Rights in *Boumediene and others against Bosnia and Herzegovina* from November 18 2008. The applications of the "Algerian six" were found inadmissible.

[25] See the preamble of the Guidelines on Human Rights and the Fight Against Terrorism (2002).

only be of the opinion that the rendition practice used in the case of the Algerian six in which the latter were treated as suspected terrorists went well beyond any acceptable boundary and cannot be seen as anything but a betrayal of the promise of citizenship of the worst kind.

References

Amnesty International (2002). *Bosnia-Herzegovina: Transfer of six Algerians to US custody puts them at risk. Amnesty International*: AI Index: EUR 63/001/2002.

Amnesty International (2006). Partners in Crime: *Europe's Role in US Renditions*. *Am*nesty International.

Borelli, S. (2004). The Treatment of Terrorist Suspects Captured Abroad: Human Rights and Humanitarian Law. In Bianchi, A. (ed). *Enforcing International Law Norms Against Terrorism.* pp. 39–61. Oregon: Hart Publishing.

Committee on Legal Affairs and Human Rights (CLAHR). (2006). *Alleged secret detentions and unlawful inter-state transfers involving Council of Europe member states: Draft Report – Part II (Explanatory Memorandum)*. Council of Europe.

Convention for the Protection of Human Rights and Fundamental Freedoms. ETS No. 005. Retrieved 29.10.2007 from http://conventions.coe.int/Treaty/EN/Treaties/Html/005.htm.

Council of Europe, Guidelines on Human Rights and the Fight Against Terrorism (2002). Retrieved 31.10.2007 from http://www.coe.int/t/e/legal_affairs/legal_co-operation/public_international_law/texts_&_documents/2002/H_2002_4E.pdf

Criminal Code of the Federation of Bosnia and Herzegovina. *Official Gazette of the Federation of Bosnia and Herzegovina.* No. 43/98; 29/00.

Criminal Procedure Code of the Federation of Bosnia and Herzegovina. *Official Gazette of the Federation of Bosnia and Herzegovina*. No. 43/98; 23/99.

Department of Defense. Military Commission Order No. 1 from 21 March 2002 (2002). Retrieved 31.10.2007, from http://www.legislationline.org/legislation.php?less=false&lid=4125&tid=46

Deren inovi , D. and Becker, S. (2008) International terrorism: the future unchained? Zagreb: Faculty of Law, University of Zagreb.

European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) (2007). *17th General Report on the CPT's activities covering the period 1 August 2006 to 31 July 2007*. Strasbourg: Council of Europe.

European Court of Human Rights (2008). The Decision in *Boumediene and others against Bosnia and Herzegovina* from 18 November 2008.

White House (2002). *Fact Sheet: Status of Detainees at Guantanamo*. Retrieved 29.10.2007. from http://www.whitehouse.gov/news/releases/2002/02/20020207–13.html

Fisher A. & Satterthwaite M. (2005). *Beyond Guantanamo: Transfer to Torture One Year after Rasul v. Bush*. New York: The Center for Human Rights and Global Justice.

Human Rights Chamber of Bosnia and Herzegovina (2002) (HRC, Decision I). Decision on admissibility and merits (11 October 2002) Cases nos. CH/02/8679, CH/02/8689, CH/02/8690, and CH/02/8691.

Human Rights Chamber of Bosnia and Herzegovina (2003) (HRC, Decision II). Decision on admissibility and merits (4 April 2003) Case no. CH/02/8961.

Human Rights Chamber of Bosnia and Herzegovina (2003) (HRC, Decision III). Decision on admissibility and merits (4 April 2003) Case no. CH/02/9499.

Supreme Court of the United States (2008). Opinion of the Court in *Lakhdar Boumediene et al. V. Bush, President of the United States et al. and Khaled A. F. Al Odah, next friend of Fawzikhalid Abdullah Fahad Al Odah et al. v. United States et al.*, 12 June 2008.

Marty, D. (2006). Alleged secret detentions and unlawful inter-state transfers involving Council of Europe member states: Draft report – Part II (Explanatory memorandum). Council of Europe. Retrieved 29.10.2007 from http://assembly.coe.int/CommitteeDocs/2006/20060606_Ejdoc162006PartII-FINAL.pdf

Oleskey, S. H. (2006). *Memorandum to the Temporary Committee on the Transportation and Illegal Detention of Prisoners of the European Parliament: Rendition of Six Bosnian Citizens and Former Residents to Guantanamo Bay*. Retrieved 29.10.2007 from http://www.statewatch.org/cia/documents/oleskey-memorandum-25–04–06.pdf.

Presidents Military Order: *Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism from November 13th 2001* (2001). Retrieved 31.10.2007 from http://www.whitehouse.gov/news/releases/2001/11/20011113–27.html

Protocol No. 4 to the Convention for the Protection of Human Rights and Fundamental Freedoms, securing certain rights and freedoms other than those already included in the ECHR and the Protocol No. 1 thereto as amended by the Protocol No. 11 (ETS no. 155). ETS no. 046. Retrieved 29.10.2007 from http://conventions.coe.int/Treaty/EN/Treaties/Html/046.htm

Protocol No. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms as amended by the Protocol No. 11 (ETS no. 155). ETS No. 117. Retrieved 29.10.2007 from http://conventions.coe.int/Treaty/EN/Treaties/Html/117.htm

Skuletic, S. (23 August 2007). BiH trazi povratak "alzirkse grupe." Dnevni Avaz: Online izdanje. Retrieved 23.08.2007 from http://www.avaz.ba

Statement by the Press Secretary on the Geneva Convention (2003). Retrieved 29.10.2007 from http://www.whitehouse.gov/news/releases/2003/05/20030507–18.html

Temporary Committee (of the European Parliament) on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners (TCEP) (2006). *INTERIM REPORT on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners.*

The Law on Citizenship of Bosnia and Herzegovina. *Official gazette of Bosnia and Herzegovina. No. 13/99.*

The Law on Citizenship of the Federation of Bosnia and Herzegovina. *Official gazette of the Federation of Bosnia and Herzegovina. No. 43/01.*

The Law on Immigration and Asylum of Bosnia and Herzegovina. *Official gazette of Bosnia and Herzegovina. No. 23/99.*

United Nations Office of the High Commissioner for Human Rights (Field Operation in Bosnia and Herzegovina) (2002) (UNOHCHR, Brief). OHCHR Submission to the Bosnia and Herzegovina Human Rights Chamber Re: Cases nos. CH/02/8679, CH/02/8689, CH/02/8690, and CH/02/8691. Unpublished.

US Congress (2001). H.J. Res. 64: Authorization for Use of Military Force. Retrieved 29.10.2007 from http://www.fas.org/irp/threat/useofforce.htm

Chapter 9
Terrorist Attacks: Criminal Prosecution or National Defence?[1]

Wolfgang Hetzer

9.1 Introduction

The USA considers itself to be at war. The Commander-in-Chief of the US Armed Forces, President George W. Bush, has declared war on international terror and time and again publicly described himself as a "wartime president." In so doing, he is continuing a tradition started by his country in connection with a different form of criminality. For many years, the USA has also seen itself as being at war with the illegal drugs trade. The "war on drugs" is also being fought on an extremely complex and dangerous battlefield. It is obvious that the planning and waging of this war has not yet achieved the desired success. A "peace treaty" with internationally operating drug traffickers is not in sight.

The American public and their political leaders believe the terrorist attacks on the USA in September 2001 to be attacks on the territorial integrity of their country, with predictable consequences. The magnitude of the attacks, the number of lives lost, the huge damage to property and above all the unique symbolism of the attacks on the World Trade Center in New York City all demanded a unique response. The whole world, and not only the USA, was in a state of shock, but even once this had passed no-one could imagine that the perpetrators, accomplices and instigators of this totally exceptional crime could be called to account simply by the opening of conventional investigation proceedings. Previous findings demonstrated at an early stage that these attacks could not have been carried out without the various kinds of political and logistical support which are typically provided by certain countries. Against this backdrop, the reaction of the civilised world and the military action

W. Hetzer (✉)
Head of Unit "Intelligence: Strategic Assessment & Analysis"
European Anti-Fraud Office (OLAF)
Brussels. OLAF, Rue Joseph II, 30, Office 03/109, 1000 Brussels/Belgium
e-mail: Wolfgang.HETZER@ec.europa.eu

[1] Originally published by Springer Science+Business Media in the *European Journal on Criminal Policy and Research* 13:1–2 (April 2007), pp. 33–55.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_9, © Springer Science+Business Media, LLC 2010

undertaken in particular against Afghanistan by the USA and their allies were in many ways both plausible and justifiable under international law. It is obvious that a sovereign state which does not merely tolerate terrorist activities, but also actively encourages them, will harbour certain structures on its territory which cannot be neutralised with the means available to traditional police law. Even with the benefit of hindsight, one can hardly deny that the politics of the Taliban in Afghanistan had created a military situation which could not be tackled without the deployment of armed forces. It was possible to do this in accordance with the principles of the United Nations Charter in order to counter further international risks to various types of objects of legal protection. The attack on Iraq by the armies of the USA and some of their allies is presumably different. Therefore in comparison as to Afghanistan, there are certain factual and legal features which need to be debated both in connection with the waging of the war against Iraq and with the basic principle as to whether war is always justifiable in the fight against international terror.

Every battle-scarred warrior knows that the rules of engagement evaporate when the first shots are exchanged. Once the firing begins, the instructions for deployment lose their guiding function, however carefully they have been worked out. Furthermore, the deployment of military resources does not follow the principles of proportionality which are enshrined in police law. Time and again, war leads to violence taking on a life of its own and, if the worst comes to the worst, this can end in institutionalised cruelty. The political and psychological damage done by the photographs of torture in Abu Ghraib is nigh on incalculable. Even the US Army's Commander-in-Chief, George W. Bush, recently described the happenings there as the "biggest mistake" (so far). If the numerous allegations of unlawful activities on the part of the American Army and other US security services should prove to be true (these include kidnappings and the running of secret prisons), this will considerably jeopardise the success of the much-needed fight against international terrorism. Additionally and above all, the fundamental question arises as to whether waging war can be a suitable instrument in the prevention of crimes motivated by terror and in the punishment of the perpetrators and their accomplices. It will not be possible to answer this question exhaustively in the context of this paper. At best, it will enable us to get closer to the heart of the problem, whereby the author has also been prompted by recent discussions on security policy in the field of certain legislative projects in the Federal Republic of Germany.

A debate has broken out in connection with the passing of an act of parliament to amend air safety and security regulations, the Aviation Security Act (LuftSiG),[2] and the relevant judgment handed down by the German Federal Constitutional Court.[3] The question being debated is whether, and to what extent, the armed forces of the

[2]German Federal Law Gazette I, 78.

[3]Federal Constitutional Court, judgment of 15.2.2006 – 1 BvR 357/05, in: 59 *Neue Juristische Wochenschrift* (2006) pp. 751–761. cf. W.-R. Schenke, Die Verfassungswidrigkeit des § 14 III LuftSiG, 59 *Neue Juristische Wochenschrift* (2006) pp. 736–739 and an early commentary by A. Meyer, Wirksamer Schutz des Luftverkehrs durch ein Lufsicherheitsgesetz?, 37 *Zeitschrift für Rechtspolitik* (2004) pp. 203–207.

Federal Republic of Germany are supposed (or allowed) to play a part in repulsing terrorist-inspired attacks. The basic problem of where the German Federal Armed Forces stand in security structures is raised by the question as to whether direct use of arms is allowed against an aircraft which has been skyjacked and which, together with its passengers, is to be misused for the purpose of a criminal attack, a question which also touches on detailed requirements under constitutional law. The situation is made more complicated by the fact that any answers to these questions and any solutions proposed must take into account security policies within the context of the European Union and the European Union's attempts to fight international crimes of violence in which terror is the motive.[4] At the same time, German leaders seem increasingly eager to (re-)present themselves to their American counterparts as reliable allies.

9.2 Averting Danger or State of Defence?

Terrorist attacks are carried out by criminals. Terrorists are therefore (suspected) criminals. If one were to attempt to dignify their mass murders by calling them attacks of war, which is a line currently taken by several political groupings, one would either be demonstrating a disturbing degree of ignorance of the law or ambitions which, if anything, can only be explained with reference to psychology. Apparently, Germany too is suffering from amnesia as to what war really is. It is not only in grey areas that the intended militarisation of domestic security policy leads to competition between constitutional limitations and the rationality of war. The principle of proportionality also comes under pressure from the destructiveness, which is the *raison d'être* of military action. It is obvious that a soldier's psychology is not determined by thoughts of rehabilitating his opposite number, but by his wish to put his enemy out of action. Sooner or later, military deployment always tends to become disproportionate. Innocent people are killed as part of isolated acts of revenge which can no longer be integrated into tactics. Furthermore, soldiers who have to move around in the confusing situation of a civil war are regularly tempted to resort to cruel repression to compensate for their lack of opportunity for orthodox military action. Evidence of this kind is now coming out of Iraq too. Even present-day military alliances do not exclusively and convincingly boil down to fighting modern terrorism in its allegedly warlike manifestations, but are of course also pursuing a more or less successfully hidden agenda. Needless to say, exporting freedom and democracy to every corner of the earth, as proclaimed by the USA in particular, is not only part of a preventive strategy against murderous terrorist attacks. It is also a matter of implementing a parallel political programme determined to a significant degree by geostrategic interests. The most important motives for deploying troops worldwide

[4]Fundamentally: J. Hecker, Die Europäisierung der inneren Sicherheit, 59 *Die Öffentliche Verwaltung* (2006) pp. 273–280. On details of these attempts: W. Hetzer, Europa gegen Terror, 36 *der kriminalist* (2004) pp. 332–339.

include the establishment and maintenance of supplies in the area of primary sector energy reserves. Fundamentalist Islamist terror is of course particularly well suited to providing an oversimplified and thus publicly effective justification for already existing or planned military policy alliances. There is a danger that the neat phrase "Germany's national security is being defended in the Hindukush" will degenerate into a useful camouflage for a security policy which is not merely directed at the questionable continuation of an outdated energy policy, but also at the restoration of a particular kind of ability to achieve satisfaction. Within the context of a re-defined German foreign policy, it may be possible to marshal facts to justify all of this and give it a legitimacy based on democratic processes. However, nothing will alter the fact that "a terrorist is a criminal is a criminal." A brief look at our traditional penal code should also convince those who bear political responsibility that there is no lack of regulations on requirements for deploying the federal armed forces in Germany either. Numerous pieces of legislation have been added in the past few years. Whole "catalogues" and "packages" have been produced, leading to security policy "re-armament," which is evidence not only of a greater or lesser degree of expertise, but also of almost warmongering and restless energy. If things go on like this, the constitutional state will degenerate into a *glacis* built up in front of a battlefield manned by young men and women who have been led on to it to deal with problems whose origin and magnitude they do not comprehend, and which they are unable to solve.[5]

Seen against this backdrop, it is not particularly surprising that in the heart of Europe, viz. in the Federal Republic of Germany, the debate on national security has not only been marred by a change in tone but by several disturbing leaps in the quality of the discussion.

For some considerable time now, the Federal Minister of the Interior in the Federal Republic of Germany, Wolfgang Schäuble, has been attempting to answer the question as to what is the currently valid meaning of "defence" within the Constitution. It seems to him that clarification is required as to whether the concept of defence needs redefining. Mr. Schäuble feels this is the vreal question" in the face of the completely new situation which has been threatening us since 9 November 1989 or 11 September 2001. The Minister is concerned that this new threatening situation be brought sensibly into line with the concept of defence as laid down in the Constitution. He says states no longer have a "monopoly" on waging war, referring not only to al-Qaeda but also to warlords who bring war to the world. Mr. Schäuble stresses the fact that defence by military means must also be allowed in the case of attacks which are in substance warlike, even if they are not led by the troops of a state. In this connection, we are

[5] Greater detail in the following articles by W. Hetzer, Terrorabwehr im Rechtsstaat, 38 *Zeitschrift für Rechtspolitik* (2005) pp. 132–135; W. Hetzer, Terrorismusbekämpfung zwischen Risikosteuerung und Rechtsgüterschutz), 88 *Monatsschzeitschrift für Kriminologie und Strafrechtsreform* (2005), pp. 111–126; W. Hetzer, Die Flucht des Gesetzgebers in die polizeirechtliche Prävention, 10 *Strafverteidiger Forum* (2005) pp. 318–324; W. Hetzer, Verschleppung und Folter, 60 *Kriminalistik* (2006) pp.148–159; W. Hetzer, Ist Freiheit durch Sicherheit korrumpierbar?, 11 *Strafverteidiger Forum* (2006) pp. 112–118.

reminded of regulations in the Constitution which allow the federal armed forces to act against armed groups of insurgents in the case of national emergencies. The Minister is reluctant to allow "defence" to be interpreted as an open constitutional concept, believing that an explicit amendment to the Constitution will be unavoidable. Referring to the Federal Constitutional Court's judgment which found that it would be unconstitutional to authorise the federal armed forces to shoot down a highjacked aircraft, Mr. Schäuble also says where he stands on the question of whether it is permissible to treat the passengers in a highjacked aeroplane as "things," and whether the lives of the persons in the aeroplane can be offset against the lives of others who are at risk. As long as we are on police territory when averting danger, the Minister is also willing to prohibit the corresponding offsetting of one life against another, but at the same time he stresses, "I cannot airbrush the new risks."

He feels that politics is under an obligation to work out a new path, and says that the prohibition of the offsetting of one life against another as described above is not part of the valid laws and customs of war. In the latter case, the principle of proportionality applies. Mr. Schäuble would like to see the German debate on international law and regulations under international law linked to the constitutional debate. He is convinced that it must be permissible to offset one life against another in the case of a defensive emergency. For him, this is not a case of some kind of martial law, but of defence. The Minister is particularly troubled by the Federal Constitutional Court's use of the expression "warlike" rather than "defensive emergency" in the judgment on the Aviation Security Act. For this reason, Mr. Schäuble recommends that in its judgments the Court should stick to the terminology of the Constitution. He believes that its decision has created "a certain transitional problem."[6]

The Minister of the Interior's argument is particularly impressive when viewed against the backdrop of German history. The public debate, which has only been going on for a short time, has revived memories of the devastating consequences which arose in connection with the deployment of German troops on the home front. Demands that soldiers should take over policing duties on the home front is seen as the product of a new security philosophy which would seem to be necessary in times of terror, as well as the simple desire to stop the gaps in the depleted police force which have come about through forced austerity measures. Some commentators do not think much of this philosophy. They deny vehemently that soldiers make the better police officers, which is not a criticism of the soldiers, as they are neither trained nor equipped for police duty, but they are against giving soldiers duties which are not theirs. They rightly stress that the proportionality of means is a characteristic of the police, whereas force is only a last resort. However, victory or defeat, the fight to incapacitate or even the annihilation of the enemy, all this is characteristic of the military. This does not mean that there are no *a priori* limits to military force, but it is almost by nature more destructive. The deployment of the German military on the home front in the 19th and 20th centuries provides impressive examples of a singularly destructive and brutal nature, which foreshadow the later breach in civilisation

[6] W. Schäuble, *Süddeutsche Zeitung* no. 45 of 23. 2. 2006, p. 11.

during the Third Reich. It was obvious, even at the time of the Weimar Republic, that the armed forces of the Reich and the paramilitary volunteer corps were consumed with hatred for democracy. The soldiers provided peace and quiet, but in their own way. They waged war on the enemy within. In the end, Weimar democracy gave in without a fight because it could never have won the fight against its own military. Public commentators point out that in Germany there is a long tradition of deploying the military on the home front. "This tradition is both bloody and dishonourable."[7] This was still etched on the memory of the authors of the Constitution when they forbade any deployment of armed military on the domestic front. It is obvious that the federal armed forces themselves are in no way eager to be active in establishing public order or cracking down with an iron fist. For the first time in its history, Germany has a military force which does not consider itself to be a state within a state, and which does not draw its legitimacy from its own allegedly higher law. This achievement cannot be valued too highly. It must not be wantonly jeopardised by turning soldiers into the German equivalent of special constables.[8]

Meanwhile, Mr. Schäuble officially admits that, following the clear-cut judgment handed down by the Federal Constitutional Court, the proposed new regulations to prevent terrorist attacks in the Aviation Security Act lack any basis under constitutional law. He is therefore determined to create such a basis. In the case of an air attack with a passenger plane like the one on 11 September 2001, he says the armed forces have to be able to intervene. In his opinion, it must be possible to regulate this. In this context, he believes that one ought to look more closely at the term "defence" and reflect on present-day threats. The Minister is also aware of the Federal Constitutional Court's finding that the order to shoot down a plane in a non-defensive situation is under no circumstances legal. He points out that the court avoided saying this where it was a case of defence, which is the (decisive) point as far as he is concerned. He says the world has changed and New York has proved that the difference between domestic security and security from outside attack has become obsolete.[9]

The agreement between the CDU (Christian Democratic Union), CSU (Christian Social Union) and SPD (German Social-democratic Party) coalition parties: "Together for Germany. With courage and humanity" (Coalition Agreement) formulates the political aims for the current legislative period in Germany. It also assumes that the terrorist attacks in various countries of the world have given rise to a threat which has taken on a new dimension. The Agreement speaks of security from attack from outside the country and from within, but says the two are becoming more closely intertwined.[10] Nevertheless, it stands by the basic separation of police and military

[7] J. Käppner, *Süddeutsche Zeitung* no. 45 of 23. 2. 2006, p. 11.

[8] Correctly stated by J. Käppner, loc. cit.

[9] W. Schäuble, *Der Spiegel* no. 21 of 22. 5. 2006, p. 38.

[10] This is not a new perception. Previously and in greater detail by W. Hetzer, *Krieg und Kriminalität. Innere und äußere Sicherheit: Unterscheidung oder Verschmelzung?*), in J. Calließ, ed., *Die Verflochtenheit und Verflechtung von äußerer und innerer Sicherheit* (Rehburg-Loccum (2003) pp. 49–69.

duties and, with reference to the judgment of the Federal Constitutional Court on the Aviation Security Act, it announces that there will be an examination of the need for regulation under constitutional law.[11]

The Coalition Agreement recognises that the federal armed forces are an instrument in national and international security. It states that the future range of tasks facing the Coalition will be determined to a significant degree by developments in security policy. The German army, it says, is to serve in the prevention of international conflict and in overcoming crises, in supporting its allied partners, in defence of the country, in rescue and evacuation operations, partnership and co-operation, as well as by "rendering aid within the home country." According to the Agreement, the "core of the federal armed forces' constitutional assignment" is still "national defence," in addition to their participation in overcoming international conflict, and despite changes in conditions and missions. Furthermore, it is no longer possible to make a clear distinction between internal and external security, especially when one considers the lack of symmetry in the threat arising from terrorist activity. The Coalition goes on to give notice of Federal Government initiatives in case of need for legislation or constitutional regulation to deal with particular risks to German security. However, it is clear that for the coalition parties of the present Federal Government: "Our Federal Armed Forces are operational."[12]

9.3 A Policy on Crime or Armament?

Politics does not always begin by studying the real world. It often starts by defining terminology. It is therefore all the more important for us to remind ourselves of constitutional requirements. It is the lower house of the federal parliament (*Bundestag*) acting with the consent of the upper house (*Bundesrat*) which determines that federal territory is under attack "by armed force" or imminently threatened with such an attack ("state of defence"). A statement to this effect is issued on the application of the Federal Government and requires a two-thirds majority of the votes cast, including a majority of the members of the *Bundestag*.[13] If the situation imperatively calls for immediate action, and if insurmountable obstacles prevent the timely convening of the *Bundestag* or the *Bundestag* cannot muster a quorum, the Joint Committee makes this determination by a two-thirds majority of the votes cast, including at least a majority of its members.[14] If the federal territory is under attack by armed force, and if the competent federal authorities are not in a position at once to make the determination provided for in the first sentence of paragraph (1) of Article 115 of the Constitution, the determination is deemed to have been made and promulgated

[11] Coalition Agreement, p. 135.

[12] cf. all of: Coalition Agreement, pp., 153, 154.

[13] Article 115a(1) of the Constitution.

[14] Article 115a(2) of the Constitution.

at the time the attack began. These provisions were introduced into the German Constitution in 1968 to regulate the state of defence, and thus emergencies due to threats from external sources caused by (present or imminent) attacks on federal territory by agents from outside it. This is in contrast to internal emergencies which have their origins elsewhere. To avert an imminent danger to the existence or free democratic basic order of the Federation or of a *Land*, a *Land* may call on police forces of other *Länder*, or on personnel and facilities of other administrative authorities and of the Federal Border Police (re-named the "Federal Police").[15] However, Articles 115a to 115l of the Constitution do not directly regulate the conditions under which the armed forces can be sent into action, nor do they authorise restrictions to civil liberties.[16]

The Federation has established armed forces for purposes of defence.[17] Apart from defence, the armed forces may be employed only to the extent expressly permitted by the Constitution.[18] During a state of defence or a state of tension, the armed forces have the power to protect civilian property and to perform traffic control functions to the extent necessary to accomplish their defence mission. Furthermore, the armed forces may be authorised to support police measures for the protection of civilian property.[19] To avert an imminent danger to the existence or free democratic basic order of the Federation or a *Land*, under certain circumstances[20] and if the police forces (of the *Länder*) and those of the Federal Police prove inadequate, the Federal Government may employ the armed forces to support the police in protecting civilian property and in combating organised armed insurgents.[21]

"Employing the armed forces" means using them to engage in hostilities or other kinds of intervention with the means provided by military organisation. This means using them at home and abroad, thereby including measures provided for under Chapter VII of the UN Charter and "blue helmet missions" as well as military action in defence of German nationals abroad and in support of police searches on home territory.

The armed forces' duties are restricted as a matter of principle to defence in accordance with the general "peace clause." An attack has to come from beyond the national borders. The federal armed forces are not allowed to take on the duties of a police force of the air.[22]

---

[15] Article 91(1) of the Constitution.

[16] Article 115c(2) of the Constitution) is, however, an exception to this.

[17] First sentence of Article 87a (1) of the Constitution.

[18] Article 87a (2).

[19] Article 87a(3) of the Constitution.

[20] Article 91(2) of the Constitution.

[21] Article 87a(4) of the Constitution.

[22] H. D. Jarass/B. Pieroth, *Grundgesetz für die Bundesrepublik Deutschland*) (München 2006) Article 87a, point 9.

Defence comprises not only defence of the nation, but also that of the alliance partners pursuant to Article 5 of the North Atlantic Treaty, and individual or collective self-defence pursuant to Article 51 of the United Nations Charter.

The Constitution expressly permits employment of the armed forces under the third and fourth paragraphs of Article 87a and the second and third paragraphs of Article 35. However, these provisions only apply to operations on home territory. To respond to a grave accident or a natural disaster, the second sentence of Article 35(2) of the Constitution states that a *Land* may call for the assistance of police forces of other *Länder* or of personnel and facilities of other administrative authorities, of the armed forces or the Federal Border Police (Federal Police). The Constitution goes on to state[23] that if the natural disaster or accident endangers the territory of more than one *Land*, the Federal Government, insofar as is necessary to combat the danger, may instruct the governments of the *Länder* to place police forces at the disposal of other *Länder*, and may deploy units of the Federal Border Police (Federal Police) or the armed forces to support the police. Relevant measures taken by the Federal Government are to be rescinded at any time at the behest of the *Bundesrat*, and in any event as soon as the danger is removed.

We mentioned above that the Federal Constitutional Court recently had to pass judgment on whether, under existing German constitutional law, it is constitutional for authorisation to be given to the armed forces to use direct force of arms on an aircraft pursuant to section 14(3) of the Aviation Security Act. In the face of attacks on this particular ruling, the highest German Court first had to enlighten the German Government and the Federal Parliament, explaining that these constitutional bodies lacked the competence to legislate in this matter. From where the provision stands within the system, the Court concluded that this was not a case of safeguarding an autonomous function of the Federation, but one of assistance in carrying out a duty which rests with the *Länder* within the context of averting danger and supporting the *Länder* police forces. The Court was of the opinion that authorising an aircraft to be shot down was not a case of "defence." Even protection of the civilian population, which is included in the power to legislate on "defence" under Article 73(1) of the Constitution, is not relevant here. The provision which is under attack cannot be backed up by the competence of the Federation to legislate with respect to air transport either,[24] because in fact this article regulates support for the *Länder* in averting danger and the deployment of the armed forces in situations covered by the second sentence of Article 35(2) and Article 35(3) of the Constitution. It is true that these provisions may be invoked to determine the Federation's competence to regulate the detailed employment of its armed forces in collaboration with *Länder* involved in coping with a regional or supraregional emergency or disaster. Nevertheless, section 14(3) of the Aviation Security Act is not covered by this federal sphere of legislation because the provision is incompatible with the requirements under the Constitution which relate to constitutional matters regarding

[23] In Article 35(3).

[24] Article 73(6) of the Constitution.

the military. The Court stresses that an authoritative interpretation and application of Article 87a of the Constitution will aim to limit possible deployments of the federal armed forces on the home front by sticking to the law as is it written. The Court is of the opinion that this aim will also determine the interpretation and application of those regulations which specifically allow for the employment of troops for purposes other than defence.[25]

The Federal Constitutional Court is persuaded that authorising the armed forces to use direct force of arms on an aircraft is incompatible with the provisions of the Constitution cited above; it goes on to say that the second sentence of Article 35(2) of the Constitution rules out this kind of force of arms in the case of regional disasters or accidents. The Court says that section 14(3) of the Aviation Security Act does not keep within the framework of this Article of the Constitution, because it does not permit the armed forces to be employed in combat using arms of a specifically military nature in their fight against natural disasters and grave accidents. In their Aviation Security Act, the legislative bodies implied that the employment of troops to support *Länder* police forces in their prevention of a particularly serious accident was to be seen as assistance within the context of averting danger, insofar as this was necessary for effective combat. The Federal Constitutional Court assumes that an alignment with this function (within the sphere of competence of the *Länder* authorities responsible for averting danger) "necessarily" determines the nature of the resources which may be used by the armed forces when they are employed for the purpose of rendering assistance. Thus, the armed forces may use the same weapons as the police, but they may not employ military weapons (e.g., aircraft weapons on board a military plane). The Court arrives at this conclusion as a result of its reading of the wording, sense and intention of the second sentence of Article 35(2) of the Constitution, as well as from the history of the origins of the provision and its position within the whole system. All these things would suggest that the armed forces should be banned from using arms of a specifically military nature when they are on duty within the area of responsibility of the *Länder*.

The Court has also decided that authorising direct force of arms is incompatible with Article 35(3) of the Constitution, which relates to disasters and emergencies which cross-regional borders. One may have misgivings about constitutionality simply because the legal deployment of troops pursuant to section 14(3) of the Aviation Security Act is not in every case conditional on a decision having been previously taken by the Federal Government (on the basis of collective responsibility) pursuant to section 13(3) of the Aviation Security Act. In fact, the first sentence of Article 35(3) of the Constitution explicitly authorises the Federal Government alone to order the deployment of the armed forces in the case of supraregional disasters. In contrast, the second and third sentences of section 13(3) of the Aviation Security Act provide

[25] The Constitution regulations contained in sentence 2 of Article 35(2) and Article 35(3) forming the basis for the provisions under the Aviation Security Act which were designed to help combat serious incidents in the air and the attendant risks.

for a decision to be taken by the Federal Minister for Defence (or, should he require a proxy, his authorised representative from among the members of the Federal Government) in consultation with the Federal Minister of the Interior in those cases where it is not possible for the Federal Government to take a decision in time. Depending on the situation, the Federal Government will be replaced by a single minister who decides on the deployment of troops, not only in exceptional cases but routinely, where there is a disaster affecting two or more regions. The Federal Constitutional Court believes that this cannot be justified in view of the first sentence of Article 35(3) of the Constitution, not even if there is particular need for haste.

Furthermore, the Court stresses that the most important way in which the Act lies outside the constitutional legal framework of the first sentence of Article 35(3) of the Constitution and its relevance to the military is because the Constitution forbids the armed forces from using weapons of a typically military nature, even in coping with supraregional disasters. The very wording of the provision shows that the deployment of troops is only permissible "to support" the police forces of the *Länder*, thus this is again a case of carrying out the duty of a *Land*. The Court believes that the purpose of this regulation (the Federation is merely to give support to the *Länder*) excludes the use of arms of a typically military nature in the light of Article 87a(2) of the Constitution, even in the fight against disasters affecting two or more regions. This opinion is further supported by the history of the origin of the first sentence of Article 35(3) of the Constitution. In drawing up this provision (which was tantamount to amending the Constitution), the legislators saw no reason to regulate the employment of the armed forces and their resources in a way which deviated from the second sentence of Article 35(2). In fact, this is understandable when one considers that the content of the expressions "for the assistance" and "to support" is identical in the two paragraphs.

The German legislature has made some alarming attempts to deal with the risk of terrorist attacks. They demonstrate more than a lack of understanding of the particular character of the threat. One can see that an almost illusionary optimism is being pinned on the militarisation of security strategies, and this is linked to a considerable lack of sensitivity towards the demands of basic constitutional liberties. These are not the only reasons why it would seem appropriate to shed at least some light on the relationship between the intentions of criminals, the methods of terrorists and the ambitions of politicians. In addition, it is worthwhile shedding light on some of the particular attempts undertaken by the European Union to counteract the risk of attacks, not only on account of the cross-border global activity of terrorist groupings. After all, a number of serious attempts have been made at European level to make a list of analytical deficits in the recording of potential threats linked to modern terrorism. The cross-border nature of this intensive kind of criminality means that it will be indispensable for the Member States of the European Union to co-ordinate their activities. Finally, one might hope that future pieces of legislation and other measures will be drafted with increased sensitivity towards the rule of law, as political compromises will have to be made, and that the governments of certain individual Member States will accordingly tone down their efforts to take the centre-stage.

9.4 Enemy or Criminal?

We can observe a worrying easiness nowadays to categorise a situation as "war." The first half of the last century was marked by two terrible world wars. Later, there were also numerous all-too-visible cases of bloody fighting and minor wars involving states and other warring factions in many and various parts of the world. Nevertheless, for a long time there was more or less general agreement that the term "war" and the concept of war should be used sparingly. This could be seen as a sign that the old orders were dying and that no new ones had yet risen to take their place. The problems connected with the term "war" are presumably in equal measure a reflection of the turbulent situation in the world both then and now. The history of international law was in any case seen as a history of the term "war." This was the time when international law was considered to be the law of war and peace. This would remain the case as long as it was part of the law of independent peoples within organised states, and if war was waged between independent states and was not an international civil war. Indeed, this is a problem which crops up in connection with the breakup of every old order and the start of every new relationship. However, one can hardly imagine that there could be two contradictory concepts of "war" within one and the same system of international law.

For many decades the term "war" has been felt to be a problem. Objective discussion has been seen as a suitable means for lifting the fog of illusory fiction, to reveal the true situation of present-day (or past) international law. In the years prior to the Second World War, the main world powers had many (good and bad) reasons for seeking to form nuanced words and terminology to deal with the nuances between open war and genuine peace. The phrase "total war" was a case in point. Of course, the problem of the term "war" could not be solved by such indecisive strategy, the main reason being that the justness of war is also part of "total" war. While it is possible to argue over whether the problems connected with the term "discriminating war" were introduced into the history of modern (or past) international law when President Woodrow Wilson of the USA made his declarations on 2 April 1917 and led his country into the First World War against Germany, it can hardly be denied that it posed the question of a just war differently from the way it had been posed by scholastic theologians of centuries gone by. Before George W. Bush took office, there were no more "holy wars" fought by religiously agnostic nations. Nevertheless, the experiences of the First World War against Germany showed that wartime propaganda was in no way prepared to abstain from mobilising the moral powers which can only be summed up under the heading "crusade."

This is not the place for deciding whether history is repeating itself. Suffice it to say that the terms "good" and "evil" have risen to become pivotal categories in recent American foreign policy, and that in the eyes of the American leadership there are some states which have aligned to form an "axis of evil." In his second Inaugural Address, President Bush also told the rest of the world that his nation had "a calling from beyond the stars." Meanwhile, there are some fundamental Islamists in our time who seem to believe that the West is (again) going on a "crusade" against the world of

Islam. It would therefore appear that the quality of analysis has not improved decisively in recent years, and that a similar type of argument is being used by some of the opposing parties in the present conflict. Of course, this is not by itself a justification for the thesis that Osama bin Laden and George W. Bush are "birds of a feather." In any case, it is more important to note that our present-day mentality needs certain legal procedures, or procedures based on moral positivism, to accept the doctrine of a "just war." Some of those alive at the time of the League of Nations held it mainly to be a legitimising system which was intended to localise (in Geneva) the monopoly on judging whether a war was just or not. With the move towards the concept of discriminating war, certain powers were to be handed the authority to decide on the right or wrong of war. At the time, the Covenant of the League of Nations saw the League merely as a means of preparing for a fully-fledged "total" war, that is, a "just" war waged in accordance with international and supranational standards.[26]

The standards set in the United Nations Charter have had a modernising influence. However, a detailed comparison will only be of limited value, not least because the President of the USA has repeatedly declared in public that the right of the USA to defend itself will not be tempered to any decisive extent by international law. This might suggest that the USA has yet to achieve the general framework standards set by the Congress of Vienna (1814–1815) in a period of general restoration, when the parties at least managed to restore the concepts related to a European law of war. This was one of the most amazing (and hugely successful) feats of restoration in the history of the world. This law of war, with its containment of hostilities within a continental land war, still held sway in the European war waged during the First World War. Even many years afterwards, it was still recognised as being a "classical" law of war on account of its clear differentiation. It differentiated between war and peace, combatants and non-combatants, enemy and criminal. War is waged by one state on another with their regular state armies, between the sovereign agencies of a *ius belli*, with respect for their enemies even in times of war. They do not discriminate against each other by calling their enemies criminals, so that peace treaties can be concluded, and even the normal end to a war remains a matter of course. Partisans only appeared on the fringe of this classical pattern of regularity, and the modern-style terrorist, even when labelled an "enemy combatant," is also way over the horizon.

Classical law of war began to be pushed to its limits when general conscription was introduced and the idea was developed of a "war between peoples." Prior to this, war had been contained as a matter of principle. Then the partisan appeared on the scene, a fighter who refused and refuses to be contained, for this is his nature and the reason for his existence. The modern partisan – herein lies his partial affinity with the modern terrorist – expects neither justice nor mercy from his enemy. He has turned his back on the conventional enmity that exists in a war which has been tamed and contained, and moved towards a different kind of genuine enmity. This is enmity which builds up through terror and counterterror and ends in destruction.

---

[26] cf. (all of): C. Schmitt, *Die Wendung zum diskriminierenden Kriegsbegriff* (Berlin 1988) pp. 1, 2.

This typology is especially found in two types of war: civil war[27] and colonial war. It is obvious that these two forms of war elude traditional European international law, according to whose regulations open civil war was considered to be armed insurrection, to be put down with the help of the police and regular troops, as long as it did not lead to the recognition of the rebels as a warring party. Military historians in European nations such as England, France and Spain had not of course lost sight of colonial war. Nevertheless, they did not call into question the classic model of normal war between states.[28] In epochs of revolutionary upheavals, this model loses its force and its ability to put its stamp on affairs. In a time of revolutions, it is of vital, existential and primary importance that one should be able to distinguish between friend and foe. This affects war and politics equally. Lenin implemented this in his political activities by recognising revolutionary war as the only "true" war. Only this kind of war springs from "absolute" enmity. He considered all other types to be a game played according to conventional rules. The consequence is clear: a war which springs from absolute enmity knows no containment; it gets its "meaning" and is "just" from its fulfilment of absolute enmity. The all-decisive question is thus: is there an absolute enemy and who in fact is he?[29]

A theory of war cannot exist without a distinction between different types of enmity. Distinctions between one kind of war and another are based on different kinds of enmity, so that this latter will be the most important term when it comes to efforts to contain war. The proscription of war under international law will never lead to its abolishment. Unfortunately, after the Napoleonic Wars, irregular war was for a long time pushed to the back of people's minds and a fatal ignorance emerged as to what it means when irregular war is let loose. Carl Schmitt believed that it was people's inability to think in concrete terms that completed the revolutionaries' work of destruction. He said that this was a source of great misfortune, since the containment of war had enabled Europeans to achieve something remarkable: the non-criminalisation of their adversaries in war, and therefore the relativisation of enmity and the denial of absolute enmity. He believed this to be a truly unusual and extraordinarily humane achievement, since it meant that people could be persuaded to give up discrimination against, and defamation of, their enemies. The present-day partisan does not go down this path, because he is characterised and bound by the most extreme form of political commitment. The political imperative towers above everything else. He is a "Jesuit of war" (Che Guevara). Nevertheless, the traditional partisan has a real (but not an absolute) enemy, and here he differs from the typical fundamental Islamist terrorist who is on the move globally. Basically, the conventional partisan remains a defender of his native soil. His enemy is real but not absolute, and he certainly does not define him as mankind's worst enemy.

Lenin moved the terminological centre of gravity from war to politics. We may pass over the question as to whether this made sense, and if it was a logical extension

---

[27] Fundamentally: H. M. Enzensberger, *Aussichten auf den Bürgerkrieg* (Frankfurt am Main 1996).

[28] C. Schmitt *Theorie des Partisanen* (Berlin 1975), pp. 16–18.

[29] cf. C. Schmitt, *Theorie des Partisanen* (Berlin 1975), pp. 55, 56.

of von Clausewitz's idea of war as a continuation of politics. The important thing is that Lenin, being a professional soldier engaged in worldwide civil war, went further still and turned the real enemy into an absolute enemy. Carl Schmitt reminds us that Clausewitz had indeed spoken of absolute war, but he had always taken the existence of the state for granted, and all that regularly goes with it. Clausewitz would have been unable to imagine a state that was the instrument of a political party. If the party is made absolute, then the partisan is absolute too, and in the end he will be the agent of absolute enmity.[30] It may sound confusing, but this could make Lenin a logical forerunner of the inhuman totalitarianism practised by terrorists who claim to be driven by religious motives. We do not need to go into detailed reasons as to why these perpetrators of violence most terribly dishonour and abuse one of the great religions of the world, to celebrate their sick view of the West as "Satan" by mass murder of their victims. In their eyes, the "infidel" is the absolute enemy. Equally absolute is the commandment to destroy him. Nevertheless, when these present-day assassins attack states in a "warlike" way, it is doubtful whether the governments of these states are allowed to (and have to) defend themselves with use of arms according to the rules for national defence.

9.5 War or Raid?

An epoch-making transition occurred when the threshold to "mass terror" was crossed. Learned discussions on law and politics do little to help evaluate this danger. The present-day desperadoes who perpetrate inhuman violence are also called "terrorists" who are frightened of nothing, because they have nothing to lose, but everything to gain. They are fighting for no-one, and therefore have no fear of retribution for the states and peoples who support them. The risk of mass terror increases, the lonelier the perpetrators are.[31] Terrorism has even moved on to become a "war of terror."[32] The victims of the "old" terrorism used to include selected representatives of the state or the business community. Nowadays, terrorist activity appears as summary and arbitrary violence. The actual damage done is in fact a consequence of indiscriminate attack. In a certain sense, chance has allied itself to terror. The whole of society is paralysed because no-one feels safe, and no-one benefits from a formal or informal "selection" any more. There is collective fear, whose catalyst no longer serves to implement a rationally developed programme of intentions, nor is it a case of facilitating the communication of any particular messages of substance.

This is a fatal way of looking at things. People cannot live with long-term fear once it has exceeded a certain degree; they either take flight or develop strategies for adapting to it. The terrorist assassin is clear in his mind about what this means

[30] C. Schmitt *Theorie des Partisanen* (Berlin 1975), p. 94.

[31] W. Sofsky, Das Prinzip Sicherheit (Frankfurt am Main 2005) p. 157.

[32] At length: H. Münkler, Die neuen Kriege (Berlin 2002).

for him: he has to boost the quality and quantity of his attacks. The terrorist is compelled to aim for total terror. It is no longer enough to demonstrate that the "enemy" is vulnerable. Assassination becomes massacre, a terrorist attack becomes a terrorist war.[33]

Terrorists live beyond the bounds of any kind of law. Their operations do not follow the rules of the international law of war. The conventions of international law are absolutely meaningless to them. The results are disastrous. It is all too tempting to renounce reasonable reciprocity. Commitment to behaviour according to the rules becomes fragile. Those countries which consider themselves to be under threat from terrorist ("warlike") attacks start to think in terms of the pure logic of self-preservation. The willingness to use illegal force grows even in democratic countries. The combination of political ambition and hysteria within society produces a dilemma for institutions and their instruments. There are hardly any more open fights on battlefields in terrorist war. Armies are reduced to specialist commandos units. Violence and killing happen invisibly. The waging of war is turning into the art of clandestine destruction. At the same time, military formations are forced to behave like police units. Both sides are overtaxed as a result of selective targets and blanket force of arms. The reliability and justifiability of selected targets suffer. Bystanders get caught in the cross-fire, becoming victims of amateurish acts of violence. At the same time, individual suspects are carefully prepared and targeted, only to be liquidated in the course of a manhunt. Acts of this kind cannot be compared to a classic military attack, or even to an execution without a sentence. The intention is annihilation pure and simple. We cannot avoid some difficult questions. What kind of success is achieved by this kind of act? Does it bring permanent peace to a territory? Is there a considerably reduced risk of further terrorist attacks? Has the pool for new recruits to carry out assassinations become smaller?

The terrorist has already won a (temporary) victory if he manages to survive. The weak man is sure of fame if we are convinced that David is always right, whether he wins, loses, or runs away.[34] The question is, is our thinking not hopelessly muddled if we then go on to believe that a superior force nearly always loses? An inescapable logic may result from the following thought: if the regular forces of the states that wish to defend themselves against attacks from terrorists manage to achieve one "victory" after another, as a result of their conventional superiority in the context of violent conflicts great or small, without producing a decisive change in the climate of threat, even triumph can easily turn into defeat. When the strong are victorious, there is always a risk that their behaviour will be seen as cruelty. Superior forces have manoeuvred themselves into an almost hopeless position. A single misdeed from among the ranks of their troops will always trigger outrage. If they hold back, they will be called weak, and this will provoke further terrorist attacks. History provides countless graphic examples of the fact that long wars against an inferior adversary

[33] W. Sofsky, Das Prinzip Sicherheit (Frankfurt am Main 2005), pp. 114–116. cf. also: W. Hetzer, Attentat und Rechtsstaat, 56 *Kriminalistik* (2002) pp. 490–497.

[34] W. Sofsky, Das Prinzip Sicherheit (Frankfurt am Main 2005), p. 125.

end in a loss of self-esteem. The morale of the troops is destroyed by brutality on all sides, and ultimately there is no more sense of justice.[35] Military tactics are replaced by murderous acts of vengeance against defenceless civilians, women and children. This provokes other important questions:

- Is it merely a matter of time before terrorists win their victory on the changing battlefields of the world?
- If the armies despatched by the western democracies are not only operating on mined territory, but also marching unstoppably into a credibility gap, can they only escape by beating a general retreat?
- What part do domestic and international law play in efforts to guarantee the safeguarding of objects of legal protection and in tempering the use of violence within the meaning of human rights?
- Is there a hostile and lasting relationship between military responses to terrorist attacks and the constitutional state's obligation to observe the commandment of proportionality when dealing with those who break the law?
- Will we ever be able to avoid the moral and humanitarian pitfalls which have already beset the soldiers of regular armies?
- Are there any precautions which might successfully be taken to prevent a victor with superior resources over an adversary who is weak from being discredited psychologically and politically?
- If one is tied up in long wars of an "asymmetric" nature, how can one avoid moral decline in individuals and false-sounding political assumptions?

The most important qualities needed in the fight against terrorist perpetrators of violence may be said to be "steadfastness and self-control." The societies affected are even recommended to practise "heroic composure" (H. Münkler) in dealing with terrorist threats. Sang-froid can of course rein in panic, and discipline can be a shield against over-reaction. Tight rules of engagement might guarantee that no-one opens artillery fire on young stone-throwers and that, if suspects are presumed to be in a certain district of a town, the whole area is not reduced to ashes after being subjected to carpet bombing. However, the binding effect of legal rules is apparently not sufficient to prevent a raid from turning into excessive violence or an interrogation from descending into torture. The whole world is now familiar with examples of this kind of failure, and they are now being traded as symbols for the profound demoralisation of some military units.

The numerous regulations present a further dilemma. On the one hand, they are intended to counteract the risk of war crimes; on the other, they have almost resulted in a soldier's being at the mercy of terrorists. If he yields to the temptation of giving back as good as he gets, he degenerates into being an armed bandit, or a member of a killer commando unit. This is military "original sin": breakdown of discipline. This is not the only reason why the extremely questionable practice of outsourcing has come into being. The result is the privatisation of war. Members

[35] W. Sofsky, Das Prinzip Sicherheit (Frankfurt am Main 2005), p. 126.

of regular military units no longer have to get their own hands dirty; mercenaries and security services, which are untrammelled by military obligations or observance of international law, are assuming duties of a precarious nature. The age-old adage still applies in our time: "War feeds on war."

One consequence of this is particularly dramatic: the dividing line between war and crime has blurred. Sooner or later, the private providers of war services will use their own methods to obtain (re-)payment. They will act in their time-honoured way, and help themselves to the treasures of the country they are in, so that it will be impossible to distinguish between them and marauding bands of criminals or terrorists. In the meantime, with the support of the states who carried out the armed intervention, a generally weak regional government will enter into alliances with warlords, some of whom will even get high-ranking positions in the regular armies of states in which the risk from terrorism is particularly acute. The fact is that the term "warlord" is used to describe a familiar cross between a terrorist and a criminal, one who has succeeded in donning a mantle of respectability and worked his way into circles of political power, to become the recognised partner of western democracies. We will not discuss whether foreign policy and security policy are at odds here, or whether it is simply a case of corruption of one's own ideals. In any case, the argument will end with the stereotype remark, "it had to be done for reasons of *Realpolitik*." Keeping to the straight and narrow path between excess and patience, desire for retaliation and discipline is surely the hardest task facing both top brass and ranks in states which believe they can defeat terrorism by feat of arms. It is an extremely delicate balancing act overall, and it cannot go on for ever. We should therefore remind ourselves of the wisdom of the old saying which goes "better a quick end with terror, than terror without end."[36] The alternative is unavoidable: total corruption of all the ideals for the sake of which we said we were going to war against terror.

9.6 Rigourism or a Sense of Proportion?

It was clear even before the recent bombings in London and Madrid that modern terrorism cannot be contained geographically, and that it is not restricted to the world beyond the apparently secure borders of the European Union. Serial mass murder must not be interpreted as the response from the downtrodden and resentful citizens of the "Third World" to an arrogant foreign policy of the only remaining world power. The attitude expressed in these assassinations cannot be explained by a religious belief. These are not combat operations in a "religious war." It seems more likely that the perpetrators are opposed to a lifestyle they consider to be "western" and decadent. Nevertheless, it would be wrong to believe that the terrorist attacks are (nothing but) the violent expression of cultural conflict. All the same, social orders

[36] W. Sofsky, Das Prinzip Sicherheit (Frankfurt am Main 2005), p. 127.

which are based on liberty, equality, tolerance and the pursuit of personal happiness must be hugely provocative to persons of a certain character type. This particular type is possibly more likely to be found in a fundamentalist Islamist environment than among people with other political and social backgrounds. Character types of this kind will presumably see not only society in the USA but also the Member States of the European Union as a gathering of infidels. In the majority of cases these will in fact be people who are unable to come to terms with the challenges of contemporary economic and social structures, and their inability to do this lies in their individual psychology, which is intensified by the dynamics of their group. They probably see Europe too as a world lacking in meaning, and in which the necessary spiritual orientation is missing on account of the primacy of material success. The (incomplete) list of ingredients which go to make up the terrorism which has now fixed its sights on Europe includes the following: disdain for humanity, a lack of gender equality, a hypocritical and rigid system of morals with almost neurotic excesses, a lack of professional and economic prospects, a murderous form of *machismo*, a lack of personal self-esteem, disrespect for people of other races, weakness of character, the inability to feel pity and many other factors besides.

The European Union has so far also been unable to prescribe any patent remedies for combating terrorism. During its extraordinary meeting on 21 September 2001, the European Council declared that terrorism was a "real challenge to the world and to Europe" and that the fight against this phenomenon would be a priority objective of the European Union. A few days later (28 September 2001), the United Nations Security Council adopted Resolution 1373 (2001), which reaffirmed that terrorist acts were a threat to peace and security. Shortly after that (8 October 2001), the European Council affirmed the determination of the European Union and its Member States to play their part, in a co-ordinated manner, in the global coalition against terrorism, under the aegis of the United Nations. They also reiterated their determination to attack the sources which fund terrorism, in close co-operation with the USA. This was to take place especially through increased co-operation between the operational services responsible for combating terrorism: Europol, Eurojust, the intelligence services, police forces and judicial authorities.

In the "Common Council Position" of 27 December 2001 on combating terrorism,[37] the Council declares that the wilful provision or collection, by any means, directly or indirectly, of funds by citizens or within the territory of each of the Member States of the European Union with the intention that the funds should be used, or in the knowledge that they are to be used, to carry out terrorist acts is to be criminalised. Funds and other financial assets or economic resources of persons or entities with a specific link to terrorism are to be frozen. Steps are to be taken to prevent the commission of terrorist acts, including by the provision of early warning among the Member States or between Member States and third States by exchange of information. Persons who participate in the financing, planning, preparation or perpetration of terrorist acts are to be prevented from using the territory of the European Union as a safe haven.

[37] OJ L 344/90, 28. 12. 2001.

Member States are to afford one another, as well as third States, the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts in accordance with international and domestic law, including assistance in obtaining evidence in the possession of a Member State or a third State which is necessary for the proceedings. The movement of terrorists or terrorist groups is to be prevented by effective border controls and controls on the issuing of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of documents.

The "Council Common Position on combating terrorism"[38] of 27 December 2001 includes a statement on what is meant by a "terrorist act" (Article 1(3)).

It must be a particular intentional act, which, given its nature or its context, may seriously damage a country or an international organisation, as defined as an offence under national law, where committed with the aim of:

- Seriously intimidating a population,
- Unduly compelling a government or an international organisation to perform or abstain from performing any act, or
- Seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

These effects can be variously achieved through the following:

- Attacks on a person's life which may cause death or attacks on the physical integrity of a person;
- Kidnapping or hostage taking;
- Extensive damage to certain facilities;
- Seizure of public means of transport;
- Manufacture, possession, acquisition, transport, supply or use of certain weapons;
- Release of dangerous substances, the effect of which is to endanger human life; causing fires, explosions or floods;
- Interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life, and threatening to commit any of the above-mentioned acts and
- Directing a terrorist group and participating in its activities.

On the same day, the Council issued "Regulation (EC) No. 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism,"[39] because it felt that a measure was needed at Community level which was complementary to existing administrative and judicial procedures regarding terrorist organisations in the European Union and third countries. The Regulation starts by defining the following terms: "funds, other financial assets and economic resources," "freezing of funds" and "financial services." It provides for the freezing of all funds, other financial assets and economic resources belonging to, or owned or

[38] OJ L 344/93, 28. 12. 2001.

[39] OJ L 344/70, 28. 12. 2001.

held by certain persons, groups or entities included in a list. It also provides for the prohibition of funds being made available or the provision of financial services.

In its "Framework Decision of 13 June 2002 on combating terrorism,"[40] the Council emphasises that terrorism constitutes one of the most serious violations of the universal values on which the European Union is founded:

- Human dignity
- Liberty
- Equality and solidarity
- Respect for human rights and fundamental freedoms
- Democracy
- The principle of the rule of law

Article 1 of the Decision lays down that each Member State of the European Union is to take the measures necessary to ensure that certain intentional acts which are defined as offences under national law be deemed terrorist offences, if they are committed with certain aims which are then listed. It is worth noting the fact that the Framework Decision does not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union (Article 1(2)).

A "terrorist group" is taken to mean a structured group of more than two persons established over a period of time and acting in concert to commit terrorist offences. A structured group is deemed to be organised if it is not randomly formed for the immediate commission of an offence. It does not need to have formally defined rules for its members, continuity of its membership or a developed structure.[41]

The Framework Decision also provides for sanctions against legal persons (Articles 7 and 8).

In its "Communication to the Council and the European Parliament on measures to be taken to combat terrorism and other forms of serious crime, in particular to improve exchanges of information" the European Commission presented a "Proposal for a Council Decision on the exchange of information and co-operation concerning terrorist offences."[42]

The Commission begins by stressing the fact that terrorism is a phenomenon with complex and various causes and implications. It can destroy the confidence of citizens and firms in economic structures, and can have a negative impact on economic growth and the preservation of an investment-friendly climate. This is why they believe that the fight against terrorism must remain high on the European Union's list of priorities. Action must be taken, they say, to "eradicate" terrorism as closely as possible to its foundations to cut off terrorist organisations from their sources of funding. The Commission believes this to be particularly difficult, and is convinced that a link should be established between measures to combat organised crime and

[40] OJ L 164/3, 22. 6. 2002.

[41] Article 2.

[42] COM(2004) 221 final, 2004/0069 (CNS).

terrorism. They go on to say that although the links between terrorism and other forms of crime, in particular organised crime, are not always immediately obvious, nevertheless there are links between the two types of crime, sometimes even between the actual groups. This is particularly true of arms trafficking, diamond trafficking and counterfeiting and piracy of goods. The financing of terrorism is already an offence in the Union, which makes it possible to tackle cases where terrorist organisations obtain financial support from legitimate sources, such as charitable or other legal bodies. Terrorist organisations which seek financing use methods similar to those of criminal organisations, such as extortion, kidnapping with ransom demands and all kinds of trafficking and fraud. Like criminal organisations, they also practise corruption and money-laundering. The Commission believes that it should be possible to dry up the "legal" sources of terrorist financing by mobilising the Member States in the fight against terrorism and increasing public awareness of this fight. It is convinced that if the fight against terrorism is to be totally effective, it must be handled in conjunction with the fight against other forms of crime.

The Commission argues in favour of a review of the Joint Action on making it a criminal offence to participate in a criminal organisation,[43] which was adopted by the Council on 21 December 1998. This measure not only concerns organised crime but also terrorist organisations, insofar as it specifically applies to the categories of offence referred to in Article 2 of the Europol Convention, which also aims at preventing and combating terrorism. The Commission says the revision should take into account those factors which have changed since 1998, including the fact that the "Framework Decision" has been introduced to provide a more suitable instrument than the "Joint Action" for harmonising the definition of offences and penalties. The Commission's aims are as follows:

- The actual harmonisation of definitions of offences and penalties as regards individuals and bodies corporate.
- The provision of a specific offence of "directing a criminal organisation."
- The determination of specific aggravating or mitigating circumstances.
- The inclusion of provisions to facilitate co-operation between judicial authorities and co-ordinate their action.

They also propose the drawing up of an electronic list of persons, groups and entities to whom restrictive measures taken to fight terrorism apply, or who are under investigation for criminal offences. We have already stated that the freezing of funds or other financial assets and economic resources of individuals, groups and entities involved in terrorism is one of the mechanisms that exist in the Union to combat terrorism. Lists are drawn up for this purpose, which are regularly updated and published in the European Union's Official Journal. A large number of the individuals and organisations whose names have been published in it need to be kept under particularly close surveillance, particularly in their banking business, as they are subject to financial restrictions.

[43] OJ L 351/1, 29. 12. 1998.

The Commission also believes that an attempt should be made to establish an efficient system for registering bank accounts in every Member State, to allow for a rapid response to requests for judicial assistance on bank accounts and movements of funds. Police and judicial co-operation faces considerable difficulties in the area of financial crime, because it is all but impossible to complete investigations into bank accounts and movements of funds with any success. If bank accounts were registered under a centralised system, this would facilitate the tracing of movements of funds within the framework of criminal investigations, above all with regard to the financing of terrorism and money laundering. The Protocol established by the Council Act of 16 October 2001 on the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union already contains provisions on requests for information on bank accounts, requests for information on banking transactions and requests for the monitoring of banking transactions.[44]

There also needs to be a mechanism for gathering and transmitting information, to prevent terrorist organisations from infiltrating legitimate activities. It has already been suggested that legitimate entities are being used to serve the needs of terrorist groups, particularly their financial needs. Likewise, organised criminal groups are infiltrating legitimate activities for money-laundering purposes. There can no longer be any doubt that improved transparency of bodies corporate and charitable organisations will help to prevent and combat both organised crime and terrorism more effectively. It is right that the Strategy of the European Union for the next Millennium should include a recommendation that the Member States should seek to collect information, in compliance with the relevant rules relating to data protection, on physical persons involved in the creation and direction of legal persons registered in the territory of Member States, as a means to prevent the penetration of organised crime in the public and legitimate private sector.[45] Regarding the implementation of the recommendations contained in this strategy paper, the Commission staff expressly support the extension of this mechanism, which was originally designed to help combat organised crime, to the financing of terrorism. Of course these measures should be devised in close co-operation with representatives of the relevant sectors. It will be necessary to ensure that greater transparency regarding the managers, shareholders and true owners of companies does not have a negative effect in terms of loss of efficiency and increased overheads, as a balance will have to be struck between the interests at stake and the proportionality of the means deployed.

Furthermore, the Commission says the establishment of a European criminal record should be envisaged, as a contribution to the effectiveness of the fight against crime, and in particular terrorism. In addition to this, they foresee (at the intermediate stage) the necessity for a total exchange of information between the Member States and the Union bodies responsible for combating terrorism. Council Decision 2003/48/JHA of 19 December 2002 on the implementation of specific measures for police and judicial co-operation to combat terrorism is already a major step forward, they say.

---

[44] OJ C 326/1, 21. 11. 2001.

[45] OJ C 124/1, 3. 5. 2000.

To sum up, the Commission is convinced that greater efforts have to be made in the fight against terrorism and the most serious forms of crime. They propose a step-by-step approach, and the steps below are an indication of some such progress in the last few years:

- The Council Decision which took account of the factors mentioned above.
- The adoption of a Framework Decision to replace the Common Position of 1998, strengthening the legal instruments at the Union's disposal with regard to criminal organisations, and harmonising existing Union regulations on combating terror.
- The establishment of a database or a consolidated electronic list of persons, groups and entities who are the subject of restrictive anti-terror measures, or who are under criminal investigation for terrorist offences.
- The development of a European legal instrument for the establishment of national systems for registering bank accounts in the Member States allowing the true account holders to be identified and facilitating investigations into bank accounts and movements of funds.
- Improvements in the transparency of bodies corporate to counter the infiltration of the legitimate sector by criminal groups and terrorist organisations.
- The organising of a debate with the Member States on the putting in place of a scheme which is proportionate and compatible with fundamental data protection rights, to implement the legal instruments, as well as the addressing of this issue in the Forum on Organised Crime Prevention.
- A debate on the introduction of an effective mechanism for the exchanging of information on convictions and disqualifications.

Following the attacks on Madrid on 25 March 2004, The European Council adopted a Declaration on combating terrorism, in which they reaffirm their conviction that terrorist acts are attacks on the values on which the European Union is founded. The Declaration stresses the need for a revised plan of action for combating terrorism, in order to supplement the plan of action which had been agreed following the attacks of September 2001. The new strategic goals which are listed in the Action Plan of 7 June 2004 may be summarised briefly under the following headings:

- A deepening of the international consensus and enhanced international efforts to combat terrorism.
- Further impediments to terrorists' access to financial and economic resources.
- Maximisation of the ability to detect, investigate, prosecute and prevent terrorist attacks within the institutions of the European Union.
- The safeguarding of international transport links and the protection of an effective frontier control system.
- Enhancement of the ability to cope with the consequences of a terrorist attack.
- Identifying and tackling factors which are significant in the support for terror and the recruitment of terrorists.
- Development of measures to assist third countries to increase their ability to defend themselves against terror within the framework of the European Union's external relations.

The European Co-ordinator for counterterrorism, Mr. Gijs de Vries, spoke in Washington on 13 May 2004 during a visit to the USA (CSIS European Dialogue Lunch) on a European strategy in the fight against terrorism and the co-operation with the USA. His assumption is that America and Europe are "natural partners" in the fight against terrorism. In view of the fact that terrorism is an all-out attack on our social, political and economic system, he sees that there is a temptation to believe that any measures can be used to fight the threats involved. However, Mr. De Vries rightly points out that we must be careful to protect and preserve the rights and liberties terrorists are seeking to destroy. Otherwise the terrorists will have won. Victory can only be won in this battle, he says, if we do not abandon the principles of legitimate action.

9.7 Final Remarks

Clear definitions are needed when problems are being described, and special efforts to attain clarity are necessary when we are dealing with a complex phenomenon such as modern terrorism. It has been shown that we in the European Union have been striving for clarity for several years. Our discourse on the threat from terrorist attacks to the western community of values now seems to have taken on an eschatological dimension, which is not surprising, given the differentiation between "good" and "evil" that determines American foreign policy.

In Germany too, international terrorism is felt to be a challenge of global and historic proportions. Our entire civilisation is felt to be under threat. The "*war on terror*" will presumably remain the dominant subject in international politics. We will presumably have to be prepared for future barbarous terrorist attacks. Islamist terrorists seem to have set their main sights on targets in the USA, Great Britain and Israel, as well as those countries' institutions abroad. However, they also carry out random attacks in other parts of the world too. People everywhere are trying to work out new defence strategies, but the USA has in many ways taken the lead. They claim to have discovered our need for something beyond conventional military deterrents. Nevertheless, even massive retaliatory threats have been unable to prevent assassins from roaming the world and carrying out their plans.

The expression "war on terror" seems to have become a *leitmotiv.* We now have to fear that the unsubstantiated assumption of a risk (i.e., the risk that there might be a danger) is sufficient justification for the fiercest kind of intervention imaginable, namely a war of aggression. The proclamation (not declaration) of war on terror, however, increasingly seems to be acting as a basis for depriving our opponents of their fundamental rights. It is no longer a case of confirming suspicion to prosecute a criminal offence, or fighting criminals who are still entitled to their procedural human rights up to the time of their conviction, and their substantive human rights once they have been convicted. The fight is against evil, pure and simple, which is so wicked that people think they do not have to respect the rights their "enemies" are entitled to either (simply because they are their enemies). It then seems logical

to carry out preventive executions of a foe who is on the run or in hiding. It also seems logical to deprive prisoners of their rights and hold them on the basis of pretended extraterritoriality, using a kind of emergency legislation to reduce even their own country's formal and substantive basic rights to an all but invisible minimum.

Security policy is currently marked by abnormal psychological fear. Some measures for combating terrorism are a kind of sedative or placebo. A fearful population is seemingly meant to feel that their government has suitable and timely methods for confronting the threat of modern terrorism. It is easy to lose sight of the fact that these are only the symptoms of much deeper underlying causes. Nevertheless, the frightened people whom the government are supposed to be protecting are so conditioned that they are willing to believe that their leaders are keeping their promises to take action.

We can leave aside the question as to whether a few particularly forceful politicians have succeeded in introducing the "messianic principle" into security policy. It is disturbing enough to observe the relatively smooth passage of anti-terror bills and the acceptance of anti-terror measures, with no questions asked as to their appropriateness and no forecasts made as to their successful outcome. Many people seem to have forgotten that there is no such thing as complete man-made security. A state that knows no bounds when it comes to the protection of its citizens is no longer free. While it is true that terrorism threatens liberty and security in equal measures, it can also happen that the threat makes us renounce freedom of our own accord, but the hoped-for security from threat will still escape us. It is to be hoped that a continuation of the traditions of the Enlightenment in Europe will save us from going down this path. There must be careful analysis in conjunction with decisive action, and it is the Member States of the European Union which are particularly called on to provide this. In some countries, there are large areas of security policy which can only be explained away in terms of the fairy tale of The Emperor's New Clothes. The idea that problems related to international terrorism can be solved by descending into a permanent state of war is analytically absurd, politically irresponsible and morally untenable.[46] The consequences would be disastrous. The European Union in particular must therefore continue to strive for a sense of proportion. If it does not, current security policy might be neatly summed up by another fairy tale: "The Pied Piper of Hamelin."

References

Enzensberger, H.M. (1996). Aussichten auf den Bürgerkrieg. Frankfurt am Main.

Hecker, J. (2006). Die Europäisierung der inneren Sicherheit. Die Öffentliche Verwaltung, 59, 273–280.

Hetzer, W. (2002). Attentat und Rechtsstaat. Kriminalistik, 56, 490–497.

[46]More on the necessary differentiation: W. Hetzer, Terrorbekämpfung -Strafverfolgung oder Kriegsführung?, 58 *Kriminalistik* (2004)pp. 508–517.

Hetzer, W. (2003). Krieg und Kriminalität. Innere und äußere Sicherheit: Unterscheidung oder Verschmelzung? In J. Calließe (Ed.), Die Verflochtenheit und Verflechtung von äußerer und innerer Sicherheit (pp. 49–69). Rehburg-Loccum.
Hetzer, W. (2004a). Europa gegen Terror. Der Kriminalist, 36, 332–339.
Hetzer, W. (2004b). Terrorbekämpfung -Strafverfolgung oder Kriegsführung? Kriminalistik, 58, 508–517.
Hetzer, W. (2005a). Terrorabwehr im Rechtsstaat. Zeitschrift für Rechtspolitik, 38, 132–135.
Hetzer, W. (2005b). Terrorismusbekämpfung zwischen Risikosteuerung und Rechtsgüterschutz. Monatsschrift für Kriminologie und Strafrechtsreform, 88, 111–126.
Hetzer, W. (2005c). Die Flucht des Gesetzgebers in die polizeirechtliche Prävention. Strafverteidiger Forum, 10, 318–324.
Hetzer, W. (2006a). Verschleppung und Folter. Kriminalistik, 60, 148–159.
Hetzer, W. (2006b). Ist Freiheit durch Sicherheit korrumpierbar? Strafverteidiger Forum, 11, 112–118.
Jarass, H.D., & Pieroth, B. (2006). Grundgesetz für die Bundesrepublik Deutschland. München.
Käppner, J. (2006). Süddeutsche Zeitung. 45 of 23. 2. p. 11.
Meyer, A. (2004). Wirksamer Schutz des Luftverkehrs durch ein Lufsicherheitsgesetz? Zeitschrift für Rechtspolitik, 37, 203–207.
Münkler, H. (2002). Die neuen Kriege. Berlin.
Schäuble, W. (2006a). Süddeutsche Zeitung no. 45 of 23. 2. p. 11.
Schäuble, W. (2006b). Der Spiegel no. 21 of 22. 5. p. 38.
Schenke, W.-R. (2006). Die Verfassungswidrigkeit des § 14 III LuftSiG. Neue Juristische Wochenschrift, 59, 736–739.
Schmitt, C. (1975a). Theorie des Partisanen (pp. 16–18). Berlin.
Schmitt, C. (1975b). Theorie des Partisanen (pp. 55, 56). Berlin.
Schmitt, C. (1975c). Theorie des Partisanen (p. 94). Berlin.
Schmitt, C. (1988). Die Wendung zum diskriminierenden Kriegsbegriff (pp. 1, 2). Berlin.
Sofsky, W. (2005a). Das Prinzip Sicherheit (p. 157). Frankfurt am Main.
Sofsky, W. (2005b). Das Prinzip Sicherheit (pp. 114–116). Frankfurt am Main.
Sofsky, W. (2005c). Das Prinzip Sicherheit (p. 125). Frankfurt am Main.
Sofsky, W. (2005d). Das Prinzip Sicherheit (p. 126). Frankfurt am Main.
Sofsky, W. (2005e). Das Prinzip Sicherheit (p. 127). Frankfurt am Main.

Chapter 10
The Evolution of the Antiterror Legal and Institutional Framework in Croatia

Davor Derenčinović

10.1 Introduction

The Republic of Croatia has been an active member of the Global Anti-terrorism Coalition since the beginning of the Afghanistan crisis. In this regard, with full respect to international law, Croatia has always acted in accordance with the obligations set out by the United Nations, in particular, the provisions of the committee established pursuant to Security Council Resolution 1267 (1999).[1] Following the horrific events of 11 September 2001,[2] which unfortunately opened a new era in international terrorism,[3] the Government of Croatia promptly established an Interagency Working Group (IWG) for Monitoring Implementation of United Nations Security Council Resolution 1373 (2001).[4] In addition to the obligation to implement the antiterrorist resolutions of the UN Security Council, the prevention and suppression of terrorism and the active contribution of the Republic of Croatia to the antiterrorist coalition was defined as one of the priorities of the National Security Strategy adopted by the Croatian Parliament at its session on 19 March 2002.[5] The Republic of Croatia is fully committed to co-operating with neighbouring countries and regional organizations, as well as with

D. Derenčinović (✉)
Faculty of Law, University of Zagreb, Zagreb, Croatia
e-mail: davorderen@yahoo.com

[1] S/RES/1267 (1999), 15 October 1999.

[2] See in general Cassese A. (2001). Terrorism is Also Disrupting Some Crucial Legal Categories of International Law, Eur J Int Law 12, 995; Becker S. (2003). "Mirror, Mirror on the Wall…", Assessing the Aftermath of September 11th, 37 Valparaiso University Law Review 563.

[3] See in general Laqueur W. (1998). The New Terrorism - Fanatism and the Arms of Mass Destruction, London.

[4] Committee of Experts on Terrorism (CODEXTER), Profiles on Counter-Terrorist Capacity – Croatia, June 2006, p. 1., available at http://www.coe.int/gmt, last visited 25 March 2008.

[5] Ibid. p. 2.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_10, © Springer Science+Business Media, LLC 2010

the United Nations and its Member States, and particularly with the Counter-Terrorism Committee[6] established by Security Council resolution 1373 (2001), in order to combat international terrorism more effectively.[7] In general, Croatia supports actions undertaken so far in accordance with relevant Security Council resolutions, in particular, resolutions 1268 (1999) and 1373 (2001), as well as the United Nations Charter, aimed at suppressing and eradicating international terrorism.[8]

In proving its commitment to share the rights and responsibilities within the global antiterrorist coalition, the Republic of Croatia has ratified the following global and regional antiterrorist conventions[9] (in chronological order, status as of 25 March 2008):

- Convention on Offences and Certain Other Acts Committed on Board Aircraft[10]
- Convention for the Suppression of Unlawful Seizure of Aircraft[11]
- Convention for the Suppression of Unlawful Acts against the Safety of Civil
- Aviation[12]
- Convention on the Prevention and Punishment of Crimes against Internationally
- Protected Persons[13]
- European Convention on the Suppression of Terrorism[14]
- International Convention Against the Taking of Hostages[15]
- Convention on the Physical Protection of Nuclear Material[16]
- Convention for the Suppression of Unlawful Acts against the Safety of Maritime
- Navigation[17]

---

[6] See http://www.un.org/sc/ctc/, last visited 25 March 2008.

[7] The current Chairman of the Counter-Terrorist Committee is Ambassador and Permanent Representative of the Republic of Croatia to the UN who took up his post in February 2008.

[8] Report of the Republic of Croatia pursuant to paragraph 6 of Security Council Resolution 1373 (2001) of 28 September 2001, par. 6.

[9] Pursuant to article 140 of the Constitution of the Republic of Croatia: "International agreements concluded and ratified in accordance with the Constitution and made public, and which are in force, shall be part of the internal legal order of the Republic of Croatia and shall be above law in terms of legal effects".

[10] Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1963. (hereinafter: Aircraft Convention).

[11] Convention for the Suppression of Unlawful Seizure of Aircraft, 1970. (hereinafter: Unlawful Seizure Convention).

[12] Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971. (hereinafter: Civil Aviation Convention).

[13] Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, 1973. (hereinafter: Diplomatic agents Convention).

[14] European Convention on the Suppression of Terrorism, 1977. (hereinafter: Depoliticizing Convention).

[15] International Convention Against the Taking of Hostages, 1979. (hereinafter: Hostages Convention).

[16] Convention on the Physical Protection of Nuclear Material, 1980. (hereinafter: Nuclear Materials Convention)

[17] Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988. (hereinafter: Maritime Convention).

- Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving
- International Civil Aviation[18]
- Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf[19]
- Convention on the Marking of Plastic Explosives for the Purpose of Detection[20]
- International Convention for the Suppression of Terrorist Bombings[21]
- International Convention for the Suppression of the Financing of Terrorism[22]
- Protocol amending the European Convention on the Suppression of Terrorism[23]
- International Convention for the Suppression of Acts of Nuclear Terrorism[24]
- Council of Europe Convention on the Prevention of Terrorism[25]

The format used in most of these instruments comprised four elements:

(a) The definition as an offence of a particular type of terrorist activity that was at that time causing great concern, as were unlawful seizures of aircraft in 1970 and attacks involving bombs and other dangerous devices in the 1990s
(b) The requirement that parties to the instrument penalize that conduct
(c) The identification of certain bases on which the parties agreed to exercise their criminal jurisdiction to control the defined offence, such as the country of registration of a ship or vessel, territoriality, or nationality
(d) The creation of the further jurisdictional obligation that a State party in whose territory a suspect is found must establish and exercise competence over the offence and refer it for prosecution if extradition is not granted pursuant to the particular convention or protocol. This last element is popularly known as the principle of "no safe haven for terrorists"[26]

---

[18] Protocol for the Suppresion of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Montreal, 1988. (hereinafter: Airport Protocol).

[19] Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, 1988. (hereinafter: Fixed Platform Protocol).

[20] Convention on the Marking of Plastic Explosives for the Purpose of Detection, 1991. (hereinafter: Plastic Explosives Convention).

[21] International Convention for the Suppression of Terrorist Bombings, 1997. (hereinafter: Terrorist Bombing Convention).

[22] International Convention for the Suppression of the Financing of Terrorism, 1999. (hereinafter: Terrorist Financing Convention).

[23] Protocol amending the European Convention on the Suppression of Terrorism, 2003. (hereinafter: Depoliticizing Protocol).

[24] International Convention for the Suppression of Acts of Nuclear Terrorism, 2005. (hereinafter: Nuclear Terrorism Convention).

[25] Council of Europe Convention on the Prevention of Terrorism, 2005. (hereinafter: Terrorism Prevention Convention, CECPT).

[26] Legislative Guide to the Universal Anti-Terrorism Conventions and Protocols, United Nations, Office for Drugs and Crime, 2004, p. 8.

I will now give a brief overview of the Croatian antiterrorism legal framework – relevant substantive and procedural criminal law provisions, as well as the assessment of its compliance with the aforementioned four elements of international antiterrorist treaties. Special attention will be given to considerations concerning the implementation of article 5 of the Council of Europe Convention on the Prevention of Terrorism. The Republic of Croatia has ratified this Convention and will be bound by its provisions after 1 May 2008. In this respect, the drafting of a separate criminal offence of public provocation to commit terrorism-related criminal offences in domestic substantive criminal law should not be treated as a purely technical issue but as a major challenge in searching for an appropriate balance in the efficient suppression of terrorism while preserving human rights.[27]

10.2 A Brief Overview of the Croatian Antiterrorism Legal Framework: Relevant Substantive and Procedural Criminal Law Provisions

The Croatian Criminal code[28] (CC) contains a number of criminal offences by which various forms of international terrorism are incriminated. These offences are international terrorism (art. 169), endangering the safety of internationally protected persons (art. 170), taking of hostages (art. 171), misuse of nuclear materials (art. 172), hijacking an aircraft or a ship (art. 179), and the endangering the safety of international air traffic and maritime navigation (art. 181). According to article 170 of the CC (endangering the safety of internationally protected persons) "whoever kidnaps an internationally protected person,[29] or commits some act of violence against such a person or attacks his official premises, accommodation or his means of transport" is criminally liable.[30] An aggravated form of the offence is when the

[27] See Human Rights and the fight against terrorism, The Council of Europe Guidelines, available at http://www.coe.int/t/E/Human_Rights/Lignes_dir_compendium_en.asp#TopOfPage, last visited 25 March 2008.

[28] Official Gazette 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, and 110/07.

[29] Under the article 1.1. (a) and (b) of the Diplomatic agents Convention "internationally protected person" is:

(a) A Head of State, including any member of a collegial body performing the functions of a Head of State under the constitution of the State concerned, a Head of Government or a Minister for Foreign Affairs, whenever any such person is in a foreign State, as well as members of his family who accompany him

(b) Any representative or official of a State or any official or other agent of an international organization of an intergovernmental character who, at the time when and in the place where a crime against him, his official premises, his private accommodation or his means of transport is committed, is entitled pursuant to international law to special protection from any attack on his person, freedom or dignity, as well as members of his family forming part of his household".

[30] Supra note 28, article 170. par. 1.

perpetrator, in the course of the perpetration of the criminal offence, intentionally kills one or more persons. For the intentional killing in the course of kidnapping, long-term imprisonment (up to 40 years) can be imposed. In case of negligently causing the death of one or more persons, imprisonment up to 5 years can be imposed. In addition, "whoever endangers the safety of an internationally protected person by a serious threat to attack him, members of his family, his official premises, private accommodation or his means of transport shall be punished by imprisonment not exceeding five years."[31] The criminal offence of hostage taking is committed when anyone "kidnaps, seizes or detains and threatens to kill, to injure or to detain another person in order to compel a certain state or an international organization[32] to do or abstain from doing any act as an explicit or implicit condition of the release of a hostage."[33] The following two paragraphs criminalize the intentional killing of a hostage (par. 2) and negligent causing of their death in the course of kidnapping (par. 3).[34]

The protection of nuclear material[35] is the *ratio legis* of the criminal offence of misuse of nuclear materials (art. 172). The perpetrator is any person who "by force, threat, the perpetration of a criminal offence or by any other way without authorization, procures, possesses, uses, transports, stores, gives to another or enables another to procure nuclear materials."[36] Endangering human lives and property to a greater extent is punishable by imprisonment for 6 months to 5 years.[37] The same punishment shall be inflicted on whoever, by serious threat to use nuclear material, endangers the safety of people.[38] An aggravated form of the offence takes place when any person, in order to compel some state or international organization or a natural or legal person to do or refrain from doing an act, "threatens to endanger the lives of people and property to a greater extent through the use of nuclear material".[39] If the result/consequence of the criminal offence provided in par. 2. was linked to the perpetrator's negligence at the time of commission, then imprisonment cannot exceed 3 years.[40] Another terrorism-related criminal offence is the hijacking an

[31] Ibid., par. 4.

[32] This provision is not entirely in line with article 1 of the Hostages Convention, which requires than an "aim to compel" could be directed not only to some state or international organization, but to natural person or legal entity or a group of persons as well.

[33] Supra note 28, article 171. par. 1.

[34] Ibid. par. 3 and 4.

[35] For the definition of the "nuclear material", see article 1.a of the Nuclear Materials Convention: "nuclear material" means plutonium except that with isotopic concentration exceeding 80% in plutonium-238; uranium-233; uranium enriched in the isotopes 235 or 233; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore-residue; any material containing one or more of the foregoing.

[36] Supra note 28, article 172. par. 1.

[37] Ibid. par. 2.

[38] Ibid. par. 3.

[39] Ibid. par. 4.

[40] Ibid. par. 5.

aircraft or a ship. Any person is criminally liable who, by force or serious threat to use force, "takes control over an aircraft in flight[41] or over a ship or a vessel".[42] The following two paragraphs incriminate the intentional killing of one or more persons in the course of the hijacking (par. 2) and the situation when the death of one or more persons or the destruction of an aircraft, a ship or a vessel, or some other extensive pecuniary damage is caused (par. 3).[43] Apart from aircraft or ship hijacking, whoever, without the aim to commit hijacking of an aircraft, "destroys or damages air navigation facilities or causes some other damage to the aircraft, places or carries into the aircraft an explosive or other device or substance capable of destroying or damaging the aircraft, gives false information regarding the flight of the aircraft, performs violence against the aircraft crew members or commits some other act of violence, endangering thereby the safety of the flight" will be punished for the criminal offence of endangering the safety of international air traffic and maritime navigation.[44]

As it can be seen, Croatian substantive criminal law has corresponded, to a great extent, to relevant international treaties. However, despite the extensive normative framework described,[45] with a view to full harmonization of the Croatian legislation with corresponding international legal documents for combating terrorism, and notably with the *acquis communautaire*, it was necessary to amend some incriminating provisions or to specify new criminal acts in the CC. This was done through the Law on the Amendments of the Criminal Code in 2003.[46] These amendments refer to a standard definition of terrorism, association into a terrorist group, the incrimination of preparatory actions preceding the perpetration of terrorist criminal acts, as well as to financing of terrorist activities. Although there is no single definition of terrorism in the CC, the legislator has enacted two different counter-terrorism provisions with the purpose to separately protect foreign countries and international

[41] According to article 3.1 of the Unlawful Seizure Convention an aircraft is considered to be in flight "at any time from the moment when all its external doors are closed following embarkation until the moment when any such door is opened for disembarkation. In the case of a forced landing, the flight shall be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board".

[42] Supra note 28, article 179. par. 1.

[43] Ibid. par. 2. and 3.

[44] Supra note 28, article 181.

[45] In the Croatian legal system, legal persons can also be held liable for all terrorism-related criminal offences. Because the Law on the Responsibility of Legal Persons for Criminal Offences does not contain a closed list (*numerus clausus*) of criminal offences for which legal entities can be legally responsible, it thus allows the initiation and carrying out of prosecution against legal entities for all criminal offences including those with elements of international terrorism. A list of possible sentences includes: fine, termination of the legal entity, parole sentence, and security measures (a ban on conducting certain activities or business affairs, a ban on acquiring permissions, authorizations, concessions or subventions, a ban on conducting business with users of a state or a local budget, and confiscation of items).

[46] Official Gazette No. 111/2003.

organizations (international terrorism) and its own population and institutions (domestic terrorism or counter-state terrorism). The criminal offence of international terrorism is provided in article 169. of the CC. It foresees that imprisonment for not less than 5 years will be sentenced for "whoever aims to cause major fear among the population, to force foreign states or international organizations to do or not do something or to suffer, or who aims to seriously jeopardize the fundamental constitutional, political or economic values of a foreign state or an international organization, and who commits a criminal offence referred to in Articles 170 through 172, and Articles 179 and 181 (all the criminal offences laid down in UN counter-terrorist conventions), as well as who causes an explosion or fire, or by a generally perilous act or means creates a dangerous situation for people or property, who kidnaps a person or commits another violent act which can seriously harm a foreign state or an international organization".[47] Milder punishment is foreseen for those perpetrators who seriously threaten to commit one of the criminal offences listed above (imprisonment from 1 to 5 years).[48] An aggravated form of this criminal offence is provided in paras. 3 and 4. Paragraph 3 describes a specific form of aggravated murder: "If the perpetrator, when carrying out a criminal act referred to in paragraph 1 of this Article, intentionally kills one or more persons, he/she shall be sentenced to a minimum ten year or long-term imprisonment (up to forty years)".[49] Paragraph 4 states that "If by a criminal act referred to in paragraph 1 of this Article the death of one or more persons or extensive destruction is caused, the perpetrator shall be sentenced to a minimum of ten year imprisonment".[50] In addition to the criminal offence of international terrorism, article 141 of the CC defines the criminal offence of counter-state terrorism. It reads as follows: "Whoever, with the aim to endanger the constitutional order or the security of the Republic of Croatia, causes an explosion, fire, or by a generally dangerous act or device imperils the lives of people, endangers property, kidnaps a person, or commits some other act of violence within the territory of the Republic of Croatia or against its citizens, thus causing a feeling of personal insecurity to citizens, shall be punished by imprisonment for no less than five years".[51]

Other terrorism-related criminal offences provided in the CC are the following: association for the purpose of committing criminal offences against values protected by international law (art. 187) and subsequent assistance to the perpetrator of a criminal offence against values protected by international law (art. 187b). Responsible under article 187. of the CC is whoever organizes a group of people or in some other way joins three or more persons in common action for the purpose of, inter alia, committing terrorism-related criminal offences.[52] Apart from the organizer, who can

[47] Supra note 28, article 169. par. 1.

[48] Ibid. par. 2.

[49] Ibid. par. 3.

[50] Ibid. par. 4.

[51] Supra note 28, article 141. par. 1.

[52] Supra note 28, article 187. par. 1.

be deprived of his/her liberty for no less than 3 years, imprisonment from 6 months up to 5 years can be imposed on whoever becomes a member of such a group. However, an organizer who, by timely uncovering the group, prevents the perpetration of the criminal offences shall be punished by imprisonment from 6 months to 3 years, but the punishment may also be remitted.[53] The punishment shall be remitted for a member of the group who uncovers the group prior to having committed the criminal offence.[54] For subsequent assistance (art. 187b) shall be responsible whoever conceals the perpetrator, inter alia, of a terrorism-related criminal offence, or who provides them with food, clothing, money, or takes care of them in another way in order to make their detection or arrest difficult.[55] Provision incriminating terrorist financing can also be found in the CC. It has been adopted for the implementation of the International Convention for the Suppression of the Financing of Terrorism. According to article 187a par. 2, responsible is anyone who "procures or collects funds knowing that these will be used in order to carry out a criminal offence of international terrorism and/or other related criminal offences".[56] Apart from this criminal offence, other counter-terrorism financing provisions in Croatia are contained in numerous laws such as the Law on Prevention of Money Laundering, the Law on the Office for the Suppression of Corruption and Organized Crime, the Criminal Procedure Act, etc.

For the sake of more efficient prosecution, in all cases of the aforementioned terrorism-related criminal offences, so-called special investigative measures provided by the Criminal Procedure Act can be applied.[57] These are measures used to temporarily limit certain constitutional rights and freedoms of citizens for the purpose of criminal proceedings. If a criminal investigation cannot be conducted in any other manner or would otherwise encounter significant difficulties, on the request of the public prosecutor, an investigating judge (investigation in criminal cases is conducted by investigating judge of the court having jurisdiction on the motion of the authorized prosecutor/State Attorney or injured person as a private prosecutor) may order measures against a person that temporarily limit certain constitutional citizens' rights if there is a well-founded suspicion that they committed a criminal offence alone or participated in a criminal offence together with other persons. The following measures can be taken:

1. Surveillance and technical recording of telephone conversations and other means of long-distance technical communication
2. Entry into premises in order to carry out the surveillance and technical recording of premises
3. Secret surveillance and technical recording of persons and objects

[53] Ibid. par. 3.

[54] Ibid. par. 4.

[55] Supra note 28, article 187b.

[56] Supra note 28, article 187a par. 2.

[57] Criminal Procedure Act, Official Gazette 110/97, 27/98, 58/99, 112/99, 58/02, 143/02, 62/03, and 115/06.

4. Use of undercover investigators and informers
5. Simulated purchase of objects and simulated giving and receipt of bribes
6. Supervised transport and delivery of objects related to a criminal offence

10.3 Public Provocation to Commit a Criminal Offence (Art. 5 of the CECPT) and Croatian Substantive Criminal Law

The United Nations Security Council in its Resolution 1624 has called on states to adopt "such measures as may be necessary and appropriate and in accordance with their obligations under international law to prohibit by law incitement to commit a terrorist act or acts".[58]

The rationale for this newly created antiterrorist standard was to fill the gap in the provisions of the existing United Nations antiterrorist conventions. Namely, the state parties to these international treaties have been under the legal obligation to incriminate direct perpetration of the respective criminal offence[59] (for instance terrorist bombings or hostage taking) but also complicity in the commission of these criminal offences[60] and other forms of participation (for instance organizing and directing others to commit a criminal offence,[61] contributing to the commission by a group of persons acting with a common purpose, etc.). Apart from direct perpetration and ancillary offences, the aforementioned conventions are silent when it comes to the criminalization of the incitement to commit a terrorist act. Although Resolution 1624 does not make any specific reference to the fact whether "incitement" should be direct and/or indirect, it is quite apparent that it goes further than requiring criminalization of mere direct incitement, which has been already punishable in most if not all legal systems. Furthermore, the very reason for the adoption of this Resolution was the universal condemnation of all of the forms and manifestations of the encouragement, glorification, and apology of terrorism, which might be the trigger of the future terrorist attacks.

On the European level, public provocation to commit terrorism-related criminal offence has been established by article 5. of the Council of Europe Convention on Prevention of Terrorism (CECPT).[62] Article 5 par. 1 of the CECPT defines this as

[58] S/RES/1624 (2005), 14 September 2005, at 1.a.

[59] See article 2.3.(a) of the Terrorist Bombings Convention, article 2.4.(a) of the Nuclear Terrorism Convention.

[60] See article 2.3.(b) of the Terrorist Bombings Convention, article 2.4.(b) of the Nuclear Terrorism Convention.

[61] See article 2.3.(c) of the Terrorist Bombings Convention, article 2.4.(c) of the Nuclear Terrorism Convention.

[62] Council of Europe Convention on Prevention of Terrorism, CETS, No 196, http://conventions.coe.int., article 5.

"intentionally distributing[63] a message to the public,[64] with the intent to incite the commission of a "terrorist offence", where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more terrorist offences may be committed".[65] Pursuant to article 5 par. 2 of the CECPT, "each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law".[66]

The need for the development of a new terrorism-related criminal offence was the subject of extensive debate in the Council of Europe Committee of Experts against Terrorism, the expert committee entrusted with, inter alia, the drafting of the CECPT. Given the fact that the concept of the public provocation has been very closely related to freedom of expression protected under article 10[67] of the Council of Europe Convention on Protection of Human Rights and Fundamental Freedoms (HRC), the main concern expressed in the debate was how to incriminate "distributing a message to the public" without infringement of this fundamental human right. It was very difficult to address this issue and to find the appropriate balance between the positive obligation of states to protect citizens from terrorism and to respect their rights emerging from article 10 of the HRC, because the freedom of expression clause does not relate only to "'information' or 'ideas' that are favorably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population".[68] However, the Committee came to the correct conclusion that

[63] The term "distribution" refers to the active dissemination of a message advocating terrorism, while the expression "making available" refers to providing that message in a way that is easily accessible to the public, for instance, by placing it on the Internet or by creating or compiling hyperlinks in order to facilitate access to it. Council of Europe Convention on Prevention of Terrorism, Explanatory Report, par. 102.

[64] The term "to the public" makes it clear that private communications fall outside the scope of this provision. In order to make a message available to the public, a variety of means and techniques may be used. For instance, printed publications or speeches delivered at places accessible to others, the use of mass media or electronic facilities, in particular the Internet, which provides for the dissemination of messages by e-mail or for possibilities such as the exchange of materials in chat rooms, newsgroups, or discussion fora. Ibid. par. 103. and 104.

[65] Supra note 62.

[66] Ibid. par. 2.

[67] Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.: 005, available at http://conventions.coe.int, last visited 25 March 2008. Article 10 ECHR reads: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises".

[68] Handyside v. United Kingdom, 7 December 1976, par. 49.

freedom of expression is not an absolute right and, as such, it may be restricted[69] in certain specific circumstances.[70] In other words, the new criminal offence of public provocation to commit terrorism-related criminal offences is not contrary to article 10 of the HRC because the incitement to violence (including terrorist violence) does not enjoy protection under the freedom of expression clause. As a result of this conclusion, CODEXTER introduced the so-called freedom of expression clause, a provision that cannot be found in previous antiterrorist conventions. Pursuant to article 12 of the CECPT, state parties have to ensure that the establishment, implementation, and application of criminalization under, inter alia, article 5 of the CECPT "are carried out while respecting human rights obligations, in particular the right to freedom of expression, freedom of association and freedom of religion, as set forth in, where applicable to that Party, the Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, and other obligations under international law".[71] In addition, the establishment, implementation, and application of the criminalization under article 5 should furthermore "be subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, and should exclude any form of arbitrariness or discriminatory or racist treatment".[72]

Because the Republic of Croatia is a party to the CECPT, I will now turn to the issue of whether its substantive criminal law provisions are in line with this international treaty. According to the Croatian Criminal code, the direct provocation to commit a criminal offence (including terrorism-related criminal offence) falls under the instigation clause. Whoever intentionally instigates another to commit a criminal offence shall be punished as if he himself committed it.[73] Notwithstanding the fact that instigation as a form of accomplice liability is accessorial to the *actus reus* of the principal perpetrator (according to the so-called limited accessorial theory), in some cases (and it would include all terrorism-related offences) the instigator will be punished even if the principal perpetrator has not even attempted to commit the respective criminal offence. Given the fact that the instigator is the "spiritual father" of the crime because of his conclusive influence on the principal perpetrator's will, he deserves to be punished even in cases of so-called unsuccessful

[69] "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary". Supra note 67, article 10. par. 2.

[70] Background Paper on Human Rights Considerations in Combating Incitement to Terrorism and Related Offences, OSCE/CoE Expert Workshop, Vienna, 2006, p. 5.

[71] Supra note 62, article 12. par. 1.

[72] Ibid. par. 2.

[73] Supra note 28, article 37.

attempts. Instigation is always exerting conclusive influence on a specific person to commit a specific criminal offence. It means that public provocation in the form of distributing a message to the public with the intent to incite the commission of a "terrorist offence", whatever the content of this message may be, would fall outside the scope of article 37 of the CC. For this reason, the domestic antiterrorist normative framework must be supplemented with a new criminal offence of public provocation to commit a terrorism-related criminal offence. Of course, this would not be an easy task, taking into account the difficulties other state parties have been faced with in drafting the respective criminal offence. The Explanatory Report to the CECPT must be used as a guideline in determining the scope of criminalization. Besides, the jurisprudence of the European Court of Human Rights concerning article 10 of the HRC must also be taken into due account not only in drafting the respective criminal offence but in its implementation and application as well. In the Explanatory Report to the CECPT, it was stressed that "presenting a terrorist offence as necessary and justified may constitute the offence of indirect incitement".[74] However, as it was underlined in the Explanatory Report, its application "requires that two conditions be met: first, there has to be a specific intent to incite the commission of a terrorist offence, which is supplemented with the requirements that provocation be committed unlawfully and intentionally; and second, the result of such an act must be to cause a danger that such an offence might be committed".[75] Regarding the first condition, it must be observed that some member states in their domestic antiterrorism laws disregarded this *mens rea* requirement. For instance, section 1 of the British Terrorism Act prohibits the publishing of "a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism or Convention offences".[76] It is quite obvious that the *mens rea* element established in article 5 of the CECPT was not followed in the drafting of the section 1 of the British Terrorism Act. This omission has extremely extended the scope of the public provocation (encouragement to terrorism) that is, in my opinion, an evident disregard of article 5 of the CECPT. Moreover, the vague language of the aforementioned provision puts the fundamental human rights protected under article 10 of the HRC under direct risk. Therefore, it is true, as one author correctly pointed out, that "the Government's resistance to the inclusion of the requirement of intention is somewhat two-faced, given that the reason offered for creating the offence was the need to comply with Article 5 of the Council of Europe Convention on the Prevention of Terrorism which expressly requires specific intent".[77] Unlike the British Terrorism

[74] Supra note 63, par. 98.

[75] Supra note 63, par. 99 and 100.

[76] Terrorism Act 2006, available at http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en_1, last visited 25 March 2008.

[77] Hunt A., Criminal Prohibitions on Direct and Indirect Encouragement of Terrorism (2007) Criminal Law Review. 441.

Act, the Draft Amendments to the Criminal Code of Bosnia and Herzegovina (unofficial version available to the author) fully comply with the *mens rea* requirement established by article 5 of the CECPT. According to article 202a, which criminalizes public instigation to terrorist activities, the perpetrator is whoever, through the public service, distributes or in any other way directs messages to the public, with the aim to instigate another to commit a criminal offence. Nevertheless, the weak point of this provision is the absence of the result (consequence) of the provocation, that is, the danger caused that such an offence might be committed. This obvious departure from the treaty language also extends the scope of criminalization of the public provocation to commit a terrorism-related criminal offence. It means that the draft article 202a as it now stands would not require the prosecution to prove that the *actus reus* of the perpetrator acting with intention to instigate another to commit criminal offence caused the danger[78] of the commission of the respective offence. The *actus reus* of the perpetrator acting with above-described intention will suffice. Such reduction of the elements of the offence does not comply with the CECPT because state parties are not allowed to go beyond the scope of article 5, which should be read together with article 12.

Prosecution and punishment of those liable for public provocation to commit terrorism-related criminal offence is a positive obligation of states. In this respect, a certain amount of discretion has been left to them to find the aforementioned "optimal path". However, this discretion, no matter how broad it could seem, is not unlimited. All those in charge of the implementation of article 5 of the CECPT must not disregard the basic requirements set out not only in this article, but in article 12 as well. This means that criminal offence of public provocation to commit a terrorist act in domestic law should be composed, inter alia, of at least three safe-guarding elements:

- Detailed determination of conduct that constitutes the public provocation to commit a terrorist offence
- Inclusion of the perpetrator's intention to incite the commission of a terrorist offence
- Causal link requirement between provocation and the preparation/commission of a terrorist offence

10.4 Conclusion

Croatia joined the antiterrorist coalition soon after it was created, expressing its commitment to accept all relevant international antiterrorist standards. Its clear position on the fight against international terrorism while preserving fundamental

[78] "When considering whether such danger is caused, the nature of the author and of the addressee of the message, as well as the context in which the offence is committed shall be taken into account in the sense established by the case-law of the European Court of Human Rights. The significance and the credible nature of the danger should be considered when applying this provision in accordance with the requirements of domestic law". Supra note 63, par. 100.

human rights was reflected in the Report of the Republic of Croatia pursuant to paragraph 6 of Security Council resolution 1373 (2001) of 28 September 2001. In this document, the Government firmly rejected any collective responsibility for international terrorism, as well as any identification of terrorist groups with any nation or religious or ethnic community. As a party to all 13 UN antiterrorist conventions and actively contributing in filling the gap that exists in the international legal framework concerning the fight against international terrorism, the Republic of Croatia has been persistent in calling upon UN member states to speed up the finalization of negotiations on Draft Comprehensive United Nations Convention on International Terrorism. At the same time, apart from its active role within worldwide antiterrorist coalition strengthened after 11 September 2001, wrong perception of terrorism as a significant but "far threat", not only in the general public but among the political elite as well, has led to a situation that no significant development has been made on the prevention of the terrorism domestically. In other words, terrorism has been perceived as a threat to others, destruction that takes place elsewhere and that is not a major threat to the fundamental values of our society. Such an approach has been reflected, inter alia, in public speeches given by some high public officials, who stressed not only that Croatia is not among potential targets of terrorist attacks, but that it could not become such a target. This diversion between formal accepting of international antiterrorist standards and misperception of terrorism as not only potential but a real threat to any country, does not have support on the ground. The need for a proactive approach in prevention of terrorism domestically derives from the political and social reality of the contemporary Croatian society and its neighbourhood (the similarity between hate crimes and terrorism in territories occupied in aggression and war against Croatia in the early 1990s, the Kosovo crisis, etc.). From this perspective, the need to have a comprehensive antiterrorist strategy based on prevention (cultural dialog, promotion of human rights, protection of minorities, etc.) is undisputable as far as the described situation in the region exists. At the same time, there is an urgent need to comply with all standards (security, human rights, especially rights of minorities) as a condition for the accession to the EU and NATO.

When it comes to the substantive criminal law, overlapping between the elements of some criminal offences might cause serious problems in criminal prosecution of perpetrators of the terrorism-related criminal offences. For instance, the aforementioned similarity between criminal offences of counter-state terrorism (or domestic terrorism) and international terrorism could cause some problems not only in international legal cooperation (for instance identity of norm requirement), but in domestic criminal prosecution as well, especially when it comes to the activities of the police in determining the legal qualification of the criminal offence. This is exactly what happened after the car bomb terrorist attack that took place in front of police headquarters in Rijeka in 1995. Due to the fact that perpetrator was a foreign citizen, this attack was legally qualified as an international terrorism, notwithstanding the fact it that was clear example of counter-state terrorism, i.e. the attack directed against the Republic of Croatia (as retaliation of *al-Gama'a al-Islamiyya*, who claimed responsibility for the attack as an answer to the alleged

involvement of the Croatian authorities in the rendition of their spokesman *Talaat Fouad Qassem* to the United States). Such confusion could easily be avoided by incriminating a single terrorist criminal offence. This would be in line with the Council of European Union's Framework Decision on Combating Terrorism (13 June 2002), as well as with suggestions put forward by the European Commission during the negotiations with the Croatian Government in chapter 24 of the *acquis*. Integration of the criminal offence of "public provocation", which is elaborated in this chapter as well as other incriminations that fall under the label of the so called pre-emptive criminal law (recruitment for terrorism, training of terrorists) in domestic substantive criminal law is one of the major challenges ahead of Croatian legislator. Because this is not a technical but rather a substantial issue raising some very serious human rights concerns (freedom of expression, association, etc.), it must be submitted to all relevant experts (not only lawyers) for thorough discussion. This is the only way to find an appropriate balance between the positive obligation of the state to protect everyone within its borders from terrorism and its obligation to protect and promote fundamental human rights and freedoms. In looking for this "optimal path", at least three safe-guarding elements mentioned earlier in the text (see Chap. 3.) must be observed. In addition, serious consideration must be given to the drafting and implementation experiences of other states.

References

A. Books and Articles

Becker S. (2003). "Mirror, Mirror on the Wall…", Assessing the Aftermath of September 11th, Valparaiso University Law Review 37, 563

Cassese A. (2001). Terrorism is Also Disrupting Some Crucial Legal Categories of International Law, European Journal of International Law 12, 995

Hunt A. (2007). Criminal Prohibitions on Direct and Indirect Encouragement of Terrorism, Criminal Law Review 441

Laqueur W. (1998). The New Terrorism - Fanatism and the Arms of Mass Destruction, London: Phoenix

B. Other

Background Paper on Human Rights Considerations in Combating Incitement to Terrorism and Related Offences, OSCE/CoE Expert Workshop, Vienna, 2006

Committee of Experts on Terrorism (CODEXTER), Profiles on Counter-Terrorist Capacity - Croatia, June 2006, available at http://www.coe.int/gmt

Constitution of the Republic of Croatia, Official Gazette 56/90., 135/97., 8/98., 113/00., 124/00., 28/01

Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.: 005, available at http://conventions.coe.int

Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971

Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988
Convention for the Suppression of Unlawful Seizure of Aircraft, 1970
Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1963
Convention on the Marking of Plastic Explosives for the Purpose of Detection, 1991
Convention on the Physical Protection of Nuclear Material, 1980
Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, 1973
Council of Europe Convention on Prevention of Terrorism, Explanatory Report, available at http://www.coe.int/gmt
Council of Europe Convention on the Prevention of Terrorism, 2005
Counter-Terrorist Committee, available at http://www.un.org/sc/ctc/
Criminal Code, Official Gazette 110/97., 27/98., 50/00., 129/00., 51/01., 111/03., 190/03., 105/04., 84/05., 71/06. and 110/07
Criminal Procedure Act, Official Gazette 110/97., 27/98., 58/99., 112/99., 58/02., 143/02., 62/03. and 115/06
European Convention on the Suppression of Terrorism, 1977
Handyside v. United Kingdom, 7 December 1976, available at http://echr.coe.int
Human Rights and the fight against terrorism, The Council of Europe Guidelines, available at http://www.coe.int/
International Convention Against the Taking of Hostages, 1979
International Convention for the Suppression of Acts of Nuclear Terrorism, 2005
International Convention for the Suppression of Terrorist Bombings, 1997
International Convention for the Suppression of the Financing of Terrorism, 1999
Law on the Responsibility of Legal Persons for Criminal Offences, Official Gazette 151/03
Legislative Guide to the Universal Anti-Terrorism Conventions and Protocols, United Nations, Office for Drugs and Crime, 2004
Protocol amending the European Convention on the Suppression of Terrorism, 2003
Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Montreal, 1988
Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, 1988
Report of the Republic of Croatia pursuant to paragraph 6 of Security Council Resolution
S/RES/1373 (2001), 28 September 2001
S/RES/1267 (1999), 15 October 1999
S/RES/1624 (2005), 14 September 2005
Terrorism Act 2006, available at http://www.opsi.gov.uk/

Chapter 11
Muslims Communities and Counterterrorism: The Dynamics of Exclusion and Possibilities of Inclusion

Tufyal Choudhury

11.1 Introduction

Muslim communities in the UK have come under increasing state and public scrutiny since the terrorist attacks of 11 September 2001. This intensified after the bombings in London in July 2005 and the rapid rise in the number of arrests and conviction of individuals in relation to plans for and attempts at further attacks. Newspapers, polling organisations, and think tanks have interrogated and examined the views, attitudes, practices, and experiences of Muslims living in Britain. The potential for mass slaughter from a terrorist bombing has meant increased support for measures that may prevent future attacks at the earliest stage possible. The former British Prime Minister, Tony Blair defended proposals for a national identity card scheme as an important weapon in their counterterrorism armoury (Blair 2006). Security services are monitoring over 2000 people in Britain that are believed to pose a direct threat to the country's national security and public safety (Norton-Taylor 2007a). New laws passed since 2001 allow stops and arrests to disrupt plots at increasingly earlier points while speech that indirectly incites terrorism is prohibited in order to disrupt radicalisation and terrorist recruitment. The involvement of second generation British born Muslims in the 7 July 2005 attacks and among those that have been arrested and currently face trial on terrorism related charges is viewed by some as evidence of the failure of Muslim integration and the policy of "multiculturalism." The latter is blamed for placing emphasis on state engagement with citizens on the basis of their ethnic and religious identities at the expense of a common British civic citizenship. While placing Muslims under this intense scrutiny, passing anti-terror laws opposed by Muslim organisations, and criticising past policies for placing too much emphasis on cultural and religious difference, the government is nevertheless attempting to engage with Muslim communities

T. Choudhury (✉)
Durham University, Durham, UK
e-mail: t.a.choudhury@durham.ac.uk

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_11,

and views such engagement as an important part of its counterterrorism policy (Department for Communities and Local Government 2007).

This chapter focuses on the role and impact of the British government's counterterrorism policies, including its anti-terrorism laws, on Muslim communities in the UK. It places the impact of such policies in the context of the experience of Muslims who, as a group, already exist at the margins of British society. It identifies aspects of current policies that threaten to intensify and reinforce existing processes of socio-economic exclusion and cultural marginalisation which in turn feed into processes of radicalisation. It is suggested that the government's policy of supporting Muslim communities and organisations in addressing violent extremism runs the risk of reinforcing public perception that domestic terrorism as a "Muslim problem." By appearing to place the onus of responsibility for tackling terrorism on Muslims, it creates the risk that Muslims as a group will be held responsible for failures to prevent future attacks. At the same time, the process and nature of the engagement with Muslim groups and organisations that has occurred threatens to reinforce Muslim perceptions and experiences of marginalisation and discrimination.

Furthermore, the enactment of new laws that create broader and wider criminal offences and give police more powers create large areas of executive discretion. In the absence of sufficient trust between Muslims and state agencies, the opaque exercise of such discretion reinforces perceptions of discrimination, Islamophobia and racism in the actions of state agencies. Aspects of counterterrorism policy may therefore contribute to a sense of being treated as a "suspect community" among Muslims, which in turn impacts on the risks of radicalisation. In other words, policies aimed at tackling terrorism may in fact be increasing the risks of another attack because of the way they impact on Muslims communities.

An attempt at evaluating the impact of counterterrorism policies on Muslim communities needs to begin, however, by considering the difficulties involved in talking about the impact of legislation and policies on "the Muslim community," and the pitfalls for counterterrorism policy in viewing Muslims as forming a monolithic single community.

11.2 Diversity of the Muslims in the UK

According to the 2001 census, there are just over 1.5 million Muslims in the UK. They constitute 3 per cent of the British population and as the largest minority faith group, account for over half the non-Christian religious population. Notwithstanding these figures, Muslims in the UK are not a single homogenous community. Understanding this is critical to any attempt to assess the differing impacts of counterterrorism policies on Muslim communities across Britain. This begins with an appreciation of the differing migration routes and settlement patterns of different Muslim groups.

Muslims first arrived in Britain over 300 years ago. Coming as sailors – from South Asia with the British East India Company and from Yemen after the opening

of Suez – they first settled around the port cities of London, Cardiff, Liverpool, Hull, and South Shields (Ansari 2004). In the post-war period, migrants from the new Commonwealth came to fill shortages in the labour market. Significantly, a large part of Pakistani migration to Britain was from the villagers displaced by the building of the Mangla Dam in Mirpur, an area on the Pakistani side of the disputed region of Kashmir. Such direct links to an area of Pakistan from where networks of militant groups operate appears to have played an important role in the training and radicalisation of the 7 July bombers (Intelligence and Security Committee 2006). Most South Asians arrived as unskilled labour migrants to work the mills and factories in the industrial areas of the West Midlands and the north west of England.

Britain reacted to the large-scale non-White migration from the Commonwealth by increasing restrictions on opportunities for immigration. Ironically, the increased restriction provided the impetus for these labour migrants' to begin the process of settlement and initiate family reunification in the UK. For Pakistanis this began in the 1970s, but for the Bangladeshi population, this occurred in significant numbers much later in the 1980s. Thus, families, wives and children, joined the men just at the point at which the factories in which the men worked began to close as part of the long-term economic restructuring of the British economy away from manufacturing towards service sector jobs.

The unskilled labour migrants began to be joined in the late 1960s and early 1970s by East African-Asians, arriving under pressure from the "Africanisation" policies in Kenya and Tanzania, and in the case of Uganda, as a result of forced expulsion (Hansen 2000). The East African-Asians were highly skilled urban middle-class professionals and entrepreneurs and tended to settle in London and the East Midlands. Most importantly, in terms of social inclusion, the experience that this group had of living in urban centres combined with their business and professional background ensured faster integration into economic and social structures. It is estimated that 20,000 of the group of 150,000 East African-Asians were Muslims, mainly Ismaili Shias, with family roots in Pakistan or the Indian state of Gujarat (The Runnymede Trust 1997).

While Muslims from South Asia constitute 68 per cent of the Muslim population in the UK, there are other significant Muslim populations in Britain. There are, for example, estimated to be around 120,000 Turkish Cypriots and 80,000 mainland Turkish and Kurdish people in the UK (Enneli et al. 2005). These three groups, while connected, have very different migration histories. The earliest to settle in the UK were the Turkish Cypriots. Tensions between Turkish and Greek communities in Cyprus created pressure for migration in the early 1960s. Migration of Turkish workmen from Turkey started from the late 1960s and early 1970s and family reunions began in the late 1970s (Ali 2001). Finally, Kurds arrived mainly as political refugees in the late 1980s and early 1990s. Muslims arriving in Britain from the Middle East have more diverse national and class backgrounds (El-Sohl 1992). Oil wealth combined with political instability in the Middle East attracted investors and professionals from the Middle East from the 1970s onwards.

Until the late-1980s, Muslims arrived in the UK mainly as economic or family migrants. In the course of the 1980s and 1990s, increasing numbers of Muslims arrived

as refugees seeking asylum. Following the steady disintegration of the former Republic of Yugoslavia, this included large numbers of Bosnian and then Kosovar Muslims. Arabs, Afghans, Kurds, North African, and Somalis formed a significant proportion of those seeking asylum in Britain. One estimate places the size of the UK Afghan community at around 70,000 (Leigh 2007). Some were political activists who maintained transnational political ties, including activists from Islamic organisations that were banned in the Middle East and North Africa. It was in this period that key figures involved in the subsequent radicalisation of young people in Britain, such as Omar Bakri Mohammed[1] and Abu Qatada,[2] arrived in the UK seeking asylum. This link between refugees and those involved in radicalisation has led to increasing public hostility towards refugees and new migrants (Crawley 2005). Given their already insecure and precarious status, a refugees and asylum seeker's experience of state counterterrorism policies is significantly different from that of Muslims who are British citizens (Rudiger 2007). This was most clearly signified by the distinction made in the Anti-Terrorism Crime and Security Act 2001 between the treatment of UK and foreign nationals relation to detention without trial.

While Muslims make up only 3 per cent of the UK population, their concentration in specific neighbourhoods and cities ensures that policing operations and practices in particular local areas have a disproportionate impact and reach into Muslim communities. Around two-fifths of Muslims in the UK (38 per cent) live in London, where they make up 8.5 per cent of the population. After London, the regions with the largest share of the Muslim population were the West Midlands (14 per cent), North West (13 per cent), and Yorkshire and Humber (12 per cent). Even within these regions, Muslims are highly concentrated spatially.

Furthermore, people's experiences and perceptions of policing are mediated by their, age, ethnicity, gender, and socio-economic position. Here the ways in which the demographic profile of the Muslim population in the UK differs from that of the general population are relevant. In relation to age, Muslims have the youngest demographic profile of any faith group in England and Wales. Over 60 per cent of all Muslims are under the age of 30. Muslims in Britain are also ethnically diverse. Three quarters of Muslims (74 per cent) are from an Asian ethnic background, predominantly Pakistani (43 per cent), Bangladeshi (16 per cent), Indian (8 per cent), and other Asian (6 per cent). There are almost 1.2 million Asian Muslims living in Great Britain in 2001. One in ten Muslims (11 per cent) are from a White ethnic group, 4 per cent are of White British origin, and 7 per cent from another White background including Turkish, Cypriot, Arab, and Eastern European. A further 6 per cent of Muslims are of Black African origin, mainly from North and East

[1]Omar Barki Mohammed sought asylum after arriving in the UK in 1986, and was subsequently granted indefinite leave to remain. He initially headed the radical Muslim organisation Hizb-ut-Tahrir and then set up a offshoot Al-Muhajiroun.

[2]Abu Qatada claimed asylum in 1994. He is said to have influenced Richard Reid and Zacarias Moussaoui, both convicted of offences related to terrorism. Qatada was placed under a control order in June 2008 after attempts to extradite him to Jordan were blocked by the Court of Appeal in England (*see*: http://news.bbc.co.uk/1/hi/uk/7459773.stm).

Africa, particularly Somalia. There are also estimated to be 5,000–10,000 Muslim converts, half of whom are from the African Caribbean community (Commission on British Muslims and Islamophobia 1997). This ethnic diversity is important to keep in mind when examining data on police stop and search. Data for this is broken down by broad racial groups of Black, White, and Asian. This therefore does not provide any indication of whether Muslims are over-represented in the number of people being stopped and searched. For example, Turkish, Arab, and North African Muslims may be classified as "White" within such statistics. The ethnic background of Muslim may also be important in shaping their interpretation of everyday experiences of racism and discrimination that different groups experience. The stereotypes and prejudices that structure the discrimination that a Black African or Black Caribbean Muslim will encounter will be different from that for a Bosnian, Turkish, Pakistani, or White British Muslim.

The British Muslim population is religiously diverse, covering a wide and broad range of religious traditions within both the Sunni and Shia traditions. It also covers a broad range of adherence and practice. This diversity in traditions and practice means that for the vast majority of Muslims, their understanding of and ability to challenge those Muslims who advocate ideologies that support or justify suicide bombings may be no better than that of the general population (Spalek and Lambert 2007). The lack of contact between most Muslims and extremists is highlighted in the response by Muslims to a YouGov poll in 2005. Forty seven per cent of Muslims in the poll believed that radicalising Imams existed. At the same time 69 per cent had never come across one, whereas 22 per cent had heard one once or twice and only 5 per cent reported coming across them frequently.

The extent to which a person is visibly identifiable as a Muslim shapes their experiences of life in the UK, with most research suggesting that the greatest public hostility and prejudice is directed towards those that are visibly identifiable as or perceived to be Muslim, including non-Muslims such as Sikhs wearing turbans (Sheridan and Gillett 2005; Ameli et al. 2004).

The importance of religion to the identity of Muslims has become clear in research since the 1990s (Modood et al. 1997). The 2001 Home Office Citizenship survey confirmed that, for Muslims as a group, religion was the second most important factor in describing themselves. For Christians, by contrast, religion ranked seventh (O'Beirne 2004). The primacy given by Muslims to family and kinship ties over religion is also an important reminder of the limits to the influence and reach of faith institutions and leaders engaged in supporting counterterrorism policies (Innes et al. 2007).

The importance of religion in the identity of many Muslims means that this is nevertheless likely to influence their experiences of and responses to policing practices and counterterrorism policy. Religion becomes a more salient and important marker of identity in response to experiences of discrimination (Ballard 1996). This would suggest that experiences of state repression and perceptions that Muslims are being treated as a suspect community and targeted by police because of their religion will increase in-group solidarity and identification with their religious identity. Creating such increasing group identification could be a cause for concern among

policymakers given that some groups use Muslim identity as a way to challenge the possibility of integration and to create an identity in opposition to British and European identity and values (Wictorowicz 2005). In the context of Muslims in France, Olivier Roy notes that the second and third generation have "recast their feeling of being excluded by importing a psychological frontier to their spaces of social exclusion in suburbs and inner cities. In this context, Islam becomes the 'otherness' of Europe" and an alternative identity for youngsters in search of a reactive identity (Roy 2004: 45).

Concern that the increasing importance of religion to the identity of Muslims may have a negative impact on integration needs, however, to be balanced against increasing evidence suggesting that religious identity plays a positive role for young second generation Muslims in Britain. A Muslim identity and Islamic discourse can be an empowering experience for young British Muslims in allowing them to critique and challenge the cultural practices of their parents (Khokher 1993; Jacobson 1997; Dywer 1999a, 1999b, 1997). Archer's (2003) study of young Muslim men suggests that a strong Muslim identity provides a positive role model as an alternative identity that they can have pride in, in contrast to the ethnic "Asian" identity of their parents (who are seen as economically weak and disempowered) and as an alternative to the gang and drug cultures of the "street." Modood (2006) also suggests that, for Muslims, religion has a positive role in encouraging and supporting educational aspirations. He argues that Islam in Britain is "finely poised between a religion of a ghetto and a religion of social mobility – a kind of 'Protestant ethic' – capable of sustaining the hope and discipline that the taking up of opportunities requires." He believes that "for the latter trajectory to be actualised, mainstream Islam requires encouragement not demonisation" (Modood 2006: 250). The danger remains that counterterrorism policies contribute to the demonisation of Muslims in public discourse, presenting Muslims and Islam as a threat to society, thereby tipping the balance towards Islam becoming "a religion of a ghetto" rather than "a religion of social mobility."

The identification of Muslims as a threat in counterterrorism policy risks feeding into a public attitude that already appears to be hardening against Muslims. Survey evidence suggests that, for the moment, there remains a majority that continue to be positive in their perceptions and understanding of British Muslims. Abrams and Houston (2006), in a survey before the 2005 London bombings, found that a quarter of respondents said that they sometimes felt prejudiced against Muslims but would not let their prejudice show. Nine per cent said they did not mind if they came across as prejudiced against Muslims. The majority, however, expressed positive (38 per cent) or neutral (43 per cent) feelings towards Muslims. One-third of respondents viewed Muslims as posing a cultural and physical threat to the UK. However, 58 per cent of people did think it was important for society to respond to the needs of Muslims. A majority (66 per cent) of people were supportive to equal employment opportunity measures towards Muslims, whereas 19 per cent thought that such measures had gone too far. An opinion poll survey of over 1,000 adults suggests that by 2006, a majority of people felt that Muslims were viewed with more suspicion by their fellow citizens while at the same time thinking that it was

unacceptable for police to view Muslims with greater suspicion because the 7 July 2005 bombers were Muslim.[3] A greater proportion of people (45 per cent) disagreed with the statement that Islam encourages more violence than other religions compared to those who agreed (30 per cent). A majority, 54 per cent, also disagreed with the statement that Islam is a threat to Britain's way of life. However, three quarters (74 per cent) felt that Muslims needed to do more to integrate into mainstream British culture. By 2007, only 45 per cent of the general public thought Muslims living in the UK are loyal to the nation (Mogahed 2007). An analysis of newspaper coverage of Muslims suggests a shift from stories that view Muslims as a security threat towards perceptions of Muslims as a cultural threat to the British way of life. At the same time, only 2 per cent of stories suggested that Muslims shared or supported society's dominant moral values (Moore et al. 2008). In assessing the impact of such growing hostility, it is important to remember that it is directed towards communities many of whose members already experiences significant social and economic marginalisation.

11.3 Social Marginalisation and Exclusion

The nature and type of Muslim migration that has taken place in Western Europe is significantly different from that of North America. While in the USA and Canada, Muslims prior to 9/11 were generally viewed as well integrated and participating in the socio-economic mainstream, the evidence is clear that in Britain, the majority of Muslims, and in particular Pakistani and Bangladeshis, live at the margins rather than the mainstream of British society. This is important in relation to counterterrorism for two reasons. First, communities and individuals that experience social marginalisation are more likely to be concerned about increased state policing powers:

> …[I]t is not the enhanced police power themselves that are the main source of community concern, but the wider social atmosphere and culture in which they are introduced. In a society where the vast majority of people feel an important and accepted part of a wider community, where inequalities of economic and social opportunity are minimal, and where instances of institutionalised racism and discrimination are rare, the prospects of wider and more coercive police powers are regarded with much less concern. In such instances there is little prospect those disadvantaged and disenfranchised sections of the community will look at such powers as simply hardening the state's capacity to maintain the social status quo by enforcing their marginal status. (Pickering et al. 2008: 39)

Second, any negative impact arising from current counterterrorism policy and practice will increase or reinforce existing experiences of social marginalisation and discrimination rather than create new ones.

Levels of poverty are among the most important indicators of economic and social exclusion. Levels of household income provide the main measure of poverty, with data from the Family Resources Survey used in the research literature to examine

[3] *See* http://www.populuslimited.com/pdf/2006_07_04_Times_ITV_General.pdf

differences between different ethnic groups. Poverty here is defined as being below 60 per cent of the median equivalised income, that is, income taking into account household type. Data from the 2002/03 to 2004/05 Family Resources Survey shows that rates of poverty are particularly high among the Pakistani and Bangladeshi groups even though they experienced a far greater fall in poverty rates than other groups in the ten years between 1994 and 2004: for Bangladeshis, the poverty rate fell from over 81 per cent in 1994 to around 67 per cent in 2004 and for Pakistanis from 70 to 55 per cent (Kenway and Palmer 2007).

Half the poverty rate of Pakistani and Bangladeshi households is accounted for by the family work status. A third of Bangladeshi households and a quarter of Pakistani households have no adult in work. When, however, we look at the gap in the poverty rates between minority ethnic groups and the white group, we find that the most striking ethnic differences are among *working* families rather than *work-less* families. Among those in working families, around 60 per cent of Bangladeshis and 40 per cent of Pakistanis are in income poverty. This is much higher than the 10–15 per cent for White British, White Other, Indians, and Black Caribbeans. Differences in pay rates are the major factor in the difference in income poverty rates once demography and family work status are taken into account (Kenway and Palmer 2007). Low pay means that one-third of Pakistanis and Bangladeshis are reliant on means tested benefits compared with 7 per cent for White households (Berthoud 2002: 7). Income poverty is intensified by asset poverty, so that 82 per cent of Bangladeshi households and 63 per cent of Pakistani households were both income- and asset-poor compared with 30 per cent of White households (Warren and Britton 2003).

Child poverty rates for Pakistani and Bangladeshi households are particularly high. One measure of child poverty is eligibility of children for free school meals (FSM). In 2005, over half of Bangladeshi and a third of Pakistani pupils in secondary school were eligible for FSMs, compared with only 14 per cent of all pupils (Department for Education and Skills 2006). Further analysis shows that even Bangladeshi and Pakistani pupils not entitled to FSM ("non-FSM pupils") live in areas of higher disadvantage than White British non-FSM pupils (DfES 2006). This is consistent with the fact that 70 per cent of Bangladeshi pupils and 60 per cent of Pakistani pupils live in the 20 per cent most deprived neighbourhoods.[4] In fact, over 40 per cent of children in both groups live in the 10 per cent most deprived postcode areas. By contrast, fewer than 20 per cent of White British pupils live in the 20 per cent most deprived postcode areas and 10 per cent in the 10 per cent most deprived postcode areas (DfES 2006).

A second key indictor of social inclusion, particularly economic inclusion, is social class mobility. This can be measured in both absolute and relative terms. In relation to social mobility, the evidence suggests that education has played an important role in the gross social class mobility experienced by Pakistani and

[4]Deprivation here is defined by the Office of Deputy Prime Minister's Index of Multiple Deprivation.

Bangladeshis, along with other minority ethnic groups (Platt 2005). On the contrary, this educational improvement has not resulted in relative social class mobility. In other words, when compared to the first generation, the second generation is improving its social class position through education, but educational improvements are not leading to the same level of social class mobility compared to those from other ethnic groups with similar levels of education. In fact, for Pakistanis and Bangladeshis, Platt finds that when education is taken into account their relative chances of occupational success actually decreases:

> …for these two groups, education is not able to compensate for whatever it is about, or associated with, Pakistani or Bangladeshi ethnicity that results in relative disadvantage. Lower levels of educational success are not able to explain lower chances of professional or managerial class outcomes for these two groups; and they are not achieving the levels of occupational success that not only their origins but also their educational achievements should imply…There seems no obvious explanation for why Pakistanis' and Bangladeshis' education does not at least reduce the impact of ethnicity. Given the important role of education as a route to success, the reasons why it does not "work" for Pakistanis and Bangladeshis, or why it is not used in the same way, warrants further explanation. There may be geographical factors that are not being captured by the area ethnic concentration variable, but it seems unlikely that such additional geographical factors could fully account for this finding. (Platt 2005: 24)

The failure of Pakistanis and Bangladeshis to get the same return on increased educational attainment must be a concern as education is a key driver of social inclusion. This should also be a significant concern for counterterrorism policy as a sense of blocked social mobility has been identified as an important risk factor in radicalisation (Wiktorowicz 2005).

Employment is crucial for social inclusion and mobility. In relation to employment, there is clear evidence of Muslims occupying a marginal space in the labour market and indicatiors that some of this labour market disadvantage is down to discrimination. Data from the 2001 Census shows that Muslims have the highest unemployment rate and economic inactivity rate and the lowest employment rate of any faith group (Bunglawala 2005). Berthoud and Blekesaune suggest that "religion rather than ethnicity is the characteristic associated with employment disadvantage" (2007:72). A cross referencing of ethnicity and religion shows that "when investigating religious groups within different ethnic groups, we find that all Muslim groups are in a disadvantageous employment position irrespective of which ethnic group they belong to" (Berthoud and Blekesaune 2007:76). Thus, the employment penalty faced by Indian Muslims was greater than that of Indian Hindus, Sikhs, and Christians. When comparing across minority groups, Pakistani and Bangladeshi Muslims experience a greater employment penalty than Caribbean or Black African Christians. Clarke and Drinkwater find "some evidence that, controlling for other factors, Muslims have lower employment rates than individuals with another, or indeed no, religion." However, they argue that the close correlation between religion and ethnicity for some ethnic groups makes it difficult to separate the influences of ethnicity and religion. Furthermore, "it may be tradition, rather than religious belief per se, that influences attitudes to female labour force participation and childcare." They argue that it could be "misleading to label behaviour, such as

presumably voluntary adherence to a particular religion, as a cause of economic disadvantage" (Clarke and Drinkwater 2007: 48).

Large pay penalties are found when the earning of ethnic minority groups are compared with those from the comparable White group. The pay gap is 27 per cent for Bangladeshi men and 20 per cent for Pakistani men (Clarke and Drinkwater 2007: 42). In fact, 45 per cent of Bangladeshi men earned below the national minimum wage compared with 15 per cent of Pakistani men and 4 per cent of White men (Heath and Cheung 2006: 17). Most worrying is the suggestion that most ethnic pay differentials are not due to differences in characteristics but different returns on the same characteristics (Blackaby et al. 2005). The reality of this pay gap is illustrated by comparing the hourly earnings of a white male of average age with no qualification, working in a large firm in the Midlands in 2004, estimated to be £7.24, with an equivalent Bangladeshi male who would earn £5.26. Or, a single white male with degree qualifications working in a large firm in London would have an average hourly earnings of £19.49, compared with an equivalent Bangladeshi male, it would be £14.15 (Heath and Chueng 2006).

Poor health is a further indictor of social exclusion. Long-term illness impacts on people's opportunities for economic and social participation, reducing employment opportunities and income levels which in turn affect people's opportunities for social and leisure activities. Questions about health, asked in the 2001 Census, show that Muslim males and females in Great Britain had the highest rates of reported ill health. Age-standardised rates of "not good" health were 13 per cent for Muslim males and 16 per cent for Muslim females in 2001. These rates, which take account of the difference in age structures between the religious groups, were higher than those of Jews and Christians, who were the least likely to rate their health as "not good." After taking account of the different age structures of the groups, Muslims had the highest rates of disability. Almost a quarter of Muslim females (24 per cent) had a disability, as did one in five (21 per cent) Muslim males.

A further feature of the social marginalisation that Muslims face and the one which has perhaps the most direct impact on the relationship with policing is their experience and exposure to crime and violence and of policing responses to this. The young demographic profile of the Muslim population, its ethnic composition, and the over representation of those who are poor means that Muslims are at increased risk of being victims of crime than the general population (Spalek 2005). Pakistani and Bangladeshis are the group most likely to be victims of household crime and racially motivated crime, and report the highest levels of anxiety about crimes such as burglary and robbery (Clancy et al. 2001). Hate crimes are identified as "signal crimes" that have a major affect on Muslim community perceptions of safety and have been identified as having an "important role in stimulating processes of radicalisation" (Innes et al. 2008). Muslims also have less confidence in how crime is dealt with in the area where they live and to believe that they will be treated worse than those from other ethnic or racial groups (Page et al. 2004; Attwood et al. 2001). Poor relationship between local Muslim youth and the police underpinned the tensions that existed in

Oldham prior to the riots that took place there in the summer of 2001 (Ahmed et al. 2001). Data showing that between 2001–2002 and 2002–2003, the number of White people stopped and searched under the Terrorism Act 2000 increased by 118 per cent, whereas the corresponding increase for Black people was 230 per cent and for Asian people 302 per cent does not tell us the extent to which this disproportionately impacts Muslims (Home Office 2004). Other surveys, however, suggest that Muslim men are more likely than other groups to report being stopped or approached by the police (Innes et al. 2008). The combination of feeling over-policed that arise from experiences of disproportionate stop and searches and of being under-policed that arise from experiences of hate crimes "contribute to and 'feed' a sense of local injustice" that increases risks of radicalisation (Innes et al. 2008).

11.4 Impact of Socio-Economic Factors and Government Policy

The importance of socio-economic marginalisation to counterterrorism policy arises from the role that the humiliation of discrimination and experiences of social, economic and cultural marginalisation play in the radicalisation process. Any discussion of radicalisation is confronted by our limited understanding of a process that itself is constantly changing. Nevertheless, an analysis by the Dutch government suggests that three aspects play a role in the process of radicalisation: the individual process, the interpersonal dynamic and the effect of circumstances. In the first of these, the individual process, violent radicalisation is seen as one possible outcome from the search for identity. For young people, in particular, the search for identity is part of the process of defining one's relationship with the world that usually takes place without violent radicalisation. Such radicalisation therefore also requires the second aspect, an interpersonal interaction with other actors who stimulate and influence the radicalisation process (Directorate of General Judicial Strategy 2005; Slootman and Tille 2006). At the same time, the third aspect, the effect of circumstances, includes the wider social, economic, and political context including experiences of discrimination and inequality, also contributes to radicalisation.

A study of the members of *Al-Muhajiroun* – a group to which some of those arrested in Britain in relation to terrorism have been linked – suggests that a common feature among those who are open to the message of the organisation, are experiences of social exclusion and discrimination. Individuals drawn to *Al-Muhajiroun*, find that experiences of Islamophobia belie society's claims of tolerance: "The experience of both racial and religious discrimination has prompted some young Muslims to think about their identity and how they fit into British society. This is particularly true of young university students who suffer from a sense of blocked social mobility" (Wiktorowicz 2005: 90). In fact, the leader of *Al-Muhajiroun*, Omar Bakri Mohammed, identifies this group as their most important recruitment pool because it is the upwardly mobile group that "believes that they face a discriminatory system

that prevents them from realising their potential. They grew up in Britain but are not considered British by many in society" (Wiktorowicz 2005: 91). Omar Bakri Mohammed emphasises the importance of this identity crisis triggered by discrimination in attracting potential joiners: "[I]f there is no racism in the West, there is no conflict of identity…If there is no discrimination or racism, I think it would be very difficult for us" (Wiktorowicz 2005: 91).

At times, the government has played down the relevance of socio-economic deprivation and marginalisation in its statements on counterterrorism. The Home Secretary has argued that violent radicalism "is not driven by poverty, social exclusion or racial justice…they were not the poor and the dispossessed. They were, for the most part, well educated and prosperous…ideas drive those people forward."[5] The profile of many of those that have been involved in or arrested for terrorism related offences reveals a diversity of socio-economic backgrounds. Ahmed Omar Saeed Shiekh,[6] Sajid Badat,[7] and Omar Khan Sharif[8]all attended private schools. Of the 7 July 2005 bombers, two, Mohammed Siddique Khan (the leader of the group) and Shehzad Tanweer, were university graduates. The former worked as a teaching assistant in a local school while the latter's father was a local businessman. The youngest of the four bombers, 18-year-old Hasib Hussain, left school in 2003 with good qualifications, but without pursuing his education further. The fourth 7/7 bomber, the Jamaican born Gemaine Lindsay, grew up in England and converted to Islam as a teenager, left school at 16 and thereafter found occasional work as a carpet fitter. Three of the four men who failed in their attempts to detonate bombs on the London transport system on 21 July 2005 – Yasim Omar, Ramzi Mohammed, and Muktar Said Ibrahim – arrived in the UK as child refugees from Somalia. They were placed in the care of local social services, and on leaving school found employment at various times in shops, bars, and street markets. One of the three, Muktar Ibrahim, had also spent time in a young offenders institute for gang-related violence. The fourth member of the 21 July bombers, Hussain Osman, arrived in Italy from Ethiopia aged 14 before claiming to be a refugee from Somali on arrival in the UK in 1996. Finally, both Kafeel Ahmed and Bilal Abdullah, who attempted to detonate a car bomb at Glasgow airport in June 2007, were medical doctors from India and Iraq working in Britain's National Health Service.

While some might seek to deny the importance of socio-economic factors given that those involved in (attempted) bombings in the UK were not necessarily from the most vulnerable background, this misunderstands the role and relevant of experiences and perception of how their communities are treated. The history of political violence has rarely suggested a straightforward relationship between deprivation and the mobilisation of individuals towards violence:

[5] Hansard, HC, vol 438 col 325 (26 October 2005).

[6] Convicted in Pakistan for involvement in the murder of Daniel Pearl in 2002.

[7] Pleaded guilty in 2005 to planning to blow up aircraft with a shoe bomb.

[8] Involved in suicide bombings in Tel Aviv in 2003.

> [M]obilisation is not about rich or poor leaders and/or perpetrators. It stands to reason that those most able to mobilise should be the educated strategists. These types of individuals are not above instrumentalising the belief or suffering of others; nor are they immune to a genuine sense of responsibility in the name of a community, on whose behalf they decide to act. (Briggs et al. 2006: 46)

Focusing on the circumstances of individuals also underestimates the impoverished nature of the communities from which they hailed, and "which held a profound resonance for them" (Awan 2007). Thus, the individual socio-economic circumstances of the 7 July 2005 bombers may not be as significant as that fact that three of them grew up in an area of Leeds, where 10,000 of the 16,000 residents had living standards that are among the worst 3 per cent nationally.

In fact, the need to address social and economic deprivation is recognised in the government's long-term counterterrorism strategy. CONTEST, the name given to the government's overarching counterterrorism strategy is a multi-dimensional strategy corresponding to the multi-faceted nature of terrorism. The strategy has four strands – Prevention, Pursuit, Protection, and Preparedness. Prevention takes in long-term goals, such as working to reduce tendencies leading to "radicalisation," for instance, through helping resolve international disputes which terrorists can exploit. Conditions of socio-economic disadvantage as well as experiences of discrimination are recognised as relevant background factors that increases the risks of radicalisation. Policies aimed at addressing these issues, which contribute towards work within the "prevent" strand, range from the enactment of legislation to prohibit discrimination on the grounds of religion or belief in the provision of goods, services, facilities, education, and exercise of public functions by public bodies through to action on reducing the ethnic minority employment and educational attainment gap. The location of the government's "Preventing Extremism Unit" within the Department for Communities and Local Government (CLG) underlines the emphasis on non-legal tools in preventing violent extremism.

11.5 Engaging Communities

Community engagement is the cornerstone of effective counterterrorism policy. As Briggs et al. (2007: 58) note, those who argue that "Muslims should tolerate inconveniences for the greater good, effectively put up and shut up…. lack understanding about how security is really delivered in practice– always through consent, never through force."

The importance of community engagement was emphasised by the British Prime Minister, Gorden Brown, in the government's National Security Statement in November 2007:

> To deal with the challenge posed by the terrorist threat we have to do more, working with communities in our country, first, to challenge extremist propaganda and support alternative voices; secondly, to disrupt the promoters of violent extremism by strengthening our institutions and supporting individuals who may be being targeted; thirdly, to increase the

> capacity of communities to resist and reject violent extremism; and fourthly, to address issues of concern exploited by ideologues, where by emphasizing our shared values across communities we can both celebrate and act upon what unites us. This will be achieved not by one single programme or initiative and it will not be achieved overnight. It is a generational challenge that requires sustained work over the long-term, through a range of actions in schools, colleges, universities, faith groups and youth clubs, by engaging young people through the media, culture, sport and arts, and by acting against extremist influences operating on the internet and in institutions from prisons and universities to some places of worship. (Brown 2007)

The need to build trust and support with communities is recognised in the National Policing Plan 2005–2008. It provides that the counterterrorism strategy of government is underpinned by "strong community ties to build and increase trust and confidence within minority faith communities" (Home Office 2008: 22).

In relation to preventing violent extremism, the Department of CLG identifies its primary task as enabling "local communities…..to robustly challenge the ideas of extremists" (Department for Community and Local Government 2007). Its strategy, entitled *Preventing Violent Extremism: Winning hearts and minds*, is focused around four themes: promoting shared values, supporting local solutions, building civic capacity and leadership, and strengthening the role of faith institution and leaders. Engagement with "the Muslim community" intensified in the aftermath of the London bombings of July 2005. The government set up a series of working groups to advise them on preventing extremism, whereas the police, after 9/11 set up the Muslim Safety Forum to provide a basis for meeting Muslim community organisations and NGOs.

For government and state institutions identifying who to engage with in relation to Muslim communities raises a dilemma and concerns that through engagement they are conferring legitimacy on particular parts of the Muslim community. This has contributed to a situation where state policy "operates according to a binary opposition of Legitimate and Illegitimate Muslims" (Spalek and Imtoual 2007). In this context, CLG is criticised for opting to focus on working with groups that it views as moderate and legitimate that are willing to accept the government's terms of engagement. The CLG policy appears to isolate and exclude those groups that it views as extreme and illegitimate, or failing to share its values and provide sufficient condemnation of terrorism. This approach may, however, serve to increase feeling of disempowerment and marginalisation as the government retains power in this relationship, setting the terms of engagement and the parameters of what is a legitimate Muslim identity (Spalek and Imtoual 2007).

Two examples illustrate how this unequal relationship can lead to decision that may undermine the broader counterterrorism strategy. The first example relates to the "Preventing Extremism Together" working groups. These were set up to advise government on its strategy after the July 2005 bombings. Many Muslims involved in the working groups were already apprehensive that the group would be used to provide cover to justify more repressive security measures and questioned the seriousness of the process in light of the tight timescales that appeared to operate to a political agenda. The government dismissed the group's central recommendation – a call for a public inquiry into the events leading up to 7 July 2005 bombings – even though it was argued to be necessary to ensure the shared understanding needed to

ensure effective community engagement on tackling extremism and countering terrorism (Blick et al. 2007). A second example is the treatment of all Salafi groups within the Muslim community as extremists. This labelling has led to the exclusion from policy discussion of those that had been the first to alert the authorities to the danger posed by extremists such as Abu Quatada and have been at the forefront of confronting Al-Qaeda propaganda (Spalek and Lambert 2007; Lambert 2008).

The opportunities for Muslims to participate in the public sphere on the basis of their faith identity have increased in the past decade. Faith based institutions were vital to the development and delivery of welfare services prior to the creation of the welfare state. Even after the creation of a largely secular welfare state, they continued to play an important part in service delivery, particularly in education. More recently, within the context of an increasing emphasis on the importance of consultation and engagement with communities in developing effective government policy interventions, and a move towards neighbourhood based regeneration strategy, the need to engage with local faith communities has been acknowledged. In its National Strategy for Neighbourhood Renewal, the government stated that "communities need to be consulted and listened to, and the most effective interventions are often those where communities are actively involved in their design and delivery, and where possible in the driving seat…this applies as much to communities of interest as it does to geographical communities." Faith communities are able to draw upon significant resources in terms of people, networks, organisations, and buildings. They may be the only community organisations in neighbourhoods where the social infrastructure has been eroded. Furthermore, "in terms of active membership, churches, mosques, temples, synagogues, and gurdwaras are often among the most substantial local community-based organisations, with as much right to be involved in discussion on neighbourhood renewal as, for example, residents' or tenants' organisations" (Neighbourhood Renewal Unit 2004: 1).

While opportunities for Muslims to participate and engage with institutions on the basis of their faith identity have increased, the response to these opportunities by Muslims has produced backlash against identity based politics. Much of this has been based on the assumption that engaging Muslims on the basis of their faith identity reinforces strong Muslim identities, which in turn are viewed as a threat to social cohesion. Furbey and Macey (2005) are critical of the development of policies for engaging with faith communities in regeneration without reference to the "negative consequences for inter-ethnic relations of an association between religion and ethnicity." This concern is echoed further in the government's public consultation on extending duties on public bodies to eliminate discrimination and promote equality – which currently exist for the grounds of race, gender, and disability – to religion and belief. The government noted that there were concerns that "extending the coverage of a single public sector duty to religion or belief might lead to particular groups being given too strong a voice in determining how public services are designed and delivered, which have a negative impact on public service provision generally and on community cohesion" (Discrimination Law Review 2007: 99). While the imperatives of security override concerns about engaging with faith institutions and leaders in relation to counterterrorism in other areas of social policy,

there appears to remain a reluctance to engage with Muslim organisations and communities. This increases the risk of Muslims feeling that the state views them through the prism of security and is only interested in engaging with them on issues of counterterrorism.

11.6 The Reinforcing Perceptions of a Muslim Threat

The framing of government counterterrorism policy in terms of supporting Muslim communities in confronting extremism also creates a danger of reinforcing the image of Muslims as a threat to society. The challenge for government is to find a language and policy approach that allows it to describe the nature of the current threat without reinforcing perceptions and stereotypes of Muslims as a threat. The government belated recognises the need to move away from inappropriate and offensive language that reinforces alienation and is seeking to ensure that Ministers do not describe the terrorist threat as a "Muslim problem" (Norton-Taylor 2007b). While any change in language is important, underpinning the CLG prevention policy remains the assumption that "Muslim communities are the locus of extremism" (Spalek and Imtoual 2007). One strand of this position is the belief that the problem lies not just with the small number of individuals that are actively involved in violence or planning acts of terrorism but also with the "fence sitters" that fail to actively condemn terrorism (Saggar 2006). The evidence about the size of this group is based in part on opinion poll surveys of Muslims.

Analysis of some of the polling data, however, suggests that the evidence from these polls about the nature and size of any such group remains partial and inconclusive. In polls taken immediately after 2005 London bombings, the overwhelming majority of Muslims said the bombings were not justified. In the three polls carried out during July, only 4–6 per cent of Muslims said the attacks were justified or that they agreed with the attacks. In a 2006 poll, the percentage of Muslims who thought the London bombings were right fell to 1 per cent. An NOP/Channel 4 poll in April 2006, however, suggested that the percentage of those that thought the July bombings could be justified was as high as 23 per cent. However, the framing of the questions here is significantly different from pervious polls. Respondents were not asked whether they thought the bombings were justified, instead they were asked whether they agreed with the view that some people held that "the July bombings were justified *because* of the British support for the US war on terror." The higher figure in this survey may reflect the impact of combining the question of justification and reasons for possible justification.

Saggar (2006) suggests that policymakers have "focused too heavily on narrow conspiracies of violence" and taken their eyes off those who "surround and tacitly support violence and its perpetrators." He suggests that concern should focus on those who have sympathy with terrorists. Here again, analysis of polling evidence suggests that care is needed before drawing definite conclusions. Two polls asked Muslims whether they had sympathy with the feelings or motives of the bombers.

In the first poll, 24 per cent, and in the second, 20 per cent, said they had some sympathy with the feelings and motives of the bombers. The questions, however, do not separate out people's potential for some sympathy for feeling the bomber may have had and sympathy with their motives. Nor, of course, does it elaborate on how these terms are interpreted. In a YouGov 2005 poll when asked "do you think you understand why some people might behave in that way," a majority of Muslim (56 per cent) said yes. However, in the NOP/Channel 4 poll, when asked whether they agreed or disagreed with the statement "I can understand why young British Muslims might want to carry out suicide operations," 13 per cent either strongly agreed (5 per cent) or agreed (8 per cent) with the statement.

Where questions are not about concrete and specific examples of the use of violence, such as the July bombings, but broader questions about the justifications of the use of violence then the percentage of people agreeing that violence may be justified falls within a broader range. In a poll before the London bombings, 11 per cent agreed with the statement that it is acceptable for religious or political groups to use violence for political ends. After the July bombings in December 2005, 6 per cent agreed with the statement "are there any circumstances under which you think that suicide bombings can ever be justified in the UK?" The question was phrased significantly more broadly, in asking whether there were *any* circumstances in which suicide bombings could be justified. The clearest example of how the levels of support for "violence" in an opinion poll can be shaped by the framing of the question is seen in a YouGov poll where Muslims were asked if they agreed with the series of statements about the nature of western society. One per cent agreed with the statement that "Western society is decadent and immoral, and Muslims should seek to bring it to an end, if necessary by violence." By contrast in an ICM poll 7 per cent agreed "Western society is decadent and immoral, and Muslims should seek to bring it to an end, if necessary by violent means." Unlike the YouGov poll, the following was not provided as an option in the ICM poll: "Western society is decadent and immoral, and Muslims should seek to bring it to an end, but only by non-violent means." Furthermore, none of the polls provide a positive alternative that allowed the respondent to disagree with the basic premise of the question that Muslims feel western society is decadent and immoral and want to bring it to an end. There is a danger of developing policy and drawing conclusions on the basis of limited evidence.

11.7 The Effect of New Laws

While engaging with Muslim communities has been one part of the government's response to the current threat, passing anti-terrorism legislation has been another notable aspect of its policy response. The legislation passed since 2001 has created new offences of indirect incitement of terrorism, widened police powers of stop and search and extended the time a suspect can be detained before charge from 14 to 28 days, after having failed to extend it to 90 days.

It is said to be a "sad historical reality" that governments too often fail to see that those who are most vulnerable to terrorist recruitment are "unreceptive to suppression or criminalisation" and that "the injudicious use of coercive powers and excessive force against these elements of society, even before they subscribe to the terrorist cause, has more often then not had the reverse effect of confirming the hostile beliefs spread by terrorist recruiters" (Pickering et al..2008: 40). If the government overreacts, counterterrorism measures themselves may feed and sustain terrorism, creating a well of sympathy and silence among sections of society, especially if these measures increase repression, stigmatise, and alienate these groups. Thus, the state's counterterrorism measures "can profoundly affect the nature and lethality" of terrorist violence. Any analysis of the causes of terrorism that does not consider the possible counterproductive effect of counterterrorism measures runs the risk of being dangerously "limited and flawed" (Silke 2005: 241).

The British government's response to terrorism in Northern Ireland provides a cautionary tale. The oppressive nature of the action by the security services was central to increasing recruitment and support for the Provisional Irish Republican Army (PIRA). It was the "crude and oppressive security policies" of the British army in the 1970s that gave "many previously uninvolved Catholics ample reason to hate the RUC and British Army" and led to recruitment en masse. A good example of this were the 1,183 raids on Catholic homes that took place during two months in 1970 involving "carpets and floorboards being pulled up, doors kicked in, walls and ceiling being knocked open with drills, and sledgehammers. Yet in only 47 cases were weapons actually found" (Silke 2005: 244). In fact, Andrew Silke suggests that "the IRA worked to provoke harsh measures from the unfortunate security services, knowing full well the benefits it would reap in terms of support and recruits." Internment of 2,357 people of whom 1,600 were released without charge led to further recruitment by the PIRA. Kieran McEvoy concludes that:

> Apart from the political fallout, in purely military terms internment was an unmitigated disaster. The degree and intensity of the violence in the aftermath of internment has not been matched either before or since. The principal justification for internment had been to take the principal players out of action and then make further inroads on their operations by gaining intelligence through interrogations. In the seven months prior to internment, eleven soldiers, and seventeen civilians died; in the five months following internment, thirty-two British soldiers, five members of the Ulster Defence Regiment, and ninety-seven civilians were either shot dead or blown up. The intended objectives of internment had clearly not been achieved (McEvoy 2001: 214–5).

The civil rights lawyer Gareth Pierce, who has experience of defending those facing terrorism charges in Irish and Muslim communities, notes the differences in the experiences of communities that are the focus of counterterrorism policing from those of the mainstream:

> Just as Irish men and women, wherever they lived, knew every detail of each injustice as if it had been done to them, long before British men and women were even aware that entire Irish families had been wrongly imprisoned in their country for decades, so Muslim men and women here and across the world are registering the ill-treatment of their community here, and recognising, too, the analogies with the experiences of the Irish. (Pierce 2008)

According to Paddy Hillyard:

> [T]he lessons from Northern Ireland are clear. Widespread violation of human rights in the so called 'war against terrorism' is counterproductive. It erodes democracy by undermining the very principles on which social order is based and alienates the communities from whom the authorities need support in dealing with political violence.'(Hillyard 2005)

In particular, "people are not going to report incidents or crucial information to the police when either their last contact was at best unpleasant and at worst humiliating and abusive or that they have heard how a neighbour or relative has been treated. Good intelligence is essential to prevent acts of terror, yet the authorities still appear to lack an understanding of the crucial role of good police community relations in this endeavour" (Hillyard 2005).

Building cooperation and trust with Muslim communities is critical not only in gathering intelligence but also in countering the strategic aims of terrorists to exploit the sensitivity of democratic societies to the insecurities of the majority of citizens and so provoke an overreaction from the state. This overreaction in turn will further alienate the minorities that are the focus of suspicion, and thus make it easier for terrorists to exploit the situation and exacerbate community tensions.

In the House of Lords debates on the pre-trail detention of up to 90 days, Lord Condon, the former Metropolitan Police Commissioner, warned that "the battle against terrorism is a battle that will last for decades. It is a battle for hearts and minds…." He feared that, on balance, "and it is a very fine balance," the extension of detention without charge might be counterproductive "in the sense of encouraging martyrdom rather than preventing it." The struggle in his view was one that was "a philosophical struggle that would endure for several decades." In this context measures, such as 90 days detention "would have enormous tactical advantage in the short term…but that longer term and strategically it could be counterproductive." Thus, the question for Parliament to decide was:

> Having heard what the police and intelligence agencies are advocating, what does this House [the House of Lords] and the other place [the House of Commons] feel is in the long-term benefit of the country in the fight against terrorism? Even though in one, two or three individual cases an extension to 90 days may help, my fear is what that might generate in terms of helping in the propaganda of terrorism. Often there is a misunderstanding about what *al-Qaeda* is. It is not a finite list of several hundred people and, once we have ticked them off and got them before a court and convicted, we will have stopped terrorism… The huge publicity that has surrounded this debate has already generated enormous fear in law-abiding communities in parts of this country. If we now go back and make it look as though we are going to challenge yet again the point of 28 days that we have reached, I fear that it will play into the hands of the propagandists, who will encourage young men and women—to all other intents and purposes, they are good people—to be misguided. Hansard HL vol 676 col 1174 (13 December 2005).

There is concern that the use of powers under anti-terrorism laws is already having counterproductive impact on community cooperation. One particular area of concern is the increased use of stop and search powers under section 44 of the Terrorism Act 2000. The Muslim Council of Britain claimed that "the police are misusing their new powers…We think that the institutional racism highlighted by the McPherson report is morphing into institutional prejudice against Muslims. We are worried a generation of young Muslim men is being criminalised" (Cowan 2004). Britain's

most senior Muslim police officer, Assistant Commissioner Tarique Ghaffur, has commented that the impact of stop and search and passenger profiling has been to create "a strong feeling of mass stereotyping within Muslim communities" (Assistant Commissioner Tarique Ghaffur 2006). He believes that incidence such as the raid by anti-terrorism police on a house in Forrest Gate in East London during June 2006 that turned out to based on unreliable intelligence and led to the shooting of an innocent young Muslim "drip feeds into vulnerable communities and gradually erodes confidence and trust." He also warns of "a very real danger that the counterterrorism label is also being used by other law-enforcement agencies to the effect that there is a real risk of criminalising minority communities. The impact of this will be that just at the time we need the confidence and trust of these communities, they may retreat inside themselves. We therefore need proper accountability and transparency round all policy and direction that affects communities."[9]

According to the Forum Against Islamophobia and Racism (2004), the enforcement of anti-terrorism legislation "has led to the victimisation and stigmatisation of the Muslim community." FAIR has also found that:

> "victimisation of Muslims under the anti-terrorism legislation has lead to increased incidences of Islamophobia and racism against Muslims. This has manifested itself in the form of vandalism of mosques, Muslim graves and homes." Furthermore, "the increased hostility towards Muslims has also seen an increase in hate campaigns against Islam and Muslims from far right groups." (Forum Against Islamophobia and Racism 2004)

Human Rights Watch has also found that the enforcement of the legislation "has harmed race and community relations" and undermined the willingness of Muslims in the UK to cooperate with police and security services (Human Rights Watch 2004).

During Parliamentary debate on legislation to create a new offence of indirect encouragement of terrorism (now Terrorism Act 2006), the former Home Office Minister John Denham M.P. placed his criticism in the broader context of the overall counterterrorism strategy:

> [This]…is not a battle over what people are allowed to say; it is a question of how we win arguments. The battle is for hearts and minds. We must persuade young British people from the Muslim community who feel angry about what is happening in the world….and who feel that in the west their Muslim lives are less valuable than others and their rights less valued than others, that engagement in politics, democracy, public life and argument is the way to achieve change, not terrorism…[A]gainst us are extremists who arguing the opposite-that there is no way forward for them in western democracy; that it is a sham, an illusion and a dead end; and that terrorist violence is not only justified but the only way. We must be careful not to feed that argument. As the Bill stands, however, it is more helpful to the propaganda of extremists than it is to winning hearts and minds.

The all encompassing definition of acts of terrorism found in the Terrorism Act 2000 and the failure to allow for distinctions between the indiscriminate killing of

[9] Assistant Commissioner Tarique Ghaffur, speech to the Association of Black Police Officers, 6 August 2006.

innocent civilians and attacks on the property and apparatus of a repressive state criminalises all support for any political violence irrespective of the circumstance. The Act, in Denham's view, impedes the potential for nuanced response to the different context, in which violence takes place:

> It allows the extremists, in arguments that will take place in communities…to argue that … it is not even possible to support people who they regard as their brothers, and who are fighting occupation and winning elections, without being silenced. They will say that it is not possible to advocate a Muslim state without being silenced. They will say that the terrorist route is the only way. That is the argument that will be advanced in streets and communities up and down the country, and what we must ask ourselves is whether the phrasing of clause 1 will help us to win the argument for democracy and engagement. Hansard HC vol 438 col 370–71 (26 October 2005).

The Report of the Working Groups set up by the Home Office in the aftermath of the July 2005 London bombings also expressed concerns about the impact of encouragement offences on political debate:

> Inciting, justifying or glorifying terrorism as currently formulated could lead to a significant chill factor in the Muslim community in expressing legitimate support for self-determination struggles around the world and in using legitimate concepts and terminology because of fear of being misunderstood and implicated for terrorism by the authorities. (Home Office 2005: 77)

The view that this legislation was aimed to circumscribe the boundaries of acceptable political debate for Muslims was reinforced by perception that the provision in the 2006 Act to allow the proscription of organisations that glorify terrorism were targeted at *Hizb-ut-Tahrir*, an organisation whose main achievement has been in shifting the debate within Islamist groups on the issue of the need for a new Caliphate and the centrality of religious identity over other national or ethnic ties.[10] This view was further reinforced by the then Home Secretary Charles Clarke in his speech to the US Heritage Foundation in October 2005 where he declared that "there can be no negotiation about the re-creation of the Caliphate; there can be no negotiation about the imposition of *Sharia* law." Along with free speech and gender equality, these matters, he said, were "simply not up for negotiation."[11] For some Muslims this was a clear signal that such issues are outside the bounds of political

[10] Founded in the Middle East, in the 1950s, but with branches now in the UK, *Hizb-ut-Tahrir* does not engage in terrorism or any direct action but in "ideological struggle." It has been accused of being a "conveyor belt for terrorists"; an organisation that "indoctrinates individuals with radical ideology, priming them for recruitment by more extreme organisations where they can take part in actual operations." It occupies as "grey zone of militancy, with its activities involving more than mere expression of opinion but less then terrorism." Z. Baran (2005) "Fighting the War of Ideas" 84 *Foreign Affairs* 68.

[11] Charles Clarke, "Contesting the Threat of Terrorism" (Speech to the Heritage Foundation, Washington DC, October 2005) available at <http://press.homeoffice.gov.uk/Speeches/10-05-heritage-foundation> (viewed 14 December 2007).

debate. For them "the main problem here is not that our governments disagree with the concept of the *Khilafah* (the re-creation of the Caliphate) and *Shariah* law. What is disturbing is the way in which they are determined to close debate and to tighten the boundaries of inclusiveness in mainstream society."[12]

11.8 Conclusion: From Exclusion to Inclusion?

The situation created by the current terrorist threat contains both risks and opportunities for Muslim communities in the UK. The risks arise from counterterrorism policies that reinforce processes and social and economic marginalisation and increase prejudice against Muslims and further alienate a socially marginalised generation. Some of the policy developments discussed here suggests movement in this direction. However, in the midst of these risks, there are also opportunities. The terrorism threat has brought urgent attention to the need for policies to address the social and economic exclusion Muslims experience. While this should have been addressed as a matter of social justice, the role of discrimination, alienation, and blocked social mobility in radicalisation has given unprecedented urgency to the development of effective social policy interventions. With unprecedented scrutiny have come opportunities for more detailed understanding of the diversity of Muslim communities and consequent development of more effective policy interventions that meet community needs.

References

Attwood, C., Singh, G., Prime, D., and Creasey, R. (2001) *Home Office Citizenship Survey: People, Families and Communities*, London: Home Office.

Abrams, D. and Houston, D. (2006) *Equality, Diversity and Prejudice in Britain – Results from the 2005 National Survey*, Kent: Centre for the Study of Group Processes.

Ahmed, N. M., Bodi, F., Kazim, R., and Shadjareh, M. (2001) *The Oldham Riots: Discrimination, Deprivation and Communal Tension in the United Kingdom*, London: Islamic Human Rights Commission.

Ali, M., (2001) *Turkish-Speaking Communities and Education – No Delight*, London: Fatal Publications.

Ameli, S. R., Elahi, M., and Merali, A. (2004) *British Muslims' Expectations of Government – Social Discrimination: Across the Muslim Divide*, London: Islamic Human Rights Commission.

[12] "In Blunkett's Footsteps" 7 *Reflections*1, reproduced in <*http://reimagginingtheummah.blogspot.com*> (viewed 14 December 2007); *see also* O Saeed, "The Return of Caliphate," The *Guardian*, 1 November 2005 <http://www.guardian.co.uk/comment/story/0,3604,1605653,00.html> (viewed 14 December 2007).

Ansari, H. (2004) *The Infidel Within: Muslims in Britain since 1800*, London: Hurst and Co.
Archer, L. (2003) *Race, Masculinity and Schooling: Muslim Boys and Education*, Maidenhead: Open University Press.
Awan, A. (2007) "Transitional Religious Experiences: Contextual Disjuncture and Islamic Political Radicalism," in T. Abbas (ed.), *Islamic Political Radicalism: A European Perspective*, Edinburgh: Edinburgh University Press.
Ballard, R. (1996) "The Pakistanis: Stability and Introspection," in C. Peach (ed.), *The Ethnic Minority Populations of Great Britain: Ethnicity in the 1991 Census*, Vol. 2 London: Central Statistical Office.
Berthoud, R. (2002) *Multiple Disadvantage in the Labour Market*, York: Joseph Rowntree Foundation.
Berthoud, R. and Blekesaune, M. (2007) *Persistent Employment Disadvantage*, DWP Research Report No. 416, Norwich: Department for Work and Pensions.
Blair, T. (2006) "We Need ID Cards to Secure Our Boarders and Ease Modern Life," Daily Telegraph 06 November 2006.
Blackaby, D. H., Leslie, D. G., Murphy, P. D., and O'Leary, N. C. (2005) "Born in Britain: How Are Native Ethnic Minorities Faring in the British Labour Market," *Economics Letters*, Vol. 88, pp. 370–375.
Blick, A, Choudhury, T., and Weir, S. (2007) *The Rules of the Game: Terrorism, Community and Human Rights*, York: Joseph Rowntree Reform Trust.
Briggs, R., Fieschi, C., and Lownsbrough, H. (2006) *Bringing It Home: Community Based Approaches to Counter Terrorism*, London: Demos.
Brown, G. (2007) *National Security Statement* (14 Nov 07) (http://www.number10.gov.uk/Page13757).
Bunglawala Z. (2005) "Muslims and the Labour Market," in T. Choudhury (ed.), *Muslim in the UK: Policies for Engaged Citizens*, Budapest: Open Society Institute.
Clancy, A., Hough, M., Aust, R., and Kershaw, C. (2001) *Ethnic Minority Experience of Crime and Policing: Findings from the 2000 British Crime Survey*, Home Office Research Findings 146, London: Home Office.
Clarke, K. and Drinkwater, S. (2007) *Ethnic Minorities in the Labour Market: Dynamics and Diversity* York: Joseph Rowntree Foundation.
Cowan, R. (2004) "Young Muslims 'Made Scapegoats' in Stop and Search," The *Guardian*.
Crawley, H (2005) "Evidence on Attitudes to Asylum and Immigration: What We Know, Don't Know and Need to Know," COMPAS Working Paper No. 23, Oxford: University of Oxford, www.compas.ox.ac.uk/publications/papers/Heaven%20Crawley%20WP0523.pdf
Department for Communities and Local Government (2007) *Preventing Violent Extremism: Winning Hearts and Minds*, London, Department for Communities and Local Government.
Department for Education and Skills (2006) *Ethnicity and Education*, London: DfES.
Directorate of General Judicial Strategy (2005) Policy Memorandum on Radicalism and Radicalisation, Ministry of Justice: the Hague.
Discrimination Law Review (2007) *A Framework for Fairness: Proposals for a Single Equality Bill for Great Britain*. London: Department for Communities and Local Government.
El-Sohl, C. (1992) "Arab Communities in Britain: Cleavages and Commonalities," *Islam and Christian-Muslim Relations*, Vol. 3 (2).
Enneli, P., Modood, T., and Bradley, H. (2005) *Young Turks and Kurds: A Set of "Invisible" Disadvantaged Groups*, York: Joseph Rowntree Foundation.
Forum Against Islamophobia and Racism (2004) *A Submission to the Home Affairs Committee's Inquiry into Terrorism and Social Cohesion*, London: FAIR.
Furbey, R. and Macey, M. (2005) "Religion and Urban Regeneration a Place for Faith?," *Policy and Politics*, Vol. 95.
Assistant Commissioner Tarique Ghaffur (2006) Speech to the Association of Black Police Officers.
Hansen R. (2000) *Citizenship and Immigration in Post-War Britain*, Oxford: Oxford University Press.
Heath, A. and Cheung, S. Y. (2006) *Ethnic Penalties in the Labour Market: Employers and Discrimination*, Research Report No 341, London: Department for Work and Pensions.

Hillyard, P. (2005), "The "War on Terror": Lessons from Ireland" in European Civil Liberties Network, *Essays for Civil Liberties and Democracy in Europe 4* <www.ecln.org> (viewed 14 December 2007).

Home Office (2004) *Statistics on Race and the Criminal Justice System: A Home Office publication under section 95 of the Criminal Justice Act 1991*, London: Home Office, 2004.

Home Office (2008) *National Policing Plan 2005–08: Safer, Stronger Communities*, London: HMSO.

Innes, M., Abbott, L., Lowe, T., and Roberts, C. (2007) *Hearts and Minds and Eyes and Ears: Reducing Radicalisation Risks Through Reassurance Oriented Policing* Cardiff: Universities' Police Science Institutes.

Intelligence and Security Committee (2006) *Report into the London Terrorist Attacks on 7 July 2005* (Cm 6785).

Jacobson, J. (1997) "Religion and Ethnicity: Dual and Alternative Source of Identity Among Young British Pakistanis," *Ethnic and Racial Studies*, Vol. 20(2).

Kenway, P. and Palmer, G. (2007) *Poverty Among Ethnic Groups How and Why Does It Differ?* York: Joseph Rowntree Foundation.

Khokher, S. (1993) "Religious and Ethnic Identity Among Young Muslim Women in Bradford," *New Community*, Vol. 19(4).

Lambert, R. (2008) "Empowering Salafis and Islamists against Al-Qaeda: A London Counterterrorism Case Study," in PS: Political Science and Politics XLI/1.

Leigh, R. (2007) *Mapping Exercise of Afghan Communities in the UK*.

McEvoy, K. (2001) *Paramilitary Imprisonment in Northern Ireland*, Oxford: OUP.

Modood, T, Berthoud, R., Lakey, J., Nazroo, J., Smith, P., Virdee, S., and Beishon, S. (1997) *Ethnic Minorities in Britain: Disadvantage and Diversity*, London: Policy Studies Institute.

Modood, T (2006) "Ethnicity, Muslims and Higher Education in Britain," *Teaching in Higher Education* 11(2), 247–250.

Mogahed, D. (2007) *Beyond Multiculturalism vs. Assimilation*, Princeton, NJ: Gallup.

Moore, K., Mason, P., and Lewis, J. (2008) *Images of Islam in the UK: The Representation of Muslims in the National Print News Media 2000–2008*, Cardiff: Cardiff School of Journalism, Media and Cultural Studies.

Norton-Taylor, R. (2007a) "Al-Qaida Recruiting Teenagers to Attack Targets in the Britain, Warns MI5 Chief," *The Guardian*, 6 November 2007, http://www.guardian.co.uk/terrorism/story/0,,2205809,00.html

Norton-Taylor, R. (2007b) "Counter-Terrorism Officials Rethink Stance on Muslims," *The Guardian*, 20 November 2007, http://www.guardian.co.uk/uk/2007/nov/20/terrorism.religion

O'Beirne, M. (2004) *Religion in England and Wales: Findings from the 2001 Home Office Citizenship Survey,* Home Office Research Study 274, (Home Office). Available at http://www.homeoffice.gov.uk/rds/pdfs04/hors274.pdf

Page, B., Wake, R., and Ames, A. (2004) *Public Confidence in the Criminal Justice System: Home Office Research Findings 221*, London: HMSO.

Pickering, S, McCulloch J, and Wright-Neville, D. (2008) *Counter-Terrorism Policing: Community, Cohesion and Security*, New York: Springer.

Platt, L. (2005) *Migration and Social Mobility: The Life Chances of Britain's Ethnic Communities*, Bristol/York: The Policy Press/Joseph Rowntree Foundation.

Pierce, G. (2008) 'Was It like This for the Irish?' *London Review of Books* 10 April 2008, [http://www.lrb.co.uk/v30/n07/peir01_.html]

Roy, O. (2004) *Globalised Islam: The Search for a New Ummah*, London: Hurst and Company.

Rudiger, A. (2007) *Prisoners of Terror? The Impact of Anti-Terrorism Measures on Refugees and Asylum Seekers in Britain*, London: Refugee Council.

Runnymede Trust Commission on British Muslims and Islamophobia (1997) *Islamophobia – A Challenge for Us All*, London: The Runnymede Trust.

Saggar, S. (2006) "The One Per Cent World: Managing the Myth of Muslim Extremism," *The Political Quarterly* 77(3),314–327.

Sheridan, L. and Gillett, R. (2005) "Major World Events and Discrimination." *Asian Journal of Social Psychology*, 8, 191–197.

Silke, A. (2005) "Fire of Iolaus: The Role of State Countermeasures in Causing Terrorism and What Needs to be Done," in T. Bjorgo (ed.), *Root Causes of Terrorism: Myths, Realities and the Ways Forward*, London: Routledge.

Slootman, M. and Tille, J. (2006) *Processes of Radicalisation: Why Some Amsterdam Muslims Become Radicals*, Amsterdam: Institute of Migration and Ethnic Studies.

Spalek, B. (2005) "Muslims and Criminal Justice" in T. Choudhury (ed.), *Muslim in the UK: Policies for Engaged Citizens*, Budapest: Open Society Institute.

Spalek, B. and Imtoual (2007) "Muslim Communities and Counter-Terror Responses: 'Hard' Approaches to Community Engagement in the UK and Australia," *Journal of Muslim Minority Affairs* 27(2),185–202.

Spalek, B. and Lambert, B. (2007) "Muslim Communities Under Surveillance," *Criminal Justice Matters*.

Warren, T. and Britton, N. J. (2003) "Ethnic Diversity in Economic Wellbeing: The Combined Significance of Income, Wealth and Assets Levels," *Journal of Ethnic and Migration Studies* 29(1) 103–119.

Wiktorowicz, Q. (2005) Radical Islam Rising: Muslim Extremism in the West, Rowman and Littlefield in Maryland USA, 16.

Part IV
Disappearing Rights

Chapter 12
Control Orders: Borders to the Freedom of Movement or Moving the Borders of Freedom?

Susanne Forster

12.1 Background to the United Kingdom's Control Order System

12.1.1 The United Kingdom's Anti-terrorism Legislation

In the past, the United Kingdom's anti-terror legislation has typically consisted of temporary laws that were usually enacted as emergency legislation addressing a specific terrorist threat and were mostly in reaction to a terrorist attack such as, for instance, the Omagh bombing in 1998.[1] However, the developments of the late 1990s led to the conclusion that general and permanent anti-terrorism legislation was desirable.[2] This idea was finally implemented by the enactment of the Terrorism Act 2000 (TA 2000). The Act comprises a definition of the concept of "terrorism" as well as a provision on who is deemed a "terrorist".[3] The TA 2000 can be regarded as the core act of the United Kingdom's anti-terror laws. However, the departure from emergency anti-terrorism legislation in the aftermath of a specific terrorist attack was short-lived. As in numerous other countries, the attacks of 11 September 2001 marked a significant change in the UK's attitude towards anti-terrorist

S. Forster (✉)
Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: s.forster@mpicc.de

[1] See for a summary of the developments: Walker, *Blackstone's Guide to the Anti-Terrorism Legislation*, Chapter 1.

[2] Those developments comprised, inter alia, the drafting of the Lloyd Report in 1996: Lord Lloyd of Berwick and Sir John Kerr, Inquiry into Legislation against Terrorism, Cm. 3420, London 1996; the enactment of the Human Rights Act 1998, as well as the peace process in Northern Ireland, and the Good Friday Agreement in 1998. For a summary of the developments see, for instance, Gearty, *Civil Liberties*, pp. 42–48.

[3] Terrorism is defined in section 1 TA 2000; the respective interpretation of the term terrorist is provided for in section 40 TA 2000.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_12,

measures. The provisions of the TA 2000 were deemed inadequate to address the terrorist threat and, as a result, new legislation was rushed through Parliament.[4] Consequently, the Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001) came into force in December 2001.[5] This Act builds on the TA 2000 and provides for additional powers.

12.1.2 Indefinite Detention Without Trial

The introduction of the ATCSA 2001 was received with harsh criticism not only from academics, but also from bodies such as the Joint Committee on Human Rights.[6] One of the most controversial features provided for by the Act was the possibility of indefinite detention without trial of foreign nationals suspected of being international terrorists.[7] This form of detention was created to address the fact that suspects could not be put on trial due to the sensitivity of evidence and the high standard of proof required for prosecution, but for whom extradition or deportation was no alternative either.[8] In view of the jurisprudence of the European Court of Human Rights (ECtHR), non-British nationals may not be deported to their state of origin if they face a risk of being tortured in the receiving state, as such a deportation would breach Article 3 of the European Convention on Human Rights (ECHR).[9] Nonetheless, foreign terrorist suspects can still be deported if they present a risk to national security and there is no such risk of torture in the state to which they are deported.[10] On the other hand, it can be argued that, notwithstanding the human rights obstacles, deportation may generally not be a sensible option, because the suspect will be removed from the UK but may continue to operate from abroad.[11]

From its outset, Part 4 of the ATCSA 2001, which included the controversial provisions on the detention without trial, created conflicts with various rights guaranteed by the ECHR, most notably with Article 5 ECHR.[12] Since the enactment of

---

[4] Fenwick, *Civil Liberties and Human Rights*, p. 1332; Walker, *Blackstone's Guide to the Anti-Terrorism Legislation*, pp. 3–5.

[5] It received royal assent on 14 December 2001 and came into force on 20 December 2001, see Statutory Instrument No. 4019/2001).

[6] For such criticism see, inter alia, Fenwick, *MLR* 65 (2002), 724–762; Tomkins, *PL* (2002), 205–220; Reports by the Joint Committee on Human Rights (Session 2001–02), *Anti-Terrorism, Crime and Security Bill, Second Report*, 14 November 2001, and *Anti-Terrorism, Crime and Security Bill, Fifth Report*, 3 December 2001.

[7] Part IV ATCSA 2001.

[8] Fenwick, *Civil Liberties and Human Rights*, p. 1422.

[9] *Chahal* v *United Kingdom*, App. No. 22414/93, 23 *EHRR* 413.

[10] See section 7 Nationality, Immigration and Asylum Act 2002 and section 97A Immigration, Asylum and National Security Act 2006.

[11] Walker, *MLR* 70 (2007), 433, citing the Report of the Privy Councillor Review Committee, *Anti-terrorism, Crime and Security Act 2001 Review: Report* (2003–04 NC 100) Pt D, para. 195.

[12] Fenwick, *Civil Liberties and Human Rights*, p. 1422.

the Human Rights Act 1998 (HRA 1998), most of the rights contained in the ECHR have been incorporated into the United Kingdom's domestic law.[13] The ECHR does not have formal supremacy over other Acts of Parliament and hence the principle of the sovereignty of Parliament remains intact.[14] However, according to section 3 HRA 1998, all legislation is to be interpreted and applied in a way that is compatible with the ECHR so far as possible. Furthermore, the House of Lords can deliver a declaration of incompatibility if it finds that an Act of Parliament is incompatible with the Convention.[15] Such a declaration, however, does not affect the validity or enforcement of the legislation.[16] The government has to repeal the respective statute and, if so desired, introduce new legislation.[17] Consequently, one can conclude that, in practice, the ECHR has gained a supreme rank through its incorporation by the HRA 1998.[18]

Because the government was aware that Part 4 of the ATCSA 2001 clearly infringed the right to liberty, as set out by Article 5 ECHR, it took recourse to the possibility of derogation from Article 5 ECHR, as provided for by Article 15 ECHR.[19] In 2004, the legality of both the provisions of Part 4 of the ATCSA 2001 as well as the government's decision to derogate from Article 5 ECHR was challenged by nine claimants who were detained under section 23 ATCSA.[20] The House of Lords quashed the derogation order and issued an order of incompatibility with regard to section 23 ATCSA 2001.[21] The detention scheme was found to violate the prohibition of discrimination, set out in Article 14 ECHR because of its discriminatory scope. The applicability of the detention rules to foreign suspects only was considered to be the key weakness of the detention system.[22] Notwithstanding these findings, the terrorist attacks in London on 7 July 2005 proved that Part 4 ATCSA 2001 had ignored the fact that the security problem was not predominantly created by foreign nationals but that the threat posed by British extremists was no less imminent.[23]

---

[13] Section 1 (1) HRA 1998.

[14] Grabenwarter, *Europäische Menschenrechtskonvention,* p. 21.

[15] Section 4 (1) and (2) HRA 1998.

[16] Section 4 (6) HRA 1998.

[17] Wadham, Mountfield, Edmundson, Gallagher, *Blackstone's Guide to the Human Rights Act 1998*, pp. 93–97, paras. 6.21–6.31.

[18] Feldman, *Legal Studies* 12 (1999), 178; Grabenwarter, *Europäische Menschenrechtskonvention*, p. 21.

[19] Human Rights Act 1998 (Designated Derogation) Order 2001 (SI No. 2001/3644). See section 15 ECHR for the conditions which have to be met for a derogation to be made. Gearty, *JLSoc* 32 (2005), 25.

[20] *A and others* v *Secretary of State for the Home Department (No. 1)* [2004] UKHL 56; [2005] 2 WLR 87. For in-depth analysis and commentary on the decision, see, for example, Poole, *JLSoc* 32 (2005), 534–61; Hickman, *MLR* (2005), 655–668; Tierney, *MLR* (2005), 668–672.

[21] *A and others* v *Secretary of State for the Home Department (No. 1)* [2004] UKHL 56; [2005] 2 WLR 87.

[22] *Ibid.*

[23] Fenwick, *Civil Liberties and Human Rights*, p. 1422–3; Gearty, *Civil Liberties,* p. 117.

In addition to finding Part IV ATCSA 2001 discriminatory, the House of Lords ruled that the conditions for the United Kingdom's derogation from Article 5 ECHR had no foundation in the actual situation, and therefore also found the provision to be in violation of the right to liberty.[24]

In January 2005 the government acknowledged the declaration of incompatibility and declared that it would seek to introduce new legislation to replace Part 4 ATCSA 2001 in the near future.[25] Subsequently, the Prevention of Terrorism Act 2005 (PTA 2005), which introduced the control order scheme, was enacted in March 2005.[26]

12.2 The Outset of the Control Order System

The PTA 2005 introduced the system of control orders that aims – as can be deduced from the name of the Act – at the prevention of terrorist acts. Control orders are therefore preventive orders that can be imposed on individuals suspected of being involved in terrorism-related activity. They are designed to restrict or prevent the further involvement in such activities.[27] The meaning of control orders is defined in section 1 (1) PTA 2005:

> In this Act "control order" means an order against an individual that imposes obligations on him for purposes connected with protecting members of the public from a risk of terrorism.

A control order can be regarded as being a measure of last resort. From its outset, control orders should only be used to address the threat posed by an individual where prosecution is impossible. Such impossibility can arise from evidence that cannot be used in court, or, with respect to foreign nationals whose presence in the UK is deemed to pose a threat to national security, because of the prohibition to deport them to countries where there is a risk of torture.[28] Due to being designed as a last resort measure, section 8 (2) PTA 2005 provides for a duty of the Secretary of State to consult the chief officer of the police force regarding whether the evidence available could be used for a prosecution of the individual. After an order has been made, the possibility of a prosecution for an offence relating to terrorism

[24] *A and others* v *Secretary of State for the Home Department (No. 1)* [2004] UKHL 56; [2005] 2 WLR 87. In particular, the majority of the Lords regarded the measures to be a disproportionate response to the situation; see, especially, Lord Bingham, para. 73, Lord Hoffmann, paras. 96–97, and Lord Hope, paras. 119–120.

[25] Bonner, *EPL* 12 (2006), 59.

[26] Once more, anti-terrorism legislation was passed through Parliament remarkably swiftly. Elliott, *IJConstL* 4 (2006), 562.

[27] PTA 2005, *Explanatory Notes,* para. 3.

[28] Fenwick, *Civil Liberties and Human Rights*, p. 1439. *Chahal* v *United Kingdom* 23 *EHRR* 413.

must be kept under review.[29] In practice, however, it is feared that the imposition of a control order is being used in preference to prosecution.[30]

Control orders can be imposed on any person suspected of involvement in terrorism-related activity, irrespective of the nationality of that individual.[31] Hence, unlike Part 4 ATCSA 2001, control orders are not designed in a discriminatory manner. Although it was argued that in practice, the majority of control orders imposed have been issued in respect of foreign nationals,[32] the latest data shows that there has been a significant increase in their imposition on British nationals.[33] Control orders do not address a specific stream of terrorist movement and can be imposed irrespective of the terrorist cause.[34]

Section 1 (9) PTA 2005 defines what constitutes "involvement in terrorism-related activity". Like the definition of "terrorism" in section 1 TA 2000, the concept is very broad because it comprises the commission, preparation, or instigation of acts of terrorism; conduct that facilitates any of those acts; conduct that gives encouragement to the commission, preparation, or instigation of such acts, or that is intended to do so; and conduct that gives support or assistance to individuals who are known or thought to be involved in terrorism-related activity.[35] It is immaterial whether the acts of terrorism are specific acts of terrorism or acts of terrorism generally.[36] Attention should be drawn to the fact that the notion of "involvement in terrorism-related activity" extends beyond the definition of terrorism. Unlike the definition of section 1 TA 2000, section 1 (9) PTA 2005 covers individuals who have not themselves taken part in terrorist activity but are associated with terrorism in one of the ways provided for by the PTA 2005.[37]

The core provisions of the PTA 2005, sections 1–9, are subject to annual renewal by order.[38] The order must only be made by the Home Secretary if a draft of the order has been laid before both Houses of Parliament and has been approved by a resolution of each house.[39] Since 2005, the relevant sections have been renewed on

---

[29] Section 8 (4) PTA 2005.

[30] Fenwick, *Civil Liberties and Human Rights*, p. 1440. This issue was raised in the case of *Secretary of State for the Home Department* v *E and another* [2007] UKHL 46, on appeal from [2006] EWCA Civ 1140, [2007] EWHC 651 (Admin), which will be discussed below.

[31] PTA 2005, *Explanatory Notes,* para. 4.

[32] Fenwick, *Civil Liberties and Human Rights*, p. 1440.

[33] Currently, 14 control orders are in operation; eight control orders were imposed in respect of British nationals; the other six are in respect of foreign citizens. Data valid as of 17 September 2007, Control Order Quarterly Statement, http://security.homeoffice.gov.uk/news-publications/news-speeches/494245?version=1. Fenwick, *Civil Liberties and Human Rights*, p. 1440.

[34] PTA 2005, *Explanatory Notes,* para. 4.

[35] Section 1 (9)(a)–(c) PTA 2005.

[36] Section 1 (9)(d) PTA 2005.

[37] Fenwick, *Civil Liberties and Human Rights*, p. 1439.

[38] Section 13 (2) PTA 2005.

[39] Section 13 (4) PTA 2005.

a yearly basis.[40] However, the issue of approval has been accompanied by harsh criticism raised by the Joint Committee on Human Rights in various reports.[41]

Until now, control orders have not been resorted to as frequently as may have been feared by the opponents of the regime.[42] Like most of the other draconian anti-terrorism measures, these have mainly had a symbolic effect and, despite their potential applicability to a large group of people, seem to have been under-used.[43] Although this development is appreciated from a human rights perspective, the rare use of control orders indicates that the need for such a restrictive instrument may not be as great as the British government purports.

12.2.1 Non-derogating Control Orders and Derogating Control Orders

The control order scheme draws a fundamental distinction between two different types of control orders: non-derogating and derogating control orders. Non-derogating control orders impose obligations short of being in breach of Article 5 ECHR.[44] A derogating control order, on the other hand, allows for restrictions that are incompatible with Article 5 ECHR and therefore requires derogation as provided by Article 15 ECHR. By way of a derogating control order, measures such as detention without trial, either in prison or in the form of full house arrest, can be envisaged.[45]

So far, the government has not made a designated derogation in respect to Article 5 ECHR, and therefore no derogating control orders have yet been imposed. However, this does not mean that all non-derogating control orders are automatically within the limits set by the human rights standards of the ECHR.[46] As will be

---

[40] The PTA 2005 was renewed in March 2006, 2007 and 2008 by order (SI 2006 No. 521, SI 2007 No. 706 and SI 2008 No. 559).

[41] See the three reports of the Joint Committee on Human Rights: *Counter-Terrorism Policy and Human Rights: Draft Prevention of Terrorism Act 2005 (Continuance in force sections 1 to 9) Order 2006*, Twelfth Report of Session 2005–06; *Counter-Terrorism Policy and Human Rights: Draft Prevention of Terrorism Act 2005 (Continuance in force sections 1 to 9) Order 2007*, Eighth Report of Session 2006–07; *Counter-Terrorism Policy and Human Rights (Ninth Report): Annual Renewal of Control Orders Legislation 2008*, Tenth Report of Session 2007–08.

[42] Gearty, *Civil Liberties,* p. 118.

[43] Fenwick, *Civil Liberties and Human Rights*, pp. 1333, 1439–40.

[44] Fenwick, *Civil Liberties and Human Rights*, p. 1439. The interpretation that section 15 (1) PTA 2005 provides for a non-derogating control order does not prove helpful because it merely sets out "non-derogating control order means a control order made by the Secretary of State". See Walker, 59 *StanLRev* (2007), 1416.

[45] Fenwick, *Civil Liberties and Human Rights*, p. 1439; Gearty, *Civil Liberties*, p. 117–8.

[46] *Ibid.*

seen from the analysis of the judgments on control orders below, whether a control order infringes on human rights, in particular Article 5 ECHR, depends on the specific obligations and restrictions imposed by the individual order.

The distinction between derogating and non-derogating control orders is reflected in the different means of making a control order and the conditions that have to be met for an order to be imposed. Non-derogating control orders may be made by the Home Secretary whereas derogating control orders can only be made by the court.[47] Furthermore, a different standard of proof is required in relation to the making of the different types of control orders. In respect of non-derogating control orders, the Secretary of State must have reasonable grounds for suspecting that the individual is or has been involved in terrorism-related activity.[48] Notwithstanding the supposedly less invasive nature of a non-derogating control order, it should be emphasised that no criminal trial or civil action is needed in order to subject a person to such an order.[49] Despite this, the obligations imposed by a non-derogating control order may still entail severe restrictions to the individual's ordinary life (see Sect. 12.2, below).

For the imposition of a derogating control order, however, the standard of proof is significantly higher. The court may only make a control order if it appears to the court that there is material evidence that (if not disproved) is capable of being relied on by the court to establish that the individual is or has been involved in terrorism-related activity.[50]

Notwithstanding the importance of the derogating control orders, this article predominantly deals with non-derogating control orders. This is because, until now, there has been no derogating from Article 5 ECHR since the enactment of the PTA 2005, and no derogating control orders have yet been made. As a consequence, unless expressly stated, the following sections solely deal with non-derogating control orders. Even the compatibility of these control orders with Article 5 ECHR has, however, been the focus of controversy. As mentioned before, labelling a control order as non-derogating does not automatically imply that all obligations imposed are indeed compatible with the ECHR. Hence, it was argued that the Secretary of State had issued control orders that were de facto derogating orders.[51] However, this will be dealt with in greater detail in Sect. 12.3 of this chapter.

---

[47] Section 2 (1) PTA 2005 in respect of non-derogating control orders; section 4 (1) PTA 2005 in respect of derogating control orders.

[48] Section 2 (1)(a) PTA 2005.

[49] Fenwick, *Civil Liberties and Human Rights*, p.1439.

[50] Section 4 (3)(a) PTA 2005.

[51] This argument was raised in *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45.

12.2.2 Possible Obligations and Restrictions

The obligations and restrictions that can be imposed by a non-derogating control order are set out in section 1 (4) PTA 2005. Despite providing for all kinds of restrictions, the list of obligations is non-exhaustive.[52] These obligations may entail, inter alia, restrictions on residence, travel, and movement;[53] the prohibition of, or restriction on the possession or the use of certain articles, services, or facilities, such as the possession of a mobile phone or the use of the internet;[54] restrictions on association;[55] submission to electronic tagging;[56] regular reporting;[57] and an obligation to allow entry, search, and seizure powers to be deployed by specified persons.[58]

Most of the non-derogating control orders that have been issued until now have contained similar obligations. They all subjected the controlled persons to an amalgamation of different obligations. As for the case of the six controlled persons in the case of *JJ and others*,[59] all controlled persons were required to live in designated places, specified residences that were one-bedroom flats. They all were subjected to a curfew that required them to remain within their residence save for a period from 10 am to 4 pm.[60] During the curfew hours, the controlled individuals were not even allowed into the common parts of the buildings in which their flats were situated. Furthermore, visitors were only allowed on authorisation by the Home Office for which their personal details and photographic identity had to be supplied. Outside their residences, they were prohibited from meeting anyone by pre-arrangement who had not been given clearance by the Home Office. The controlled persons were subjected to spot searches by the police, and their movements outside the curfew were restricted to a specified area. Moreover, they were required to wear an electronic tag and to report to a monitoring company. Finally, they were not allowed to use or possess any communications equipment other than a landline that had been provided and maintained by the monitoring company.[61]

As the analysis of the case law on control orders will demonstrate in greater detail, it is the amalgamation of various obligations that causes non-derogating control orders to interfere with the life of the controlled person in a severe manner.

---

[52] See the wording of section 1 (4) PTA 2005: "Those obligations may include, in particular (…)".

[53] Section 1 (4) (e)–(i) PTA 2005.

[54] Section 1 (4) (a) and (b) PTA 2005.

[55] Section 1 (4) (d) PTA 2005.

[56] Section 1 (4) (n) PTA 2005.

[57] Section 1 (4) (o) and (p) PTA 2005.

[58] Section 1 (4) (j)–(l) PTA 2005.

[59] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45.

[60] For a summary of the facts, setting out the obligations of the control orders, see *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, para. 20.

[61] *Ibid.*

The PTA 2005 does not specify what obligations can be imposed by way of a derogating control order. To date, no derogating control orders have been issued. However, it must be assumed that those obligations would be in the range of a clear deprivation of liberty, such as detention or a full house arrest.

12.2.3 Duration of Control Orders

A derogating control order ceases to have effect after 6 months.[62] However, at the end of this period, it may be renewed for another period of up to 6 months.[63] The power to renew a derogating control order is exercisable on as many occasions as the deciding court thinks fit, provided that the prerequisite conditions are still met.[64] However, the possibility of renewal is subject to the derogation still being in force. In addition, it must have been declared within the previous 12 months.[65]

A similar regime applies to non-derogating control orders. They can initially be imposed for up to 12 months, and can be renewed indefinitely for 12 months at a time.[66] It should be noted that, when renewing a non-derogating control order, the Secretary of State only has to consider whether it is necessary for purposes connected with protecting the public from a risk of terrorism that the order continues to be in force.[67] In regard to the obligations, the Secretary of State must still consider them necessary for purposes connected with preventing or restricting the controlee's involvement in terrorism-related activity.[68] There is, however, no need to prove that the reasonable suspicion regarding the individual's involvement in any terrorism-related activity still exists.[69]

So far, some of the controlees have been subjected to control orders for a significant length of time.[70] The present possibility of an indefinite duration of control orders has been criticised by Lord Carlile of Berriew QC, the Independent Reviewer

[62] Section 4 (8) PTA 2005.

[63] Section 4 (9) PTA 2005.

[64] Section 4 (10) PTA 2005.

[65] Section 6 (1) PTA 2005.

[66] Section 2 (4) and (6) PTA 2005.

[67] Section 2 (6)(a) PTA 2005.

[68] Section 2 (6) (b) PTA 2005.

[69] Walker, 59 *StanLRev* (2007), 1417.

[70] According to information given by the Home Secretary in a letter of 18 February 2008, two individuals have been on control orders since they were introduced in March 2005. A total of 7 of the current 15 control orders have been on control orders for longer than 2 years. See Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights (Ninth Report): Annual Renewal of Control Orders Legislation 2008*, Tenth Report of Session 2007–08, pp. 24–25, paras. 82–87.

of the PTA 2005, as well as by the Joint Committee on Human Rights.[71] All call for an absolute time-limit of control orders, arguing that in most cases control orders cannot be justified for longer than 2 years. Lord Carlile points out that within that time the utility of the controlee as a terrorist would have been seriously disrupted, and therefore it seems unlikely that the individual would be of operational use to a terrorist plot any longer.[72] Hence, the control order would cease its function to restrict or prevent the individual from further involvement in terrorism-related activity. Lord Carlile suggests that a statutory presumption against the extension beyond 2 years should be introduced.[73]

12.2.4 Procedure

The preventive nature of control orders as well as their being executive measures are mirrored by procedural particularities. These are partly set out in the PTA 2005, but have mainly been established through Part 76 of the Civil Procedure Rules (CPR), which were enacted according to the Schedule to PTA 2005.[74] The provisions on the affirmation and review of control orders are set up as special procedures that are equivalent to those applicable to the Special Immigration Appeals Commission.[75] They involve the use of material not usually admissible as evidence in criminal trial, closed hearings, the non-disclosure of information, and the appointment of special advocates.[76] Control order proceedings are construed as civil proceedings that operate on a lower standard of proof than criminal trials. The control order system enables the executive to curtail an individual's freedom on the basis of reasonable grounds for suspicion, proven in civil proceedings to the balance of probabilities.[77] Moreover, as will be discussed in greater detail throughout this article (see Sect. 12.3.2, below), because of the deliberately construed civil nature of control orders, the suspect is afforded fewer safeguards in terms of the right to a fair trial.[78]

---

[71] Lord Carlile of Berriew, *Third Report of the Independent Reviewer pursuant to Section 14 (3) of the Prevention of Terrorism Act 2005*, 18 February 2008, p. 17.

[72] Lord Carlile of Berriew, *Third Report of the Independent Reviewer pursuant to Section 14 (3) of the Prevention of Terrorism Act 2005*, 18 February 2008, p. 17; Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights (Ninth Report): Annual Renewal of Control Orders Legislation 2008*, Tenth Report of Session 2007–08, pp. 24–25, paras. 82–87.

[73] Lord Carlile of Berriew, *Third Report of the Independent Reviewer pursuant to Section 14 (3) of the Prevention of Terrorism Act 2005*, 18 February 2008, p. 18. He argues, however, that in genuinely exceptional circumstances, the possibility of duration beyond 2 years should still be maintained.

[74] Paragraph 4 of the Schedule to the PTA 2005 provides for the making of rules of court.

[75] For an overview of the nature and the work of the Special Immigration Appeals Commission (SIAC), see, House of Commons Constitutional Affairs Committee, *The operation of the SIAC and the use of Special Advocates*, Seventh Report of Session 2004–05, April 2005.

[76] See the s. 11 (5) PTA 2005 and the Schedule of PTA 2005.

[77] Sandell, *EHRLR* (2008), 121.

[78] This was the decisive issue in the case of *MB*, and is analysed below in greater detail.

Unlike in a criminal trial, the decision to impose a control order can be based mainly or even solely on evidence that would not be admissible in a criminal trial. Such evidence includes intelligence as well as material obtained through the interception of communication.[79] Because of the sensitivity of such material, paragraph 76.2 CPR Part 76 provides for a duty of the court to ensure that information is not disclosed contrary to the public interest.[80] During the last couple of years, and in particular with regard to anti-terrorism measures, the issue of the use of intercept evidence in British criminal procedure has been a matter of great controversy.[81] By now, there are clear indications that the general prohibition might not be upheld for that much longer.[82] It has been argued, however, that the general availability of intercept evidence would not have a great impact on control order cases.[83]

Basing evidence solely or predominantly on material that may not be disclosed to the suspect or their legal representative bears the risk of rendering the proceedings unfair and hence violating the suspect's right to a fair trial. This problem was first addressed in 1997 with regard to immigration deportation decisions. The Special Immigration Appeals Commission (SIAC) Act 1997 introduced the role of the special advocate.[84] These are security-vetted lawyers who are permitted to attend those hearings in which security-sensitive material is disclosed and that therefore are held as closed sessions. Because the control order proceedings are modelled according to those applicable to the SIAC, the PTA 2005 and the CPR Part 76 also provide for the use of special advocates.[85] In control order cases, the function of the special advocate is to represent the interests of the suspects in closed sessions by making submissions to the court in writing or at hearings and to cross-examine witnesses at such hearings.[86] Once the special advocate has seen any closed material, however, he may no longer communicate with the suspect or their legal representative.[87] Although the role of the special advocate surely serves the fairness of the

[79] Section 17 RIPA 2000 prohibits the use intercept evidence in criminal trials. The issue of intercept evidence is discussed in greater detail by John Spencer in this volume.

[80] Paragraph 76.2 CPR Part 76.

[81] For an overview, see the so-called Chilcot Report (Privy Council Review of Intercept Evidence, Cm. 7324 (2008).

[82] See Counter-Terrorism Bill 2008. For an insight into the discussion on the matter see the House of Commons Research Paper, *Counter-Terrorism Bill*, Bill 63 of 2007–08, Research Paper 08/2008, pp. 44–48.

[83] Walker, *CrimLR* (2008), 500.

[84] The Treasury Solicitor's Office: A Guide to the Role of Special Advocates and the Special Advocates Support Office (SASO), p. 4–5.

[85] Walker, *Crim LR* (2008), 498. The use of special advocates is provided for in para. 7 of the Schedule to PTA 2005 and in paras. 76.23–76.25 CPR Part 76.

[86] Paragraph 76.24 CPR Part 76.

[87] Paragraph 76.25 CPR Part 76.

proceedings, the restriction of communication obviously weakens the suspect's opportunities of an effective defence.[88] These constraints have not only been criticised by controlees and their legal representatives but, in protest at the restrictions that they have to work under, a number of special advocates have resigned.[89]

12.2.5 Court Supervision of Control Orders

As has been explained above, derogating control orders can only be made by the court.[90] However, in regard to non-derogating control orders, the court serves as a supervisory body. Because this chapter examines how this function has been carried out in practice, for a better understanding, the role of the court regarding non-derogating control orders shall briefly be described.

According to section 3 PTA 2005, the Secretary of State must seek permission from the court to make a non-derogating control order.[91] The function of the court at the initial stage is to consider whether the Secretary of State's decision that there are grounds to make the order is obviously flawed.[92] The court can only refuse permission, and hence quash the order, if it finds that the decision is obviously flawed.[93] The use of the term "obviously flawed" makes it unlikely that the court will withhold permission at this early stage.[94] On confirmation of the order, the court giving permission must order a hearing.[95] The purpose of the hearing is for the court to determine whether the decisions of the Secretary of State regarding the making of the control order were flawed.[96] First, the court has to decide whether the conditions for making a control order were met, i.e. whether the Secretary of State had reasonable grounds for suspecting that the individual is or has been involved in terrorism-related activity and whether he considered it necessary, for purposes connected with protecting members of the public from a risk of terrorism, to make a control order imposing obligations on that individual.[97] It then has to

[88] This issue was addressed in the case of *Secretary of State for the Home Department* v *E and another* [2007] UKHL 47.

[89] See http://news.bbc.co.uk/1/hi/uk_politics/4405415.stm (accessed 9 July 2008).

[90] Section 4 PTA 2005.

[91] Section 3 (2) PTA 2005. In urgent cases, the Secretary of State can make a non-derogating control order without the permission of the court. He then must apply to the court immediately for obtaining its permission. The court has to consider whether the Secretary of State's decision to make the order was obviously flawed. Further details on the procedure regarding the obtainment of permission on the review of the court are set out in paras. 76.7–76.15 CPR Part 76.

[92] Section 3 (2)(a) PTA 2005.

[93] Sections 3 (2)(b), 3 (6) (a) PTA 2005.

[94] Fenwick, *Civil Liberties and Human Rights*, p. 1445.

[95] Sections 3 (2)(c), 3 (10) PTA 2005.

[96] Section 3 (10) PTA 2005.

[97] Section 3 (10)(a) with reference to the conditions set out in Section 2 (1) PTA 2005.

determine whether the Secretary of State's decision on the imposition of each of the obligations imposed by the order was flawed.[98] In determining whether these decisions were flawed, the court has to apply the principles applicable to judicial review.[99] This means the court can only review the Secretary of State's decision with regard to the recognised grounds for review – irrationality, illegality, procedural error, and proportionality.[100] The court may not, however, substitute its own judgment on the merits for that of the Secretary of State.[101] As described above, the affirmation and review of control orders follow a special procedure, involving the use of closed material and special advocates.

From its outset, the supervisory role of the court may seem rather weak because it is limited to the principles of judicial review. Consequently, the courts may only decide whether the executive acted lawfully, but it cannot give a judgment on the merits. When discussing some recent control order decisions in the following part, however, it will become clear that the courts were ready to fulfil their new task with great dedication. In doing so, the courts have played a significant role in making control orders compatible with the ECHR.

12.3 Control Orders on Trial

In October 2007 the House of Lords delivered three judgments on three different important issues regarding control orders. The most prominent issue regarding the focus of this chapter is the decision dealing with the impact of control orders on the right to liberty. However, the judgments dealing with the other two issues, namely, the impact of control orders on the right to a fair trial as well as the relationship between control orders and the possibility of criminal prosecution should not be ignored either.

12.3.1 Control Orders and the Right to Liberty

In 2006, a court had to rule on the compatibility of control orders with the right to liberty and security as guaranteed by Article 5 ECHR for the first time.[102] As briefly

[98] Section 3 (10)(b) PTA 2005.

[99] Section 3 (11) PTA 2005.

[100] In judicial review proceedings, a court may review decisions taken by the executive. However, the court may only test whether the decision is in line with the recognised principles of judicial review. These principles are illegality, irrationality (in the sense of the so-called "Wednesbury" unreasonableness), procedural impropriety, and proportionality. See on judicial review in general, Loveland, *Constitutional Law, Administrative Law, and Human Rights,* chapters 13 and 14; Sunkin, Grounds for Judicial Review: Illegality in the Strict Sense, in: Feldman (ed.), *English Public Law*, Chapter 14.

[101] Walker, *StanLRev* 59 (2007), 1422–1423.

[102] *Re JJ and others* [2006] EWHC 1623 (Admin).

summed up by A.T.H. Smith in this volume, in the High Court, the case of *JJ and others* was decided by Sullivan J who came to the conclusion that the orders were incompatible with the HRA 1998 because they violated Article 5 ECHR.[103] Finally, after the Court of Appeal had dismissed the Secretary of State's appeal,[104] the House of Lords had to decide whether control orders violated the right to liberty or not.[105]

In *JJ and others*, each of the controlees' orders, in essence, contained the same obligations.[106] They had to live in specially provided one-bedroom flats in an area where they had not lived previously, away from their families and friends. The orders contained curfews for 18 h every day. The controlees were only allowed to leave their flats between 10 am and 4 pm. For the non-curfew hours, they were restricted to an urban area of a maximum of 72 sq. km, which did not extend to the area were they had lived before. Visitors and anyone whom they wanted to meet outside their flat prior to arrangement had to be authorised in advance by the Home Office. The flats could be subjected to spot searches by the police at any time. They were only allowed to use the land line in their flat and had no internet access. They had to wear an electronic tag and had to report to a monitoring company before leaving their flat and on return to the flat.

The House of Lords had to decide whether these obligations amounted to a deprivation of liberty and therefore violated Article 5 ECHR, or not. Because the United Kingdom has not ratified Protocol 4 to the Convention, Article 2 of the Protocol dealing with restrictions of movement does not apply. However, despite there being two different provisions, the ECtHR has recognised that "The difference between deprivation and restriction upon liberty is nonetheless merely one of degree or intensity, and not one of nature or substance".[107] The crucial question was what notion of liberty is applied by Article 5 ECHR. Does the right to liberty only cover individual liberty in the classic sense, and hence, only literal physical restraint constitutes a deprivation of liberty?[108] Or must liberty be understood in a broader sense so that a deprivation of liberty can occur in other forms that fall short of classic detention?

In order to reach a conclusion, their Lordships analysed the applicable case law of the ECtHR at great length. Although a series of Strasbourg decisions exist,

---

[103] *Ibid*.

[104] *Secretary of State for the Home Department* v *JJ and others* [2006] EWCA Civ 1141, [2007] QB 446.

[105] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45.

[106] For the exact obligations contained in the orders, see *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, para. 20 and Annex I to Sullivan J's judgment, *Re JJ and others* [2006] EWHC 1623 (Admin).

[107] *Guzzardi* v *Italy*, judgment of 6 November 1980 (Application no. 7367/76).

[108] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, para. 36, Lord Hoffmann citing the case of *Engel* v *The Netherlands*, judgment of 8 June 1976 (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72), para. 58.

dealing with 24-h house arrest,[109] regarded by the court as a clear deprivation of liberty, and overnight curfews that did not amount to such deprivation,[110] none of these cases are in fact comparable to control orders. Therefore, the judges had to decide on the issue by applying the general criteria developed in the decisions *Engel* and *Guzzardi*.[111] Thus, their starting point had to be the concrete situation of the individual while taking into account a whole range of factors such as the nature, duration, effects, and manner of execution or implementation of the penalty or measure in question.[112] A further important consideration had to be that, although a single feature of an individual's situation might not be regarded a deprivation of liberty taken on its own, the combination of measures considered together might, however, have that result.[113]

By a majority of three votes to two, the House of Lords ruled that the control order obligations amounted to a deprivation of liberty, and consequently, Sullivan J had been correct in quashing the orders.[114] The majority argued that the cumulative effect of the obligations had deprived the controlees of their liberty in breach of Article 5 ECHR.[115] Lord Bingham held that in his view they were in practice in solitary confinement for the lengthy period of 18 h every day for an indefinite duration with very little opportunity for contact with the outside world.[116] Baroness Hale added that not only during the curfew hours, every aspect of their lives was severely controlled and that in several respects a prisoner might even be better off.[117] Furthermore, Lord Brown emphasised that the dividing line between deprivation of liberty and restriction of liberty of movement could not vary according to the particular interests (such as countering terrorism) sought to be served by the restraints imposed. Article 5 ECHR represented a fundamental value and was absolute in its

[109] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, para. 14. *Mancini* v *Italy*, judgment of 2 August 2001 (Application no. 44955/98); *Vachev* v *Bulgaria*, judgment of 8 July 2004 (Application no. 42987/98), *Nikolova* v *Bulgaria* (No. 2) judgment of 30 September 2004 (Application no. 40896/98).

[110] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, para. 18; *Raimondo* v *Italy*, judgment of 22 February 1992 (Application no. 12954/87); *Cianciminio* v *Italy*, decision of 27 May 1991 (Application no.12541/86).

[111] *Engel* v *The Netherlands*, judgment of 8 June 1976 (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72); *Guzzardi* v *Italy*, judgment of 6 November 1980 (Application no. 7367/76).

[112] *Engel* v *The Netherlands*, judgment of 8 June 1976 (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72), para. 59; *Guzzardi* v *Italy*, judgment of 6 November 1980 (Application no. 7367/76), paras. 92, 94.

[113] *Guzzardi* v *Italy*, judgment of 6 November 1980 (Application no. 7367/76), para. 95.

[114] For the majority: Lord Bingham of Cornhill, Lord Brown of Eaton-under-Heywood and Baroness Hale of Richmond; Lord Carswell and Lord Hoffmann dissented; see *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45.

[115] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, paras. 21, 24.

[116] *Ibid.*, para. 24.

[117] *Ibid.*, para. 62.

terms. He regarded liberty as a right too precious to be discarded except in times of genuine national emergency, which was not suggested in the present case.[118]

Lord Hoffmann and Lord Carswell who did not regard the control orders to amount to a deprivation of liberty pointed out that after all Article 5 ECHR only protected the individual against deprivation of liberty *stricto sensu*.[119] They argued that it was essential not to give an over-expansive interpretation to the concept of deprivation of liberty.[120] In their view, the situation of the controlees, although greatly restricted compared with an ordinary person, could not be compared with someone in prison.[121]

JJ and others can be regarded as the leading case on the issue of the right to liberty. However, although the focus was on different issues, also in the cases of *E* and *AF*, the House of Lords had to decide on the compatibility of the control orders with Article 5 ECHR.[122] In these cases, the orders were regarded not to violate Article 5 ECHR. The curfews were significantly shorter than in *JJ and others*, 12 and 14 h, respectively.[123] However, it was deemed to be more decisive that the controlees lived with their families and therefore were not forced to lead an (almost) isolated life, as had been the case in *JJ and others*.[124]

With the exception of Lord Brown, the Law Lords refrained from stating any absolute maximum for the duration of curfews that in their opinion would still be in line with Article 5 ECHR. Despite holding with the majority that the control orders in question amounted to a deprivation of liberty, Lord Brown indicated that, in his opinion, curfews of up to 16 h a day would not amount to a deprivation of liberty.[125] Attention should be paid to the fact that supposedly this indication of a maximum length caused the Home Secretary to adjust several control orders accordingly. In the light of the judgments in *JJ and others* in the lower courts, in four cases the curfews were reduced from 18 to 14 h and then to 12 h. Once Lord Brown had indicated the absolute maximum of 16 h,[126] however, the curfews were increased to 16 h, and one new control order containing a 16 h curfew was

[118] *Ibid.*, para. 107.

[119] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, paras. 40, 69.

[120] *Ibid.*, para. 44.

[121] *Ibid.*, para. 45.

[122] *Secretary of State for the Home Department* v *E and another* [2007] UKHL 47; *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46.

[123] *Ibid.*, para. 7; *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46, para. 7.

[124] See especially the case comment by Feldman, *CamLJ* 67 (2008), p. 6–7, and Walker, *CrimLR* (2008), p. 497.

[125] *Secretary of State for the Home Department* v *JJ and others* [2006] EWCA Civ 1141, paras. 105 and 108.

[126] *Secretary of State for the Home Department* v *JJ and others* [2006] EWCA Civ 1141, para. 105.

imposed.[127] Due to this development, the Joint Committee on Human Rights showed its disappointment that the lengthy judgments regarding the compatibility of control orders with the right to liberty in Article 5 ECHR, after all, had merely resulted in reducing the curfew period from 18 to 16 h.[128] This may indicate that the Home Office does not view these judgments to be fundamentally undermining the value or viability of the control order system in general.[129]

The differing decisions show that the length of the curfew alone will not necessarily give a clear answer to the question whether a control order infringes Article 5 ECHR, or not. Instead, a whole range of factors have to be taken into account. This is in line with the holistic approach taken by the ECtHR. However, despite these judgments giving an indication regarding when a control order clearly oversteps the line to a deprivation of liberty, they offer little guidance for borderline cases. This seems to cause problems insofar as, with its counter-terrorism measures, the British government has constantly shown a clear willingness to impose measures that operate on the edge of human rights guarantees. This balancing act has become most obvious with regard to control orders. Concern was raised regarding the House of Lords' failure to give precise guidance on the boundaries of Article 5 ECHR and to provide a clear distinction between a deprivation of liberty, and a mere restriction of liberty.[130]

12.3.2 The Right to a Fair Trial

It has been depicted above that the control order system implies various deviations from a criminal trial. It operates on a rather low level of proof because reasonable suspicion is sufficient for the issuing of a control order. More strikingly even, this suspicion can be based solely on material that is not disclosed to the suspect because of national security. In the cases of *MB* and *AF*, the House of Lords had to decide whether the control order proceedings were compatible with the right to a fair trial guaranteed by Article 6 ECHR.[131]

The Home Office applied for control orders against *AF* and *MB*. According to the open statements, they allegedly were Libyan or Islamist extremists, moreover, *MB* intended to travel to Iraq to fight against coalition forces.[132] The evidence supporting these allegations was contained in the closed material. Therefore,

---

[127] Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights (Ninth Report): Annual Renewal of Control Order Legislation 2008, Tenth Report of Session 2007–08, pp. 13–14, para. 39.

[128] *Ibid*, p. 14, para. 40.

[129] Walker, *CrimLR* (2008), 497.

[130] Sandell, *EHRLR* (2008), 131.

[131] *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46.

[132] *Ibid.,* paras. 5, 37.

neither of them knew the case against them and they argued that the modified procedural and evidential rules of the PTA 2005 and the CPR Part 76 violated Article 6 ECHR.[133] They claimed that the control order proceedings engaged the criminal limb of Article 6 ECHR or, alternatively, that they should entail the same procedural safeguards.[134]

First of all, it had to be assessed whether control orders were indeed civil measures, or whether they amounted to the determination of criminal charges, and hence whether the controlees also enjoyed the rights of Article 6 (2) and (3) ECHR, which only apply to criminal cases.[135] Although Article 6 ECHR provides considerable safeguards for both civil matters and criminal charges, Article 6 (2) and (3) ECHR contain important additional safeguards for those charged with a criminal offence.[136] These include the presumption of innocence[137] and the right to examine or have examined witnesses and to obtain the attendance and examination of witnesses on their behalf under the same conditions as witnesses against them.[138]

Prima facie, control orders are civil matters. The Joint Committee of Human Rights has argued, however, that non-derogating control orders could amount to the determination of a criminal charge against the individual who is the subject of the order.[139] Applying the criteria that were set out in *Engel* v *The Netherlands*,[140] they provide three reasons for this classification. First, the reason for the imposition of a control order is conduct of a particularly serious criminal nature, second, the nature of the restrictions imposed are of a nature and severity equivalent to a criminal penalty, and third, their duration makes them tantamount to a criminal sanction considering the possibility to renew them an indefinite number of times.[141] It was argued that a fourth reason for control orders falling within the criminal limb of Article 6 ECHR could be adduced from the requirement in section 8 PTA 2005, obliging the Home Secretary to consult with the police prior to making a control order with regard to the possibility of a criminal prosecution.[142]

The ECtHR's approach on the matter was established in *Engel* and ever since the decisive criteria has been reiterated in ensuing jurisprudence.[143] The Court focuses

---

[133] *Ibid.*, para. 3.

[134] *Ibid.*, paras. 3, 15.

[135] *Ibid.*, paras. 13–18.

[136] Sandell, *EHRLR* (2008), 124.

[137] Article 6 (2) ECHR.

[138] Article 6 (3)(d) ECHR.

[139] Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: Draft Prevention of Terrorism Act 2005 (Continuance in force of sections 1 to 9) Order 2006*, Twelfth Report of Session 2005–06, para. 50.

[140] *Engel v The Netherlands*, judgment of 8 June 1976 (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72).

[141] *Ibid,* para. 51.

[142] Sandell, *EHRLR* (2008), 124.

[143] *Engel* v *The Netherlands*, judgment of 8 June 1976 (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72), *Öztürk* v *Germany*, judgment of 21 February 1984 (Application no. 8544/79), paras. 49–50; *Lauko* v *Slovakia*, judgment of 2 September 1998 (Application no. 4/1998/907/1119), paras. 56–59.

on three considerations: the formal classification of the matter in the domestic legal system, the nature of the offence, and the severity of the penalty.[144] However, despite being the starting point for the Court's considerations, the domestic classification is the least important, because the meaning of "criminal charge" in the context of the Convention is autonomous, and cannot be circumvented through the state's own classification.[145]

Regarding the classification of control orders, one can start with the observation that the suspicion that may trigger a control order is a suspicion of criminal activity.[146] However, according to the Strasbourg approach, the decisive factor seems to be the consequences of a measure. The crucial issue is whether the measure entails consequences that are predominantly punitive.[147] Interestingly, in *JJ and others*, Lord Bingham (for the majority) held that control orders could be compared with detention in an open prison.[148] In the case of *MB* and *AF*, however, where the issue at stake was whether control orders in fact constituted the determination of a criminal charge with regard to Article 6 ECHR, the Law Lords unanimously rejected their criminal nature for the purposes of the Convention.[149] Lord Bingham justified this finding essentially on the grounds that the purpose of control orders was preventative, not punitive.[150] As has been pointed out before, this view, however, is not in line with the ECtHR's approach, which turns on consequences, not on legislative or executive purpose.[151]

Despite the House of Lords ruling being moot on this issue and even slightly contradictive to its judgment in *JJ and others*, this did not result in a victory for the Home Office. In fact, the court upheld the alternative assertion made on behalf of *AF*, ruling that although control orders did not fall within the criminal limb of Article 6 ECHR, they were sufficiently stringent to demand procedural protection "commensurate with the gravity of the potential consequences", that is, procedural safeguards similar to those entailed by criminal charges.[152]

---

[144] *Engel* v *The Netherlands*, judgment of 8 June 1976 (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72), para. 82.

[145] *Öztürk* v *Germany*, judgment of 21 February 1984 (Application no. 8544/79), para. 49; *Engel* v *The Netherlands*, judgment of 8 June 1976 (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72), paras. 81–82.

[146] Sandell, *EHRLR* (2008), 125.

[147] *Öztürk* v *Germany*, judgment of 21 February 1984 (Application no. 8544/79), para. 53.

[148] *Secretary of State for the Home Department* v *JJ and others* [2007] UKHL 45, paras. 21, 24.

[149] *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46.

[150] Lord Bingham's judgment is the only one which is fully reasoned on this question, see *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46, para. 24.

[151] Sandell, *EHRLR* (2008), 125; *Öztürk* v *Germany*, judgment of 21 February 1984 (Application no. 8544/79), para. 53.

[152] *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46, para. 24.

Turning to the substantial issue, whether the control order system was unfair, the House of Lords first stated that they regarded the special advocate procedure as being far from perfect. However, they concluded that at least to a certain extent, it redressed the inequality of arms that necessarily existed in control order proceedings.[153] Regarding the fairness of these proceedings, they applied the test whether the process as a whole involved significant injustice to the controlled person.[154] Although they regarded that such injustice had been done in the present cases, they did not go as far as to make a declaration of incompatibility.[155] Instead, they agreed with Baroness Hale's view that the non-disclosure provision of paragraph 76.2 CPR Part 76 had to be read down, in accordance with the court's duty under section 6 (1) HRA 1998,[156] in a way that would make it compatible with Convention rights. Consequently, the precept of non-disclosure should be given effect "except where to do so would be incompatible with the right of the controlled person to a fair trial".[157]

This judgment has some significant practical implications. Because the House of Lords shifted the procedural rule in favour of fairness, special advocates can now argue for disclosure to those they represent. Judges may not require the Home Secretary to disclose all evidence necessary for the individual to enjoy a fair hearing.[158]

This decision was regarded as being much more uncomfortable for the Home Office than the judgment regarding Article 5 ECHR.[159] One human rights group, JUSTICE, even welcomed the judgment as "a victory for fairness over secrecy".[160] However, it is still far from a declaration of incompatibility that had been advocated by some and that would have sent an even stronger message to the executive.[161]

---

[153] *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46, paras. 35, 90.

[154] *Ibid.,* paras. 25–43, 92.

[155] *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46. Lord Bingham was the only one who seriously considered the possibility of a declaration of incompatibility, whereas Baroness Hale regarded this option as inappropriate; see paras. 44 and 70.

[156] Section 6 (1) HRA 1998 provides: "It is unlawful for a public authority to act in a way which is incompatible with a Convention right."

[157] *Secretary of State for the Home Department* v *MB*; *Secretary of State for the Home Department* v *AF (FC)* [2007] UKHL 46, paras. 44, 70, 92

[158] Sandell, *EHRLR* (2008), 128.

[159] Walker, *Crim LR* (2008), 500.

[160] JUSTICE press release, 31 October 2007, available from: http://www.justice.org.uk/inthenews/index.html (last accessed 1 September 2008).

[161] Sandell, *EHRLR* (2008), 129.

12.3.3 Control Orders as a Measure of Last Resort?

Throughout the legislative procedure, it has been emphasised by the government that the prosecution of terrorist suspects is the preferred choice, and hence control orders should only serve as a measure of last resort.[162] Because this relationship between prosecution and the imposition of control orders initially seemed inadequately mirrored in the underlying legislation, section 8 was inserted into the PTA 2005. This section imposes a duty on the Secretary of State to consult with the police regarding the possibility of prosecuting the terrorist suspect for an offence.[163] The duty does not only comprise a one-time decision when the Secretary of State initially decides whether to make a control order or not,[164] but rather, embraces continuous obligations to keep the possibility of prosecution under review throughout the duration of a control order.[165]

In the case of *Secretary of State for the Home Department* v *E and another*,[166] however, the issue arose regarding how this duty had to be carried out and what consequences a breach of that duty should entail. The House of Lords unanimously held that the conditions precedent to the making of a control order were set out in section 2 (1) PTA 2005 only, and that the duty to consult with the police was not included as a qualifying condition.[167] However, they emphasised that section 8 PTA 2005 contained a continuing duty for the Home Secretary to assist the Chief Officer in keeping the decision to prosecute under review.[168] Despite their ruling that a breach of the duty imposed by section 8 PTA 2005 did not imply the invalidity of a control order, the court admitted that such a breach might, however, provide grounds from which to infer that the decision of the Home Secretary to impose a control order was flawed, if, for example, it could be demonstrated that the Home Secretary had acted irrationally or for an improper purpose.[169] Nevertheless, in the case of *E*, the court did not find that the breach of the duty imposed by section 8 PTA 2005 resulted in the control order being faulted, and thus did not quash the order.[170]

---

[162] This was voiced, inter alia, by Charles Clarke, the then Home Secretary, Hansard, HC Vol. 431, col. 339 (February 23, 2005), This has been reiterated on several occasions, e.g. in July 2007, the Government Response to Lord Carlile's Second Report on Control Orders.

[163] Section 8 (1) PTA 2005.

[164] Section 8 (2) PTA 2005.

[165] Section 8 (4) PTA 2005.

[166] *Secretary of State for the Home Department* v *E and another* [2007] UKHL 47.

[167] *Ibid.,* para. 15.

[168] *Ibid.,* para. 18.

[169] Forsyth, *CamLJ* 67 (2008), 3.

[170] *Secretary of State for the Home Department* v *E and another* [2007] UKHL 47, paras. 21, 23, 29, 34, 36.

The significance of the judgment in the case of *E* may be less obvious than in the other decisions in regard to the compatibility of control orders with Convention rights. However, considering that the government has repeatedly pronounced that prosecution should have absolute priority over the imposition of control orders, it is interesting to note, that until now, no controlee has subsequently been prosecuted apart for breaches of his obligations imposed by the order.[171] Therefore, concern has been expressed that it seems questionable if priority is really given to criminal prosecution rather than control orders that provide for indefinite and extensive grounds, however, without the judicial safeguards accorded to the suspect in the criminal trial.[172] Due to the absence of any prosecutions subsequent to the imposition of a control order, it would have been appreciated had the House of Lords argued for more serious consequences for breaches of the duty of section 8 PTA 2005.

12.4 Consequences for the Right to Liberty and Concluding Remarks

Control orders are executive measures through which severe restrictions on the individual's right to liberty can be imposed. Although the courts have been ready to scrutinise control orders most thoroughly and hence have taken on their supervisory role in a welcome manner, the measure remains controversial. The issue of the compatibility of the control order system with human rights appears for now to have been decided in favour of the government's view in so far as the system has not as such been declared incompatible with the ECHR.

However, as can be seen from the judgments of the House of Lords, this only is true with certain reservations. The question of whether a control order that is deemed to impose a mere restriction on the freedom of movement in fact constitutes an infringement of the right to liberty has to be decided on a case-by-case basis. Even if the restrictions are regarded to fall short of a violation of Article 5 ECHR, control order obligations are still a severe intrusion into the ordinary life of the controlled person. The obligations available for a control order resemble those that are usually imposed on offenders who are subject to parole. The crucial difference, however, is that control orders are executive measures, whereas the parole obligations are preceded by a judgment of a criminal court. Even though a court is involved when a control order is made, as long as the court is not supposed to carry out a comprehensive supervisory function on the merits of each case, control orders remain a tool that is dominated by the executive.

---

[171] Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights (Ninth Report): Annual Renewal of Control Orders Legislation 2008*, Tenth Report of Session 2007–08, p. 20, para. 65.

[172] *Ibid.*

Despite the landmark rulings of the House of Lords, control orders remain open to abuse. Although the decision in *JJ and others* indicates the absolute limit for a deprivation of liberty, a stronger line of argument would have been appreciated. The lack of sufficient guidance becomes more obvious when taking the cases of *AF* and *E* into account. In these cases, daily curfews of 12 and 14 h were regarded to be compatible with Article 5 ECHR. These curfews still constitute a significant length of time, and, especially in combination with other obligations, amount to a severe restriction if not a deprivation of the individual's liberty. Although they applied a wider notion of deprivation of liberty than literal physical restraint, the Lords' interpretation of Article 5 ECHR does not provide an encouraging outlook.

In conclusion, with regard to the right to liberty, it seems that with the introduction of control orders, the borders of free movement have indeed been moved. Considering that until now, only a relatively small number of orders have been issued, the question arises whether the control order system, and the challenges to the right to liberty posed by it, is necessary after all. It seems that the same result could be achieved by means of surveillance, implying lesser threats to human rights. In contrary though, the issue would arise whether information gathered throughout such surveillance would be admissible in court, and hence one would be faced with the same situation that lead to the introduction of control orders in the first place. However, bearing in mind that the notion on the use of intercept evidence seems to be changing, and that the creation of specific terrorist offences allows for the prosecution of all kinds of preparatory acts, the British anti-terrorism legislation as a whole would still allow for the prevention and prosecution of terrorist activity before a terrorist attack has occurred.

References

Carlile of Berriew, Lord (2008). *Third Report of the Independent Reviewer pursuant to section 14 (3) of the Prevention of Terrorism Act 2005*, 18 February 2008.

Elliott, M. (2006). United Kingdom: Detention Without Trial and the "War on Terror", *International Journal of Constitutional Law* (*IJConstL*) 4, 553–566.

Feldman, D. (2008). Deprivation of Liberty in Anti-Terrorism Law, *Cambridge Law Journal (CambLJ)* 67, 4–8.

Fenwick, H. (2002). The Anti-Terrorism, Crime and Security Act 2001: A Proportionate Response to 11 September? *Modern Law Review (MLR)* 65, 724–762.

Fenwick, H. (2007). *Civil Liberties and Human Rights*. 4th ed., Oxford: Routledge.

Forsyth, C. (2008). Control Orders, Conditions Precedent and Compliance with Article 6 (1), *Cambridge Law Journal (CambLJ)* 67, 1–4.

Gearty, C. (2007). *Civil Liberties*. Oxford: OUP.

Grabenwarter, C. (2008). *Die Europäische Menschrechtskonvention*. 3rd ed., Munich: Beck.

Hickman, T. R. (2005). Between Human Rights and the Rule of Law: Indefinite Detention and Derogation Model of Constitutionalism, *Modern Law Review (MLR)* 68, 655–668.

House of Commons (2008). Research Paper, *Counter-Terrorism Bill*, Bill 63 of 2007–08, Research Paper 08/2008, 26 February 2008.

House of Commons Constitutional Affairs Committee (2005). *The Operation of the Special Immigration Appeals Commission (SIAC) and the Use of Special Advocates*, Seventh Report of Session 2004–05, Volume 1, HC 323–1, 3 April 2005.

Joint Committee on Human Rights (2006). *Counter-Terrorism Policy and Human Rights: Draft Prevention of Terrorism Act 2005 (Continuance in Force Sections 1 to 9) Order 2006*, Twelfth Report of Session 2005–06, 14 February 2006.

Joint Committee on Human Rights (2007). *Counter-Terrorism Policy and Human Rights: Draft Prevention of Terrorism Act 2005 (Continuance in Force Sections 1 to 9) Order 2007*, Eighth Report of Session 2006–07, 28 February 2007.

Joint Committee on Human Rights (2008). *Counter-Terrorism Policy and Human Rights (Ninth Report): Annual Renewal of Control Orders Legislation 2008*, Tenth Report of Session 2007–08, 19 February 2008.

Loveland, I. (2006). *Constitutional Law, Administrative Law, and Human Rights*. 4th ed., Oxford: OUP.

Poole, T. (2005). Harnessing the Power of the Past? Lord Hoffmann and the *Belmarsh Detainees* Case, *Journal of Law and Society (JLSoc)* 32, 534–561.

Privy Councillor Review Committee, *Anti-terrorism, Crime and Security Act 2001 Review: Report* (2003–04 NC 100).

Sandell, A. (2008). Liberty Fairness and the UK Control Order Cases: Two Steps Forward, Two Steps Back, *European Human Rights Law Review (EHRLR)* 120–131.

Sunkin, M. (2004). Grounds for Judicial Review: Illegality in the Strict Sense. In David Feldman (ed.), *English Public Law*. Oxford: OUP.

Tierney, S. (2005). Determining the State of Exception: What Role for Parliament and the Courts? *Modern Law Review (MLR)* 68, 668–672.

Tomkins, A. (2002). Legislating Against Terror: the Anti-Terrorism, Crime and Security Act 2001, *Public Law (PL)* 205–220.

The Treasury Solicitor's Office (2006). A Guide to the Role of Special Advocates and the Special Advocates Support Office (SASO) – Open Manual.

Wadham, J., Mountfield, H., Edmundson, A., Gallagher, C. (2007). *Blackstone's Guide to the Human Rights Act 1998*. 4th ed., Oxford: OUP.

Walker, C. (2002). *Blackstone's Guide to the Anti-Terrorism Legislation*. Oxford: OUP.

Walker, C. (2007). Keeping Control of Terrorists Without Losing Control of Constitutionalism, *Stanford Law Review (StanLRev)* 59, 1395–1463.

Walker, C. (2008). Terrorism: Prevention of Terrorism Act 2005 ss. 2 and 3 – Non-derogating control order – Whether "Deprivation of Liberty" Under European Convention on Human Rights Article 5, *Criminal Law Review (CrimLR)* 486–503.

Chapter 13
Telephone-Tap Evidence and Administrative Detention in the UK

John R. Spencer

13.1 Introduction

In the UK, it is currently the law that the contents of intercepted telephone calls, or letters intercepted by transmission in the post, are generally inadmissible as evidence in civil or criminal proceedings; and this so, whether the interception was carried out legally or illegally. This is, of course, in sharp contrast to position everywhere else in the world, including the rest of the common law world, where (broadly speaking) the rule is that the intercepts are admissible, provided they were obtained legally. It is also counterintuitive to the point where even intelligent people with legal training sometimes find it hard to grasp. (When setting examination papers in evidence for law students, I regularly include, as a trap to the unwary, a problem where a piece of damning evidence against the defendant is an intercepted phone-call: and although the class has heard the rule explained in lectures, at least a third invariably tells me, wrongly, that the intercept is admissible, provided it was lawfully obtained.)

"Difficulties with the rules of evidence" when suspected terrorists are prosecuted in the criminal courts are one of the reasons that the government has repeatedly put forward as a justification for trying to find other means of locking them up: such as internment without trial, or "control orders"[1] - the current euphemism for house arrest – by command of the Home Secretary. But measures such as these are highly unpopular in certain quarters, and at the time of writing, this has produced a backlash against the rule that currently excludes the use of intercepts in criminal proceedings. The argument of those who wish to change the rule, naturally, is that if

J. Spencer (✉)
University of Cambridge, Cambridge, UK
e-mail: jrs1000@cam.ac.uk

[1] *See also* Forster, this volume.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_13, © Springer Science+Business Media, LLC 2010

intercepts were admissible in the criminal courts, suspected terrorists could then be prosecuted, and the pressure to create what has been described as "a 'shadow system' of criminal justice, driven the executive"[2] would then abate.

The aim of this chapter is to tell the strange story of how the current evidential ban in the UK arose – and the even stranger story of how it has taken us so long to abolish it.

13.1.1 The Ban: Ancient or Modern?

Contrary to what might be thought, the ban on intercept evidence is not an ancient construct of the common law, derived from its real or supposed concern for civil liberties. It is recent, and a creature of statute; and a statute, furthermore, that was not inspired by any great desire to protect human rights or civil liberties. The statute from which it originated was the Interception of Communications Act (IOCA) 1985, which was Mrs Thatcher's government's legislative response to the condemnation of the UK by the European Court of Human Rights in Strasbourg in the *Malone*[3] case – a response which *The Times* described as "one of this Government's 'dumb insolence' measures (like the Bill on caning in schools and earlier provisions regarding the equal treatment of the sexes), in which the minimum action possible is grudgingly taken to comply with the letter of rulings under international agreements."[4] But for the statutory ban, there is no doubt that the contents of intercepted communications would be admissible in evidence – at any rate, provided the interception was lawful.

In the common law, as elsewhere, the basic rule of evidence, both criminal and civil, is that anything is admissible in evidence if it is relevant[5]; from which it follows that, if an intercept contained material that was logically relevant to the defendant's guilt or innocence, it ought in principle be admissible as evidence in his trial. Before the statutory ban was enacted, indeed, such evidence was admissible, and sometimes used. An often-quoted case in which such evidence was used to powerful effect was the trial of Mary, Queen of Scots, in 1587, where part of the evidence against her were letters, intercepted and decoded by Queen Elizabeth's secret service, which showed she knew about the

---

[2] A. Blick, T. Choudhury and S. Weir, *The rules of the game – terrorism, community and human rights*, a report by Democratic Audit for the Joseph Rowntree Trust (2006).

[3] *Malone v UK* (1984) 7 EHRR 14.

[4] Editorial, 6 March 1985.

[5] "The main general rule governing the entire subject is that all evidence that is sufficiently relevant to an issue before the court is admissible and all that is irrelevant, or insufficiently relevant, should be excluded." Rupert Cross, *Evidence*, 3rd ed 1967, 13; cf (ed Colin Tapper) *Cross and Tapper on Evidence*, 11th ed 2007, 69.

plot to depose Elizabeth and put her on the throne instead.[6] Evidence of this sort has also featured in more recent *cause célèbres*, including the trial of Art O'Brien and others for seditious conspiracy in 1923.[7] Some 40 years later, the legal status of an intercepted letter was considered by the House of Lords. In *Rumping v DPP*,[8] the House of Lords had to pronounce on the admissibility of an incriminating letter the defendant had written to his wife, and which had been intercepted on its journey between the writer and the postbox. It was held, by a majority, to be admissible – and those who thought otherwise based their argument on the confidentiality of communications between a husband and a wife, not the inadmissibility of private letters that have been intercepted. And after the statutory ban was enacted in 1985, the UK courts, which do not like it, have construed it narrowly, and in the process have held to be properly admissible various intercepts to which the statutory ban, as so narrowly interpreted it, did not apply. In *Aujla*,[9] for example, the Court of Appeal held that the ban only applied to intercepts obtained in the UK; and in consequence, the court could receive in evidence the contents of the defendants' incriminating telephone calls with various accomplices in Holland, intercepted by the Dutch police. It follows that, in the UK, it is the statutory ban, and that alone, which makes such evidence inadmissible – and that if the provisions that impose it were repealed, intercept evidence could then be freely used.

How did this ban come about? In order to explain this, it is necessary to give a thumbnail account of the official interception of communications in the UK – the earlier part of which is conveniently summarised in an official report, the Report of the Birkett Committee in 1957,[10] which drew in turn on the reports of two Parliamentary Committees that, a century before, had examined the opening of letters in transit by what was then called the General Post Office.[11]

13.1.2 The History of Interceptions in the UK

The General Post Office, which until recently was a government agency enjoying a monopoly on the transmission of letters, was originally created with the express aim of enabling the government to spy on its citizens by opening and reading

---

[6] The trial of Mary Queen of Scots is printed in 1 *Howell's State Trials*, 1161.

[7] *The Times*, 5 July 1923. This example together with a number of others were given in §149 of the Report of the Birkett Committee, *see* footnote 10.

[8] [1964] AC 814.

[9] [1998] 2 CrAppR 16; noted [1999] Cambridge Law Journal 43. The decision was approved by the House of Lords in *R v P* [2002] 1 AC 146.

[10] *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications*, Cmnd. 283 (1957).

[11] *See* footnote14.

their correspondence. Indeed, this was candidly stated in the preamble to the Ordinance of 1657 by which the General Post office was set up, which said that one of the advantages of the new arrangement was that it provided the best means "to discover and prevent many dangerous and wicked designs which have been and are daily contrived against the peace and welfare of the Commonwealth, the intelligence whereof cannot well be communicated but by letter of escript."[12] The practice was, it seems, for letters to be opened by postal officials when they received a written warrant from the Secretary of State; an authorisation which, according to the theories of constitutional law that then prevailed, would have been enough to make any actions lawful. The practice of opening letters on the order of the Secretary of State, and its presumed lawfulness, were recognised in the Post Office (Revenue) Act of 1710, which made it an offence to open or delay letters "… except by an express warrant in writing under the hand of one of the principal Secretaries of State." The provisions of this Act were re-enacted in a series of later statutes, one of which, after telegrams had been invented, extended the same rule to them as well.

In 1844, the interception of letters became the centre of a political row when it came to light that the Home Secretary, Sir James Graham, had ordered, at the request of the Austrian government, the opening of the correspondence of the Italian nationalist, Giuseppe Mazzini, who was then living in exile in England. Mazzini was a popular figure with important friends, and popular too in Britain was the struggle for the independence of Italy, a large part of which was then occupied by Austria. The revelation that the government had been tampering with a political exile's correspondence to do a favour to an oppressive foreign government caused an uproar which vented itself in heated debates in Parliament, and outside it in a brief fashion for writing "Not to be Grahamed" on envelopes.

In Parliament divergent views were expressed on the legality of what the Home Secretary had done. The government, of course, claimed that it was legal, but Lord Campbell – later to become Lord Chief Justice and then Lord Chancellor – argued that it was not. In the end, as Campbell sarcastically remarks in his autobiography, "both parties were pleased to have the matter hushed up by the appointment of a Select Committee."[13] In fact there were two of these, one for the House of Commons and one for the House of Lords. Their Reports[14] described past practice, concluded that previous Secretaries of State had not generally abused their supposed power to

[12] Birkett Report, §31.

[13] *Life of John, Lord Campbell*, edited by M.S. Hardcastle (London, John Murray, 1881), vol. 2, 187–188.

[14] Report from the Secret Committee of the House of Lords relative to the Post Office. 1844. 601 (7 August 1844). Report from the Secret Committee on the Post Office. 1844. 582 (5 August 1844). The Committees were "secret" in the sense that they took evidence in private, which was not published with the Report; but the Report from the Commons Committee was published with a long Appendix with documents relating to the history of the Post Office and the interception of letters.

intercept letters,[15] and expressed the view that such a power was necessary. And they left open the question of whether, for the future, the practice should be regulated by statute. In response to these Reports a Member of the House of Commons sought leave to introduce a Bill to make interceptions illegal, but this the Government successfully opposed, and so the "Mazzini affair" eventually died down. But the incident seems to have left its mark on the official memory. Sir James Graham, the Home Secretary involved, ruefully told his friends and family that "he would go down to posterity famously only for having opened letters at the Post Office"[16] – as indeed he has. It led, for a time, to greater caution in the issue of such warrants. And ever since, the leitmotif of governmental reaction to the interception of communications has been the supreme importance of keeping the existence of the practice secret.

When a national telephone system was put under the control of the General Post Office in 1912, its officials first acted on the assumption that they could tap telephones whenever they thought fit, and in consequence, "arrangements for the interception of telephone conversations were made directly between the Security Service or the Police Authorities and the Director-General of the Post Office,"[17] with no warrants from the Secretary of State being asked for, or received. In 1937 there was a change of policy on this, and it was agreed between the Home Secretary and the Director-General of the Post Office that, in future, telephones should only be tapped on the receipt of a warrant from a Secretary of State, similar to those issued for the interception of letters. But the provisions of the Post Office Acts which appeared to recognise, or possibly to grant, an express power in the Secretary of State to authorise the opening of letters were never extended to cover the authorisation of telephone intercepts; and so the legality of this practice was in doubt – and long remained so.

It was under this ram-shackle legal framework that telephones were tapped and letters were opened both for law enforcement purposes, and also in the interests of "national security." Although for neither type of intervention was there any clear legal basis, the Secretaries of State operated – or at any rate, claimed to operate – within internal guidelines which were relatively clear. Officially, interception warrants would be issued to the police and to Customs and Excise for law enforcement purposes only where the offence in question was "really serious," "normal methods of investigation must have been tried and failed, or must, from the nature of things, be unlikely to succeed if tried," and there was "good reason to think that an interception would result in a conviction."[18] Interception warrants were issued at the

[15] Lord Campbell gleefully recorded (footnote 13) that the debates about the Mazzini affair revealed that "Of all the Secretaries of State, Mr Fox, during his short tenure of office, appeared to have carried the practice to the greatest extremes." Charles James Fox (1749–1806) was a political figure who was generally thought of as a friend of public liberties.

[16] *Life and Letters of Sir James Graham 1792–1861*, ed. C.S. Parker, (John Murray, London, 1907), 447.

[17] Birkett Report, §40.

[18] Birkett Report, §64.

instance of the Security Services where there was "a major subversive or espionage activity that is likely to injure the national interest" and the "the material likely to be obtained by interception must be of direct use in compiling the information that is necessary to the Security Service in carrying out the tasks laid upon it by the State."[19] However, complaints were made from time to time that warrants were issued, particularly in security cases, in situations which appeared to fall outside these guidelines; and these in turn provoked a more general complaint that these practices took place without any clear legal basis, let alone any form of legal redress if they were unreasonably used.

One of these periodic outcries involved an incident which became known as the "Marrinan case." A barrister called Patrick Marrinan found himself under investigation by the Bar Council following stories in the press that he had improperly obstructed justice for the benefit of a notorious London gangster, Billy Hill, and the Home Secretary of the day (Gwilym Lloyd George) decided to help the investigation along by releasing to the Bar Council the transcripts of intercepts incriminating Marrinan that had been made by the authorities when tapping Hill's phone. The end of the story was that Marrinan, who unlike Mazzini deserved little sympathy, was eventually disbarred; but before this happened, the release of the intercepts to the Bar Council had sparked a public row,[20] which the government (like its predecessor a century before) deflected by setting up a Committee, the Birkett Committee, whose report was mentioned earlier in this chapter.

This Committee produced a number of conclusions and recommendations, the first of which was to condemn the Home Secretary's decision to release the Marrinan intercepts to the Bar Council as "mistaken." Its recommendations for change, however, were all relatively minor, and in essence the Committee gave the existing informal system of regulation a clean bill of health. It did not make the obvious point that intercepts made to catch criminals raise different issues from intercepts made for purposes of national security, and that if it needs to be the Home Secretary who authorises them on grounds of national security, it would be preferable if judges authorised those that the police make to catch criminals. And although the Committee was unable to identify any clear legal basis for the Secretary of State to authorise the tapping of telephones, it then failed to make the point that, if the practice was to continue, a proper legal basis therefore ought to be created. In fact, the Birkett Committee was, in retrospect, the dampest of damp squibs – and its main interest is the clear account it gave of the situation as it then existed, and how it had evolved.

One of the points to emerge from the Birkett Report was that a convention had grown up to the effect that, in the criminal justice context, intercepts should only ever used for operational purposes, and that the resulting evidence should not produced in court. According to the Committee, "… the Home Office insists that the power [to intercept communications] should be exercised for the purpose of detection only, primarily on the ground that the use of the information so obtained, if used in court,

[19] Birkett Report §67.

[20] An account of Marrinan's later unsuccessful attempts to sue various people over these allegations appear in the Law Reports as *Marrinan v Vibart and Another* [1963] 1 QB 234 and 528.

would make the practice widely known and destroy its efficacy to some degree."[21] So sensitive were "the authorities" on this point, indeed, that they even wanted to stop the Birkett Committee publishing figures about the number of interception warrants that were issued.[22] But the Committee was sceptical. Although it condemned the release of the Marrinan intercepts to the Bar Council, which it saw as only a "private body or domestic tribunal,"[23] the Committee "could see no reason why in a proper case the evidence should not be tendered" in a court of law. And against the wishes of the Home Office, it insisted on publishing some statistics in its Report.

The reason the Home Office gave to Birkett for not allowing intercept evidence to be used in court – that this would give the game away by showing criminals that interceptions happen, and so destroy their utility as an investigative tool – has been repeatedly recycled in the 50 years that followed. In 1985, it was the official reason given for the enactment of a legal ban on the use of such evidence in the IOCA, and more recently, it has been put forward as the official reason for maintaining the ban in the face of mounting pressure to abolish it. But this argument seems particularly weak. That the authorities sometimes tap telephones and open letters has been widely known for many years. Indeed, it was public concern about this that led to the Birkett Committee being created. And if the public in general is aware of this, why should the government (or anyone else) imagine that, of all people, spies, subversives, and major criminals are not? Fingerprints and DNA profiles are useful forms of evidence; but it would not occur to us to prevent their use at trials, lest this should induce more criminals to wear gloves or other forms of protective clothing.

It is difficult to avoid the suspicion that this argument about the risk of alerting criminals has been used, at least sometimes, to mask other arguments that Ministers and civil servants in the Home Office have been less prepared to use, at any rate in public. At the time of the Birkett Report, a further reason might well have been an official fear that, if an attempt were made to use such evidence in court, this would lead to a legal challenge on the ground that it had been unlawfully obtained – and this challenge, if upheld, would have exposed the fact that there was no legal basis for interception as things stood, and so forced the government to stop doing it. And after 1985, when the Secretary of State's power to issue interception warrants had acquired a statutory basis, the real reason could well have been a fear that, if the resulting evidence were used in court, this might lead to arguments about the basis on which the warrant had been granted, with the attendant risk of the Secretary of State being told by a judge that, although he had in principle the legal power to authorise interception, in the case in hand he had exceeded it.[24]

---

[21] Birkett Report §152.

[22] Birkett Report §119.

[23] Birkett Report §101.

[24] It is possible to see in this a parallel with the bizarre arguments that were put forward by the government to resist public pressure for the introduction of tape-recording of interviews with suspects: one of which was that, as soon as the tape-recorder was switched on, every suspect would say "Aagh! Stop torturing me and I will tell you anything!" On this, see generally John Baldwin, "The police and tape recorders," [1985] *Criminal Law Review* 695.

The Birkett Report, and the minor administrative changes that were made in response to it, did not bring public complaints about the interception of communications to an end. At regular intervals thereafter, complaints were made, in particular, about the apparently excessive use of telephone tapping on "national security" grounds.[25] In partial response to these, in 1980, the Government announced the appointment - initially without any statutory basis – of a Commissioner, whose role was to conduct a continuous check that the official procedures were being followed, and to report at intervals to the Prime Minister. This did little to improve public confidence, particularly when, in response to an emollient report which the then Commissioner, Lord Bridge,[26] had produced at short notice at the request of the Prime Minister (Mrs Thatcher), Roy Jenkins, a former Home Secretary, wrote an explosive letter to *The Times* saying that the Commissioner had "made himself appear a poodle of the executive."[27] Then in 1981, the Royal Commission on Criminal Procedure said that telephone taps and other forms of covert surveillance in the context of criminal investigations should be regulated by statute, and that warrants should be issued not by the Home Secretary, but – as with search warrants – by the courts.[28] But although the government eventually accepted most of this Committee's other recommendations about investigative powers, and secured their enactment in the Police and Criminal Evidence Act 1984, its recommendations on covert surveillance did not find favour. And so intercepts, even in criminal cases, continued to be made on the basis of warrants issued by the Secretary of State – usually the Home Secretary – under the arrangements of dubious legality described in the Birkett Report a quarter of a century before.

13.1.3 The Malone Case, and the Creation of the Statutory Ban

In 1985, these arrangements eventually led to the condemnation of the UK in the *Malone* case. Unlike most of the recent cases which had given rise to unease and criticism, the background to this case was a criminal investigation by the police, rather than surveillance of possible subversives by MI5 (the security service). Malone, an antiques dealer, was prosecuted for handling stolen goods. At his trial, it emerged that his telephone had been tapped by the police, on the basis of a warrant issued by the Home Secretary, and executed by the Metropolitan Police. In response to this, Malone went to the High Court seeking a declaration that the tapping of his telephone in these circumstances was unlawful. Malone's main

[25] For an account, *see* K.D. Ewing and C.A. Gearty, *Freedom under Thatcher* (Oxford, Clarendon Press, 1990) Chap. 3.

[26] 1917–2007; Law Lord from 1980 to 1992.

[27] 12 March 1985. Mr Jenkins later publicly withdrew this comment following Lord Bridge's dissent in the *Spycatcher* case, in which his judgement, unlike that of his brother judges, was uncomfortable to the executive.

[28] *The Royal Commission on Criminal Procedure, Report*, Cmnd 8092 (1981), §3.53–3.60.

argument was that the Home Secretary's warrant could not render lawful the acts of the police when they tapped his phone. This was because the famous eighteenth century case of *Entinck v Carrington*[29] had established that – contrary to popular opinion at the time – the mere issue of warrant from the King or his Secretary of State could not render lawful an act which the law otherwise forbade. Such a warrant, it was there held, could only be effective if it had a statutory basis; and the defendant, who had entered and searched the plaintiff's property on the basis of warrant from the Secretary of State, was liable in damages for trespass.

After hearing 80 days of argument, the judge, Sir Robert Megarry VC, delivered a lengthy judgment in which he dismissed Malone's action.[30] It was true, Sir Robert said, that a warrant from the Secretary of State could not make something lawful when otherwise it was not. But whereas entering another person's house without his consent was in principle an unlawful act – a trespass – intercepting another person's telephone calls was not. It was, in effect, something that, as English law then stood, anyone was free to do at any time, whether he had a warrant from the Secretary of State or not. This state of affairs, the judge added, might well be contrary to Article 8 of the European Convention on Human Rights, which guarantees, within limits, a right to privacy; but as things then stood "the Convention does not, as a matter of English law, confer any direct rights on the plaintiff that he can enforce in the English courts."

Malone then took his case to Strasbourg, where, unsurprisingly, the UK was condemned.[31] Article 8 of the European Convention guarantees the right of everyone "to respect for his private life, his home and his correspondence," and provides that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the freedoms of others"; and, said the Strasbourg Court, the law of UK failed to respect this right because the fuzzy administrative arrangements under which telephones were tapped on the authority of the Secretary of State could not be regarded as a set of legal rules, and, so did not satisfy the requirement of Article 8 that any interference with a person's privacy by a public authority should be "in accordance with the law."

Although it was clear that the UK would have to put the interception of communications on a legislative basis to comply with its obligations under Article 8, the Strasbourg Court – to the surprise and disappointment of some commentators[32] – gave no guidance as to what the contents of this legislation ought to be; and from Mrs Thatcher's government, the reaction was a Bill that, as we saw earlier, was described by *The Times* as one of the government's "dumb insolence" measures, designed to

[29] (1765) 19 St. Tr. 1029.

[30] [1980] QB 49.

[31] *Malone v UK* (1984) 7 EHRR 14.

[32] Ewing and Gearty, footnote 25, p.59.

comply with the letter of the UK's international obligations, but not their spirit. In broad outline, the Bill which later became the IOCA 1985 just gave statutory authority to the informal arrangements that had existed heretofore. In particular, it provided that the authority for granting permission for the opening of letters and the tapping of telephones should be, as previously, the Secretary of State, and this should be so not only when the security services wished to do this in the interests of national security, but also when the police wanted to do it in the context of an investigation into crime. And it set out, as the grounds on which the Secretary of State could issue such a warrant, the same sort of things as were mentioned in the "internal guidance," which the Birkett Committee described in its Report 30 years before.

However, the IOCA 1985 did more than just confirm the status quo. It made it, for the first time, a criminal offence for anyone to intercept communications except in pursuance of a warrant from the Secretary of State; although as we shall see later, the drafting of the new offence left a number of important holes. It put the Commissioner, created informally in 1980, on a statutory footing. And it also set up a statutory Tribunal to which, in theory, those who were aggrieved because their communications had been intercepted might make a formal complaint. But the powers of this new Tribunal were severely limited, because as a result of the "small print" in the provisions that created it, the only matter that the Tribunal could investigate was whether, in a given case, an interception warrant had been issued, and if so, whether this had been done on the appropriate statutory grounds. In particular, it had no power to investigate whether an unauthorised interception had taken place.[33]

Furthermore, a guiding principle of this piece of legislation was to ensure, so far as possible, that nothing in connection with the Secretary of State's issue of interception warrants, or interception of communications in pursuit of them, could ever be investigated in the ordinary courts. Thus, as regards the Tribunal, it provided that it should not give its reasons (as against its general conclusions) to the complainant, and – most unusually – that the Tribunal's decisions, including its decisions relating to its jurisdiction, should "not be subject to appeal or liable to be questioned in any court." And it seems to have been in pursuit of this general policy that, in addition, the IOCA 1985 changed the law (though not the current practice) by providing that, in future, evidence obtained by intercepting letters in the post or tapping telephones should be inadmissible in the courts.

This policy of "keeping judges out" was not given as the reason for the creation of this ban when the Bill was being prepared and then introduced. Indeed, the government did not condescend to give any reason for the ban at all. On this point, the White Paper that was the forerunner of the Bill – a slender document of 12 A5 pages only - merely said "The Bill will provide for controls over the use of intercepted material. By making such material generally inadmissible in legal proceedings it will ensure that interception can be used only as an aspect of investigation, not of prosecution."[34]

---

[33] The duties of the Tribunal were extended to cover other forms of covert surveillance by the RIPA 2000. For an account of the Tribunal and its present functions, *see* Victoria Williams, *Surveillance and Intelligence Law Handbook*, (Oxford, OUP, 2005).

[34] *The interception of communications in the UK*, Cmnd. 9438 (February 1985), §12(f).

This White Paper and the public debates that it provoked were mainly concerned with other aspects of the matter. But the editor of *The Times* saw the point, when in an editorial[35] he said "The Bill proposes unnecessarily wide measures to protect confidentiality – extending even to a ban on references in any court or tribunal to the very possibility that official sources could engage in illegal tapping." And the point was not lost on those who commented on the legislation afterwards.[36]

13.1.4 The Scope of the Ban

In its original form, the ban was contained in section 9 of the IOCA 1985, the key parts of which were as follows:

1. In any proceedings before any court or tribunal, no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest
   a. that an offence under section 1 [i.e., the new offence of intercepting communications without a warrant] has been committed by any of the persons mentioned in subsection (2) below or
   b. that a warrant has been or is to be issued to any of those persons.
2. The persons referred to in subsection (1) above are
   a. any person holding office under the Crown,
   b. the Post Office and any person engaged in the business of the Post Office, and
   c. any public telecommunications operator and any person engaged in the running of a public telecommunications system.

Two further subsections set out a list of minor exceptions where the rule prescribed by section 9 did not apply – at the head of which, of course, were prosecutions for the new criminal offence of unlawful interception.

In the space of a few years, this provision spawned a body of intricate case law which must rank as one of the most difficult chapters in the history of the law of evidence. The problems that it raised attracted the attention of the House of Lords (*qua* final court of appeal) on no less than four occasions between 1993 and 2001. A full account of its ramifications would cover many pages. Fortunately, only an outline account of them is necessary here, and this will now be given in the remaining paragraphs of this section.

As is clear from its wording, the ban imposed by section 9 consisted of two parts: *either* evidence revealing the fact that the Secretary of State had issued a warrant *or* evidence revealing that any person holding an official position had carried out an interception without a warrant when he needed one, and by doing so, had committed an offence under section 1.

---

[35] 6 March 1985.

[36] Ewing and Gearty, footnote 25, 83.

But what was meant by evidence that "revealed" one or other of these matters? On one possible interpretation, the prosecution (or, if they had it, the defence) were free to put the product of an intercept in evidence if they wished to do so, and the only effect of section 9 was to prevent any further questions being asked that bore on the circumstances in which the intercept had taken place.[37] This was not, of course, what the government had had in mind when devising section 9, and unsurprisingly the courts, after a period of some confusion, eventually rejected this line of argument, and held that the effect of section 9 was to render inadmissible the fruit of any intercept that had been obtained either under a warrant or without one, where the law required one to be obtained.[38] (When section 9 was eventually replaced by a new and similar provision in the Regulation of Investigatory Powers Act (RIPA) 2000, the drafting of the new provision made this point clear beyond all doubt.)

But when, exactly, did the law require a warrant?

In *Effick*,[39] some suspected drug dealers were foolish enough to communicate by using mobile telephones which produced radio signals that were picked up not only by the device which then fed them into the landlines of the Post Office but also by a group of police officers armed with a portable radio in the flat next door; and what they so heard was admitted in evidence at the drug dealers' eventual trial, which resulted in their conviction. When eavesdropping, the police had acted without a warrant. On appeal, the defendants argued that the evidence had been admitted in contravention of section 9, because it revealed that the police had committed an offence under section 1 of the Act. Their argument failed, both in the Court of Appeal and in the House of Lords, on the ground that what the police had done here did not require a warrant from the Secretary of State, and hence had not involved the commission of an offence under section 1. This was because, when properly construed, section 1 of the IOCA only made it an offence to intercept a telephone message when it was passing through a *public* system, the mobile phones that the defendants in this case were using were part of a *private* system - and though winging their way towards a public system, the signals had been intercepted by the police before they had got there.

Although helpful to the police in this and other cases, this narrow construction of the offence created by section 1 meant that it failed to carry out its main supposed aim, which was to protect the privacy of citizens by making it illegal for all and sundry (including journalists) to eavesdrop on their private conversations. In January 1993, this gap in the law was demonstrated with stunning clarity by the interception and subsequent "splashing" in the popular press of Prince Charles's now notorious "Tampax" conversation with Camilla Parker-Bowles, which made it clear beyond any doubt that they were having an affair; and in another case, 4 years later, it led to the condemnation of the UK by the European Court of Human Rights

[37] *See* Steyn LJ's judgement in *Effick* (1992) 95 CrAppR 355 in the Court of Appeal: taking a position which in *Morgans v DPP* (*see* footnote 38) he later acknowledged to be wrong.

[38] The argument was finally laid to rest in *Morgans v DPP* [2001] 1 AC 315; noted by Munday, [2000] CLJ 267.

[39] [1995] 1 AC 309.

at Strasbourg for failing to protect its citizens' right to privacy as guaranteed by Article 8 of the Convention.[40]

To jump ahead in the story, this gap in the law was filled shortly afterwards, when section 1 of the IOCA was replaced by a wider offence created by section 1 of the RIPA 2000 – for breach of which, in 2007, a journalist and private investigator who had spied upon the private conversations of the Royal family were sent to prison.[41] The 2000 Act continued the ban on the use of intercept evidence in legal proceedings, and the ban in its new form, like the earlier one, prohibited the use of any evidence that revealed the commission of an offence of unlawful interception. The result of this, of course, was to extend the ban by making the fruits of telephone intercepts inadmissible where the tap had been carried out on a private network, and so reversing the result in *Effick*.

In *Preston*,[42] the issue was whether the ban in section 9 applied equally to the defence. Preston was accused (with others) of conspiracy to import drugs. They were caught, as the prosecutor disclosed, as result of the police intercepting their telephone calls. Preston accepted that he had done the acts the prosecution alleged but sought to rely on the defence of duress. The telephone intercepts, he said, had they been available in evidence, would have helped to establish this defence, and for this reason, should have been disclosed by the prosecution as part of their general duty to disclose "unused material" in their possession that might be helpful to the defence. These intercepts had not been so disclosed, and indeed could not have been, because after the police had used them to catch the defendants, the tapes and transcripts had been destroyed.[43] And the fact that this had happened, said Preston, made it unfair for the Crown to continue with the case against him, and so the judge should have stopped the proceedings as an abuse of process. The House of Lords held that the ban in section 9 applied to the defence as well as to the prosecution, and that it therefore trumped the normal duty of disclosure.

That the ban on intercept evidence shuts out such evidence even where it is of use to the defence must generate a feeling of unease. In relation to the facts of Preston's case, this is reduced (a little) by prosecuting counsel's statement to the court that he had been reliably informed that the intercepts, now destroyed, lent no support to the defence that Preston was trying to put forward.[44] And in relation to other cases yet to come, it is tempered (a little) by comments from the House of Lords to the effect that, though not bound to disclose such evidence to the defence, the police ought to disclose it to the prosecution lawyers, to enable them to consider whether they ought to drop the case. The decision of the House of Lords in *Preston*, and its qualifying comments about the duty to disclose intercepts potentially helpful

[40] (1997) 24 EHRR 523.

[41] *R v Goodman and Mulcaire*, *Media Guardian*, 26 January 2007.

[42] [1994] 2 AC 130.

[43] Quite properly, because s.6 of the IOCA required this to be done.

[44] Preston took his case to Strasbourg, arguing that the ban on the use of intercept evidence infringed his rights under Article 6 of the Convention; but his application was rejected by the Commission: *Preston v UK*, 2 July 1997.

to the defence to the prosecution lawyers, was later confirmed by statute, first in 1996[45] and then again in 2000.[46] But despite this, the possibility that the ban on intercept evidence could in some case result in the suppression of cogent evidence of innocence, and so contribute to the conviction of an innocent defendant, has been one of the recurrent arguments for its abolition.[47]

A third doubtful point that reached the House of Lords concerned the type of conduct to which the offence in section 1 of the IOCA (and hence the ban in section 9) applied. This section - and the section of RIPA 2000 that replaced it – referred to intercepting communication "in the course of transmission… by means of a… telecommunication system." And so, of course, neither the offence nor the evidential ban applies to words overheard by planting bugs in rooms or cars, or using other technological devices to eavesdrop on conversations held face to face, which were (and still are) freely admissible in evidence.[48] Nor, according to the House of Lords in *Preston*, did the ban apply to evidence of "metering": keeping a record of the numbers which were called from a given phone, or which called it. And in practice, evidence of this sort is widely used in criminal trials to suggest by implication that X was planning crimes with Y, even though the contents of their conversations cannot be put before the court. But what about the intermediate case, in which the device installed on someone's line records not the words he speaks, but the numbers that he subsequently keys in having got through to the number that he originally dialled? This was one of the points that went to the House of Lords in *Morgans v DPP*.[49] The defendant was prosecuted for fraudulently using X's telephone by (in effect) dialling up X, and then dialling a series of other numbers, which enabled him to use X's phone to make long and expensive calls to the Philippines, for which X's line was charged. This fraud was detected by putting a device on the defendant's line which recorded all the digits that were dialled when using it, a printout from which was put before the court of trial in evidence. The House of Lords held that this constituted making an "intercept," so the evidence was not admissible, and the conviction based on the evidence had to be quashed.

The fourth doubtful point about the scope of section 9 to reach the House of Lords concerned the admissibility or otherwise of evidence, not of the intercept itself, but of a confession resulting from it. In *Sargent*,[50] a telephone engineer, suspecting that his ex-wife might be responsible for an arson attack on his house and

---

[45]Criminal Procedure and Investigations Act 1996, s.3(7) and 8(7), forbidding the prosecution to disclose intercepted material to the defence as part of its general duty to disclose "unused material."

[46]RIPA 2000, s.18(8), providing for the disclosure of intercept material to prosecuting lawyers to enable them to decide whether a prosecution should be halted.

[47]*See*, inter alia, David Ormerod and Simon McKay, "Telephone intercepts and their admissibility," [2004] *Criminal Law Review* 15; Matthew Ryder, "RIPA reviewed," *Archbold News*, Issue 4, 5 May 2008, 6.

[48] Khan [1997] AC 558.

[49] [2001] 1 AC 315.

[50] [2001] UKHL 54, [2003] 1 AC 347.

car, used his position to tap her telephone, and so recorded an incriminating conversation between her and the defendant Sargent. The police arrested Sargent and in interview confronted him with the tape, at which point he confessed. Quashing his conviction, the House of Lords held that the effect of section 9 was to make the confession inadmissible, as well as the intercept that had provoked it.

The decision in *Sargent* puts a spotlight on another oddity about the ban in section 9. As explained earlier, it operates by making inadmissible any evidence suggesting that (i) a warrant has been issued or (ii) an offence has been committed by tapping a telephone (or intercepting a letter) without one. But the second limb of the ban was so phrased that it only applied where the offence of unlawful interception (if there was one) was committed by a person holding one of a number of official capacities: a police officer, a member of the security services, or an official of the telephone company. In *Sargent*'s case, the telephone had been tapped, illegally, by a telephone engineer acting outside the scope of his duty, and the prosecution sought to argue that in consequence the ban did not apply, and so the evidence was admissible. This argument was rejected, the court taking the position that what counted was the status of the person who carried out the tapping, not whether he was acting in the course of his official duties. However, from all this, it is clear that, if a telephone conversation or a letter was illegally intercepted by someone who had no official position – a journalist, for example – the contents of the intercept *would* be legally admissible. And so the position, broadly speaking, is that telephone taps obtained *lawfully* are *in*admissible, but those that are *un*lawfully obtained are *ad*missible, provided the breach of the law was sufficiently flagrant; a bizarre paradox, on the face of it, though one that makes some degree of perverted sense if we remember that the purpose of the ban is simply to protect the actions of officials from examination by the courts. (Needless to say, this strange feature of section 9 of the IOCA 1985 was carried over when in 2000, it was replaced by section 17 of RIPA.)

The four House of Lords cases discussed in the previous paragraphs contain only part the story about what is and is not excluded by the statutory ban on intercept evidence first created by section 9 of the IOCA 1985 (and then re-reacted 15 years later by section 17 of RIPA). Thus, to mention a few other points, as the ban only applies to telephone conversations intercepted "in the course of transmission," it does not apply to tape recordings made of words as they are spoken into the mouthpiece of the telephone at one end of the conversation,[51] or as they emerge from the earpiece of the receiver at the other.[52] Nor does it apply to material intercepted "in the course of transmission" where the tap has been placed on the line with the consent of either sender or receiver in the context of a "surveillance operation" carried out under Part II of RIPA.[53] Nor, by statute, does it apply where the intercept was of a letter or a phone call made from a prison or a high-security mental hospital[54]; in

[51] *R v E* [2004] 1 WLR 3279; [2004] 2 CrAppR 29 (484).

[52] *R v Hardy et al*. [2002] EWCA Crim 3012, [2003] 1 CrAppR 30 (494).

[53] RIPA s.3(2); subsection (1) of this section also says that no warrant is required in the rather more unlikely event that *both* parties consent.

[54] RIPA s.4, and Regulations made by the Secretary of State under it.

consequence of which, at the high-profile trial of Huntley for the Soham murders in 2003,[55] the court was able to hear the contents of incriminating calls made by Huntley from Woodhill prison, and his girlfriend Maxine Carr from Holloway.[56] And more fundamentally, the ban does not extend to the fruits of telephone tapping carried out abroad. So in *Aujla*[57] the defendants were convicted of conspiracy to smuggle illegal immigrants into the UK on the basis of telephone conversations tapped in Holland by the Dutch police which, of course, would not have been admissible if they had been tapped by the UK police in England, however lawfully.

Sections 17 and 18 of RIPA 2000 re-enacted the ban imposed by section 9 of the IOCA 1985, and also extended it, as we have seen, to the intercepts made on private telephone systems. The new provisions, which are much longer than the old one, were also intended to clear up various points of doubt arising from the earlier law. But in the process, regrettably, they have not made the law any easier to understand. This is clear from *Attorney-General's Reference (No 5 of 2002)*,[58] the first case in which the new provision, like its predecessor, found its way into the House of Lords. In this case, some policemen were suspected of corruption, and the Chief Constable had taps placed on their phone extensions. With these, incriminating conversations were recorded, which the prosecution proposed to use against the officers at trial. The prosecution took the position that the taps had been placed on a "private system" by the "controller" of the system, a practice which RIPA permits to be done without a warrant, and hence did not fall within the statutory ban. The defence sought to show that the taps were, in fact, placed on a "public system," in which case the ban applied. The judge interpreted section 17 to mean that this issue could not be explored at trial, a situation which made the use of the evidence "unfair," in consequence of which it should be excluded.[59] The House of Lords held that, on a proper interpretation of section 17, the judge was wrong, and this disputed issue could have been explored at trial. In reaching this decision, however, the judges criticised the drafting of the new provision. Lord Bingham, having quoted an earlier judge's comment[60] that the IOCA was a "short but difficult statute," said that the new one "is both longer and even more perplexing." And expanding on this theme, the writer who commented on the case in the *Criminal Law Review* said: "Having agonised over its provisions for too many hours, this commentator can

[55] The shocking murder in 2002 of the two schoolgirls, Holly Wells and Jessica Chapman – which became a *cause célèbre*.

[56] *See Intercept Evidence: Lifting the Ban*, JUSTICE 2006, §5 and §103.

[57] Footnote 9.

[58] [2004] UKHL 40, [2005] 1 AC 264.

[59] Under section 78 of the Police and Criminal Evidence Act 1984, which provides: "In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it."

[60] Lord Mustill, in *Preston*. And compare Lord Lloyd in his *Inquiry into Legislation against Terrorism* (footnote 63): "In my six years as a Commissioner under the Act, I was never able to discern why the section is drafted so obliquely" (§7.7).

only endorse that view by suggesting that it must be one of the most complex and unsatisfactory statutes currently in force."[61]

13.1.5 The Arguments For and Against the Ban

Lawyers from other parts of the world, where telephone-tap evidence is universally admissible, are astonished when they hear about the ban on telephone-tap evidence in the UK. They can see there might be good libertarian arguments against allowing the state to intercept its citizens' private communications at all. But if interception is allowed, as it is in the UK, the arguments in favour of admitting the products of it are so obvious, and so strong, that they find it difficult to imagine what the argument for excluding it could be. In this part of the chapter, the official arguments will be examined, together with the arguments the other way. And foreign readers, I suspect, will be surprised by what they read.[62]

The central argument for introducing and maintaining the ban is that, if the evidence were admissible, this would "compromise methods of interception": in other words, criminals and terrorists would learn that their communications are intercepted, and the way that this is done, and once alerted, would avoid using these means of communication, so that a valuable tool for gathering information would be lost. Subsidiary arguments are that abolishing the ban would "harm the relationship between the police and the intelligence services," that it would "hamper the ability to adapt to rapid changes in communications technology," and that it "would increase the burden on intelligence services, police and prosecutors."

As suggested earlier in this chapter, the central argument about alerting criminals, terrorists, and subversives to the fact that communications are intercepted seems most implausible, since it is widely known in the UK that this is sometimes done. If the general public is aware of this, why should criminals, terrorists, and subversives, of all people, be ignorant of it? As Lord Lloyd (of whom more later) said in his official review of terrorist legislation in 1996:

> Sophisticated criminals are well aware that their telephones are, or may be, tapped…. As for the fear that criminals would cease to use the telephone altogether, I regard this as fanciful. Drug dealers planning an importation, or terrorists planning to plant a bomb, must communicate with each other and with those who are directing the operation by some means. It cannot be done by pigeon post. There is no practicable alternative to the use of the telephone.[63]

Supporters of the ban say that, quite apart from alerting criminals and others to the fact that their communications are being intercepted, if this evidence were admis-

---

[61] David Ormerod, in [2005] *Criminal Law Review* 220, 223.

[62] In 2006, the arguments were set out and analysed with great lucidity in a report published by JUSTICE, and what follows here adopts much of what said in this report. *See Intercept evidence: Lifting the ban. A JUSTICE report*. October 2006. (Available online at the JUSTICE website.)

[63] *Inquiry into Legislation against Terrorism*, Cm 3420 (1996), §7.17.

sible in court it would lead to the details becoming public of the way that this is done. But this argument is unconvincing, too. If prosecutors could use intercept evidence when they want to, this would not force them to reveal its existence when they do not. If security considerations made it wiser not to use it, they could "leave it in the cupboard." To this, supporters of the ban respond by saying that, even if the prosecutor decided to do this, the methods would still end up in the public domain because the evidence would have to be revealed to the defence as "unused material." But this is not the case because where information is sensitive it is protected by the rules relating to public interest immunity, alias "PII."[64]

Of the rules on public interest immunity, the first is that the prosecution are only obliged to disclose unused material that might be helpful to the defence in resisting the accusation. "Neutral material or material damaging to defendant need not be disclosed," as Lord Bingham reminded us in the leading case.[65] So where (as usual) the telephone intercepts show the defendant to be doubly guilty, the prosecution would not have to share it with the defence if they did not propose to use it.

In cases where the material that the prosecution wish to keep hidden might help the defence, the rules on public interest immunity require them first to show it to the judge. The judge then decides whether the public interest requires it to remain confidential, and if so, whether the case can be fairly tried without disclosing it to the defence. If the judge rules that a fair trial without disclosing it is possible, it is not disclosed. If he rules otherwise, the prosecution has a choice: either it must disclose the material, or if it is not prepared to do this, it must drop the case. But in no way would the prosecution be forced to disclose truly sensitive information about telephone tapping if it thought this would be dangerous.

The "unused material" problem already arises, of course, in respect of the other forms of covertly obtained material that (unlike intercepts) are admissible in evidence–such as information from informers and secret agents, conversations overheard by other kinds of listening device, and indeed telephone intercepts, where phones were tapped abroad; and here the security issue is dealt with, more than adequately, the rules relating to public interest immunity. There is no reason to believe that, if the fruits of telephone tapping or other interceptions of communications were potentially admissible in evidence, the rules about public interest immunity would not provide an adequate safeguard here as well.

The subsidiary arguments in favour of the ban are equally unconvincing.

The argument about "harming the relationship between the police and the intelligence services" was answered by JUSTICE as follows:

> At its root… the government's concern appears to be that allowing intercept evidence may lead one government agency or public body to refuse to co-operate or share vital information with another. We find such an explanation surprising, to say the least. Whatever the complexities of the working relationship, the suggestion that intercept evidence could lead to an

[64]For a detailed account of the rules relating to public interest immunity, *see Archbold, Criminal Pleading, Evidence and Practice* (2009) §12.33 onwards. For a simpler account, *see* Ian Dennis, *The Law of Evidence*, (2nd ed, Sweet and Maxwell, 2002) chapter 9.

[65]*R v H* [2004] UKHL 3; [2004] 2 AC 134.

> increase in inter-agency tension seems to us a poor argument against allowing its use in court. Similarly, even if such tensions did arise, we do not think it credible that any government would ever permit them to compromise the fight against serious crime and terrorism.[66]

The government, in other words, is either in charge of its agents or it is not; and if it is not, it ought to be, and should not parade its inability to control them as the basis for a rule of evidence.

The argument that allowing intercept evidence would increase the burden on intelligence services, police, and prosecutors is based on the mistaken idea that, if such evidence were admissible, every telephone intercept would have to be transcribed in order to make it available to prosecution and defence. But as Lord Lloyd points out, this is based on ignorance of the rules about PII.

> In a case where there is intercept material, there is an existing duty on the prosecution to make sure that there is nothing which helps the defence… What happens in practice is that senior counsel go through the summaries. If there is nothing helpful to the defence nothing is disclosed and nothing transcribed. If prosecuting counsel are in doubt about anything in the summaries they will raise the matter with the judge on an application for PII. It is only then that anything need be transcribed. That is what happens now. Exactly the same would happen if intercepts were admissible, save that the passages in the intercept favourable to the prosecution would be transcribed in the ordinary way for putting before the jury. There would be no additional burden…[67]

And the argument that admitting intercept evidence would in some way "hamper the ability to adapt to rapid changes in communications technology" seems difficult to understand. Why would making intercept evidence admissible as evidence hinder new methods being developed that make it possible to intercept new means of communication? Removing the ban on intercept evidence would not involve imposing any kind of restrictive legal framework, either on the forms of communication that are intercepted or on the ways in which its interception is carried out.

The implausibility of these reasons for maintaining the ban is underlined by the fact that intercept evidence is admitted in evidence all over the rest of the world without causing the practical difficulties that supporters of the ban assure us would inevitably follow if it became admissible here. When confronted with this, supporters of the ban usually retort by saying that the countries that allow intercept evidence to be used in court have "the inquisitorial system." But as JUSTICE points out in its report, this just not true, because "… intercept evidence has long been admissible in criminal proceedings in Australia, Canada, South Africa and the United States."[68] In fact, the UK appears to be the only country in the world in which a ban on the use of such evidence exists.

And a further reason for treating these dire predictions about the ill effects of admitting intercept evidence with scepticism is that we already admit in evidence the fruits of other forms of under-cover surveillance, like information from informers and secret agents and information from other kinds listening devices, like hid-

---

[66] §65.

[67] In his written evidence to the Chilcot Committee, *see* footnote 94.

[68] JUSTICE, footnote 56, §80 onwards.

den microphones and long-range listening devices – and indeed intercept evidence itself, in those cases where it is admissible despite the ban; and this is done without causing any of the practical difficulties which supporters of the ban assure us would happen if the courts could receive intercept evidence. It is hard to avoid the conclusion hinted at earlier in this chapter: that behind these weak arguments there lurks a strong desire by the Home Secretary and his officials not to have the legality of their decisions to grant interception warrants examined in the courts.

The arguments for abolishing the ban and admitting intercept evidence, by contrast, all seem to be extremely strong.

In the first place, it is objectionable at a theoretical level. The basic rule of evidence is that if material is relevant, it is admissible – and to this rule, the ban on intercept evidence is a major exception. In criminal cases, few things are more relevant than what the defendant said: his words uttered when overheard planning the offence, or confessing to it afterwards – or with crimes like conspiracy and incitement, actually committing it. Where his damning words were tape-recorded, stronger evidence is rarely to be found. Normally, of course, they are admissible. Tape-recorded interviews with the police (or transcripts of them) are heard in evidence all the time. And less commonly, the courts also hear tapes of things like disgruntled spouses negotiating deals with supposed "hit men" who were policemen in disguise, conversations between drug-smugglers overheard by bugs planted in houses and cars, and tapes of incriminating conversations between murderers whispered in bugged cells. But where the defendant's words, however damning, were intercepted when spoken on the telephone they cannot be used in evidence. In principle, an exception to the basic rule of admissibility of such obvious importance should only be permitted where there is a very cogent reason for it, and there is not. And so the ban, as a Member of Parliament put it in a phrase that has been often quoted since, is "a carbuncle on the face of the law of evidence."[69]

Secondly, the ban is objectionable in practice, because – as with the suppression of any other form of highly relevant evidence – it increases the risk of miscarriages of justice by reason the courts reaching results that do not accord with factual truth.

No one – not even the strongest supporter of the ban – has any doubt that it makes it impossible to convict some people who whose guilt could be shown beyond all reasonable doubt if such evidence could be used against them. This is strongly suggested by information from other countries about the extent of its use, and how helpful prosecutors in those countries find it.[70] And it is also strongly suggested by evidence emanating from within the UK. In his evidence to the Chilcot Committee (of which more is said below), Lord Lloyd said:

> Most judges at the Old Bailey will have had experience of cases in which there are tape recordings of conversations which prove guilt beyond doubt. Yet they and the jury will have to listen to explanations given by the defendants which could easily be contradicted if the tape recordings had been admissible. This does not serve the cause of justice.

---

[69] Mr Andrew Mitchell, MP; Hansard, 7 February 2005, col. 1233.

[70] The JUSTICE report, footnote 56, contains a collection of material of this sort.

And in their eventual report in 2008 the Chilcot Committee (which was very cautious) said:

> As part of this Review, the Metropolitan Police have reviewed cases involving interception during 2006–07 in which charges were discontinued or failed to result in conviction. They concluded that intercept as evidence might raise the conviction rate in cases involving interception (excluding those still awaiting trial) from 88% to 92%.

Other evidence supports these views:

- ACPO[71] considered a number of cases, in two of which intercept could have been used as supporting evidence.
- The Serious Fraud Office (had the law allowed) would have used intercept evidence in a particular insider-dealing conspiracy case.
- The Northern Ireland Public Prosecution Service consider that removal of the bar could assist considerably in a small number of important cases, either helping to meet the test for prosecution or strengthening prosecution cases that already met the test.[72]

Although the miscarriages of justice that would be avoided by the abolition of the ban will usually be failures to convict the guilty, the fact that the ban applies equally to the defence does also raise the spectre of miscarriages of justice in the form of the conviction of the innocent.[73]

And even if, despite the ban, the right result is eventually achieved, it makes the legal process slower, more complicated, more expensive, and less efficient. To quote Lord Lloyd again:

> And even if there is just enough other evidence to bring them to trial, it is painful to watch the prosecution attempting to prove a conspiracy by adducing evidence of a pattern of telephone conversations between the conspirators when the best evidence is there on the tape recording. The criminal courts cannot do their job properly if vital evidence is excluded.[74]

Lord Lloyd also gave the Chilcot Committee a hypothetical example, inspired by the notorious Birmingham Six case.[75]

> … On the day of the Birmingham pub bombing five of the six defendants travelled back to Northern Ireland. They changed trains at Crewe, where some of them made telephone calls home. They were asked about these conversations at the trial, and they gave various explanations, which may or may not have convinced the jury. I have no idea whether the conver-

---

[71] The Association of Chief Police Officers.

[72] §§56 and 57.

[73] Although in practice, the likely outcome in this situation is that the contents of the intercept becomes known to prosecution counsel, who discontinues the proceedings. But where the evidence of innocence, though helpful to the defence, is not conclusive in the defendant's favour, the result may be the discontinuance of a case in which, if all the relevant evidence were put before the court, the defendant would have been convicted. *See* Matthew Ryder, "RIPA reviewed," *Archbold News*, Issue 4, 5 May 2008, 6.

[74] Written evidence to the Chilcot Committee (footnote 94).

[75] In which Lord Lloyd, when a judge in the Court of Appeal, delivered the judgement in which the convictions were finally quashed: *R v McIlkenney and others* (1991) 93 CrAppR 287.

> sations were taped or not. But if they were, and if the conversations were incriminating, it is at least possible that one or more of the defendants would have pleaded guilty. If on the other hand the conversations had an innocent explanation they would have helped the defendants. Either way it simply does not make sense that the jury should have been deprived of what may have been the best evidence in the case.

13.1.6 Terrorism, and Pressure to Remove the Ban

In recent years, there has been growing pressure within the UK for the ban on the admissibility of intercept evidence to be reversed. As is explained below, a reason for this has been concern about terrorism, and the legal measures introduced by the government to counter it.

A person who has taken a leading part in this movement is Lord Lloyd of Berwick, a former senior judge and, since his retirement, an active member of the House of Lords *qua* Upper Chamber of the legislature. For a period of 6 years, he was the Commissioner responsible for overseeing the interception of communications – the institution mentioned earlier in this chapter. For 7 years, he was the Chairman of the Security Commission, a permanent official body existing within the Cabinet Office and responsible for investigating lapses of security in the public service. And in the 1990s, he was charged by the government with conducting a major review of the law relating to terrorism, the Report of which was published in 1996.[76] His experience in these various capacities therefore enables him to speak on both terrorism and the interception of communications with great authority. The recommendations in his 1996 Report formed the basis for a reform and codification of the law in the Terrorism Act 2000. Since then, he has been an outspoken critic of the wave of further anti-terror laws that the government has promoted in reaction to the events of 11 September 2001 – legislation that he has described as having "grave implications for the constitution."[77]

In his Report in 1996, Lord Lloyd concluded that the ban on using intercept evidence significantly increased the difficulty in prosecuting terrorists, and recommended that it be relaxed in that category of case.[78] And since then, he has repeatedly argued that the ban should be abolished altogether. In 2006, he even introduced a Private Member's Bill in the House of Lords designed to reverse it. In the face of opposition from the government, this did not, of course, succeed. But this and his other efforts have undoubtedly helped to bring about the governmental change of mind that is mentioned in the concluding paragraphs of this chapter.

A central part of the government's legislative response to the threat of terrorism since the events of 11 September 2001 has been a push to create extra-judicial methods by which terrorist suspects can be locked up indefinitely without the need to have them prosecuted, convicted, and sentenced by the criminal courts. The first

---

[76] *Inquiry into Legislation against Terrorism* (October 1996: Cm 3420).

[77] In a speech at a conference organised by the city law firm, Clifford Chance, in June 2006: *see The Independent,* 6 June 2006.

[78] Ibid, footnote 76, §7.25.

of these, contained in Part IV of the Anti-terrorism, Crime and Security Act 2001, was a measure that enabled the Home Secretary to order the indefinite detention without trial of foreign terrorist suspects whom he would have deported if he could, but was unable to deport because of the risk that if they were returned to their countries of origin they would be tortured or put to death.[79] A group of foreign suspects detained by order of the Home Secretary in Belmarsh prison under these provisions challenged them in the courts, and in a spectacular judgment in December 2004, the House of Lords – sitting, unusually, as a panel of ten instead of the usual five – declared, by a majority of nine to one, that this legislation was incompatible with Article 5 of the European Convention on Human Rights.[80] In a sentence which has become famous, and which is said to have particularly nettled the Prime Minister, Mr Blair, one of the judges, Lord Hoffman, said:

> The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from such laws as these.[81]

The effect of this "declaration of incompatibility" was not to render the legislation invalid, and so the detainees remained in prison. But it did motivate the government to get Parliament to repeal the relevant provisions of the 2001 Act that provided for the indefinite administrative detention of foreign terrorist suspects, and to pass legislation replacing them with something else.

The "something else" was, in effect, house arrest by order of the Home Secretary. And because one of the reasons why the House of Lords had condemned the earlier legislation as contrary to the European Convention on Human rights was that it discriminated unfairly between foreign terrorist suspects and national ones, the new measure was (and still is) applicable to foreigners and citizens alike. Under the Prevention of Terrorism Act 2005, terrorist suspects can now be subjected to what are called "control orders." These are administrative measures, of indefinite duration, imposing restrictions on the way that those subject to them are allowed to live their lives. In their most severe form, these orders can, in effect, put the person subjected to them under house arrest. In their less severe form, they are ordered by the Home Secretary, but – a concession extracted by Parliament before it would pass the legislation – in their most severe forms, which are called "derogating control orders," they are imposed, on the request of the Home Secretary, by a judge. Control orders, like the administrative detention that they replaced, have also attracted serious criticism. But in a series of three cases decided at the end of 2007, the House of Lords gave them what might be described as a "qualified clean bill of health."[82]

---

[79] As a result of the decisions of the Strasbourg Court in *Chalal v UK* (1996) 23 EHRR 413, reaffirmed in *Saadi v Italy,* Grand Chamber, 28 February 2008 (Application No. 3720/06).

[80] *A v Secretary of State for the Home Department* [2004] UKHL 56, [2005] 2 AC 68, [2005] 2 WLR 87.

[81] Ibid at §97.

[82] *Secretary of State for the Home Department v MB* [2007] UKHL 46; [2007] 3 WLR 681; *Secretary of State for the Home Department v E* [2007] UKHL 47, [2007] 3 WLR 720; *Secretary of State for the Home Department v J* [2007] UKHL 45, [2007] 3 WLR 642. For detailed analysis, *see* Forster, this volume.

In parallel with these measures to enable terrorist suspects to be locked up indefinitely without the need for criminal proceedings, the government has also sought to alter against terrorist suspects the rules about the powers of the police to gather evidence with a view to prosecution: in particular, the power to detain suspects without charge, in the hope of extracting from them by questioning, or by other means, enough evidence to charge[83] them. Under the Terrorism Act 2000, the maximum period for which terrorist suspects could be detained for questioning was fixed at seven days (as against 96 hours–4 days – in cases of ordinary crime). Under a provision buried in the depths of the Criminal Justice Act 2003, this period was quietly doubled to 14.[84] Then in 2005, the government, led by Mr Blair, decided that it would try to have this period increased to 90 days. This change was too authoritarian for the House of Commons to accept, even in the face of a strident campaign of support provided by the normally all-powerful best-selling tabloid newspaper *The Sun*, which went so far as to publish a "list of shame" giving the names of those "traitors" in the House of Commons who were thought to be opposed to the measure, and inciting its readers to write and tell them what they thought of them (!). In November 2005, a group of members of Mr Blair's party the House of Commons rebelled and voted with the opposition, so defeating the proposal; and the legislation[85] that was eventually enacted "merely" doubled the existing period once again, which then went up from 14 to 28 days. But Mr Blair's successor, Gordon Brown, was determined to show that he could succeed where his predecessor failed, and in May 2008, by twisting every available arm, he managed to persuade the House of Commons to pass a Counter Terrorism Bill which contained a clause designed to increase the period from 28 days to 42. In the autumn of 2008 the clause was, predictably, deleted by the House of Lords. At this point the Government gave up the fight, and for the moment the period remains 28 days.

As a justification for these authoritarian measures, the government has repeatedly invoked "difficulties with the law of evidence." Administrative detention, or house arrest by order of the Home Secretary (alias control orders) are necessary, it has repeatedly said, in order to neutralise persons whom the Home Secretary "knows" to be terrorists - but his knowledge is based on evidence which, regrettably, the law does not permit to be used in criminal proceedings. So, sadly, these persons cannot be prosecuted for offences of terrorism, and the only way to keep the public safe from them is for them to be detained by order of the executive. And a similar argument is used for seeking to extend the period during which the police can detain terrorist suspects without charge for questioning. The police "know" that they are guilty, but the evidence they have is not admissible in criminal proceedings, so it is necessary to allow the police to detain them for 14, or 28, or 42, or 90 days, in the hope that in the end they will have gathered evidence that is.

[83] In English criminal procedure, the "charge" is the formal step, in a serious case, that turns a suspect into a defendant.

[84] s.306. (This Act is an easy document in which to bury things, because contains 339 sections and 38 Schedules!)

[85] Terrorism Act 2006.

And, of course, the evidence the Home Secretary has, or the police have, but regrettably cannot use, is typically incriminating conversations, tapes of which the police or the security services have obtained by tapping telephones. As a Home Office Minister, Lord Rooker, told the House of Lords when it was debating the Bill that eventually led to the legislation providing for the administrative detention of foreign terrorist suspects:[86]

> If we could prosecute on the basis of the available evidence in open court, we would do so. There are circumstances in which we simply cannot do that because we do not use intercept evidence in our courts.[87]

(It goes without saying that although intercept evidence may not be used at criminal trials, it may justify the police in detaining suspects for questioning; and sections 17 and 18 of RIPA 2000, which contain the general ban on using intercept evidence in legal proceedings, make an exception for the Special Immigration Appeal Tribunal, which handles (inter alia) legal issues arising from the expulsion of terrorist suspects, and proceedings in relation to control orders.[88])

Naturally, those who are opposed to administrative detention, control orders, and infinite extensions of the power of the police to hold terrorist suspects for questioning have responded to this argument by saying "The ban on using intercept evidence in criminal proceedings only exists because, in 2000, you – the government – chose to preserve it. It is there only because of section 17 of the RIPA, which you promoted. If it were abolished, these terrorist suspects could be prosecuted in the criminal courts, and these authoritarian measures would not be necessary." This argument was put forward, with great force, by JUSTICE in a report in 2006.[89]

And it convinced the Parliamentary Joint Committee on Human Rights which in a Report in 2007 said:

> The difficulty of obtaining sufficient admissible evidence to prosecute terrorist offences has frequently been relied on in the past by the government to justify exceptional counter-terrorism measures, including detention of foreign nationals without trial under Part IV ATCSA 2001, control orders and, most recently, pre-charge detention of up to 28 days. In each case, the government has repeated its preference for criminal prosecution, but has cited evidential difficulties as one of the main justifications for its exceptional measures. The government's failure, so far, to bring forward proposals for relaxing the ban on the admissibility of intercept therefore has important human rights implications, because it contributes to the need for exceptional measures which themselves risk being incompatible with the UK's human rights obligations. Permitting the use of intercept as evidence may be necessary in order to guarantee a fair trial for those accused of involvement in terrorism who are currently subjected to other forms of control which are not accompanied by the criminal "due process" guarantees with go with a fair criminal trial.[90]

---

[86] Part IV of the Anti-terrorism, Crime and Disorder Act 2001 – condemned by the House of Lords in the case mentioned at footnote 80.

[87] Hansard, HL, vol 629, col 146, 27 November 2001; quoted by JUSTICE, footnote 56, §29.

[88] Subsection 18 (da), added by the Prevention of Terrorism Act 2005.

[89] Footnote 56.

[90] Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning* (HL Paper 157/HC 394, 16 July 2007), §116.

This Committee had heard evidence from, among others, the Director of Public Prosecutions (DPP), the former Attorney General (Lord Goldsmith), and the Commissioner of the Metropolitan Police, all of whom had recently "gone public" in favour of abolishing the ban. And in the light of this, the Committee also said:

> We are satisfied that the evidence of the DPP and the former Attorney General puts the matter beyond doubt: that the ability to use intercept as evidence would be of enormous benefit in bringing prosecutions against terrorists in circumstances where prosecutions cannot currently be brought, and that the current prohibition is the single biggest obstacle to bringing more prosecutions for terrorism…. The difficult question is not whether the current ban on the evidential use of intercept evidence should be relaxed, but how to overcome the practical obstacles to such a relaxation.[91]

In the past, the government's routine response to pressure of this sort had been to get the Home Secretary to commission an "internal review" – in other words, a review conducted within the Home Office. Of these, there had been no less than six,[92] each of which had, unsurprisingly, reported that nothing could be done. But by this stage, the pressure was too strong for the issue to be swept under the carpet in this way, and in July 2007, the government commissioned a review by a small group of Privy Counsellors, chaired by a distinguished senior civil servant, now retired, Sir John Chilcot.[93] And in January 2008, the Chilcot Committee, unlike all the previous internal reviews, reported in favour of lifting the ban.[94]

In relation to terrorist suspects, the Chilcot Committee was very cautious. In paragraph 59 of its Report, it stated:

> No one has asserted that the evidential use of intercept would bring about a major increase in successful prosecutions. The limited evidence available suggests that there would be a modest increase in successful prosecutions, at different levels of seriousness, as a result of intercept evidence. We have not seen any evidence that the introduction of intercept as evidence would enable prosecutions in cases currently dealt with through control orders.

This was a "downbeat" assessment of the situation compared with the view Lord Lloyd had expressed in his 1996 Report, where he had said:

> It is always difficult to look backwards and point to specific cases in which interception material would have enabled a person to be charged or a conviction obtained. But I have been shown a list of some twenty cases, including four recent cases in which intercept material would have been of assistance to the prosecution; and I was told of at least one terrorist investigation in which the interception evidence would have provided "the missing pieces in the jigsaw" and thus enabled a prosecution to be brought.[95]

---

[91] §126.

[92] Chilcot Report, footnote 94, §11, in which it announces that this report is "the seventh report to Ministers on the issue of intercept as evidence in the last thirteen years, but it is the first to have been produced by people who are not currently within government."

[93] The other members were Lord Archer of Sandwell (a barrister, and Labour politician), Alan Beith (a Liberal Democrat MP), and Lord Hurd of Westwell (who as Douglas Hurd MP had been both Home Secretary and Foreign Minister in Conservative governments in the 1980s and 1990s).

[94] *Privy Council Review of Intercept as Evidence; Report to the Prime Minister and the Home Secretary*, 30 January 2008. Cm 7324.

[95] *Inquiry*, footnote 76, §7.11.

And the Chilcot Committee's cautious tone was reflected by the Prime Minister, Gordon Brown, when he announced his conversion to the idea of abolishing the ban some weeks later. In a statement to Parliament, he stressed that changing the law to make intercept evidence admissible would not remove the need for control orders, or the need (as seen by the government) to extend to 42 days, the period during which suspected terrorists could be detained by the police for questioning.[96] And so, to the disappointment of those who (like the author of this paper) are opposed to creation of the "shadow system of criminal justice" mentioned at the beginning of this chapter, it looks as if the "collateral damage" that the ban has caused in the UK will survive the abolition of the ban itself.

Eighteen months later, when this chapter goes to press, we are still waiting for the government to introduce legislation to bring this change about. At first sight, this delay appears surprising because the legislation that is needed to produce it is extremely simple: a short Bill to repeal sections 17 and 18 of RIPA 2000, the effect of which would be to put intercept evidence within the same legal framework as any other piece of evidence obtained by methods of covert surveillance.

It seems, however, that the government, though prepared in principle to lift the ban, is not prepared to admit that 23 years of stubborn resistance to the use of intercept evidence in court was a fuss about nothing, and is determined to see the problem as being more complicated than it really is. When announcing his conversion to the use of intercept evidence in court, Mr Brown told Parliament that there were "very big hurdles" to be overcome, and stressed that there would have to be "further extensive work to ensure that sensitive surveillance techniques were protected under any new regime." In taking this line, the Prime Minister had once again the encouragement of the Chilcot Committee, which stressed the need for a legal regime that met a list of no less than nine requirements. So it seems likely, alas, that the legislation, when it eventually comes, will replace a complicated and indigestible scheme for the exclusion of intercept evidence with an equally complicated and indigestible scheme for its admission.

At the root of the problem, I believe, is the fact that the law and practice on the interception of communications in the UK has grown up without drawing the obvious distinction between information-gathering for general purposes of national security and information-gathering for the purpose of collecting evidence for a prosecution. In France, for example, this line is clearly drawn. National security intercepts are made on the authority of a Minister, and are not admissible in evidence at trial, and intercepts for the purpose of evidence-gathering are made on the authority a judge. In retrospect, it is a pity that, 50 years ago, the Birkett Committee did not point us in that direction.

[96] *BBC News*, 6 February 2008.

References

Archbold, J.F. (2008). *Criminal Pleading, Evidence and Practice in Criminal Cases*. London: Sweet and Maxwell.

Baldwin, J. (1985). The police and tape recorders. *Criminal Law Review, Issue 11 (November)*, 695–704.

BBC News, 6 February 2008.

Blick, A., Choudhury, T. and Weir, S. (2006). *The rules of the game – terrorism, community and human rights: A report by Democratic Audit for the Joseph Rowntree Trust.* http://www.democraticaudit.com/download/breaking-news/Terrorism-Final.pdf

Committee of Privy Councillors (1957). *Report Appointed to Inquire into the Interception of Communications (Cmnd. 283)*. London: The Stationery Office.

Cross, R. (1967). *Evidence* (3rd edition). London: Butterworths.

Dennis, I. (2002). *The Law of Evidence* (2nd edition). London: Sweet & Maxwell.

Ewing, K.D. and Gearty, C.A. (1990). *Freedom Under Thatcher: Civil Liberties in Modern Britain*. Oxford: Clarendon Press.

Hardcastle, M.S. (1881). *Life of John, Lord Campbell (Volume 2)*. London: John Murray.

House of Lords (2007). *Counter-Terrorism Policy and Human Rights: 28 Days, Intercept and Post-Charge Questioning (HL Paper 157/HC 394)*. http://www.publications.parliament.uk/pa/jt200607/jtselect/jtrights/157/157.pdf

JUSTICE (2006). *Intercept Evidence: Lifting the Ban*. http://www.justice.org.uk/images/pdfs/JUSTICE%20Intercept%20Evidence%20report.pdf

Lord Lloyd of Berwick (1996). *Inquiry into Legislation against Terrorism Volume one (Cm 3420)*. London: The Stationery Office.

Munday, R. (2000). The inadmissibility of evidence relating to intercepted communication. *Cambridge Law Journal, Volume 59*, 267–270.

Ormerod, D. and McKay, S. (2004). Telephone intercepts and their admissibility. *Criminal Law Review, Issue 1 (January)*, 15–38.

Ormerod, D. (2005). Commentary. *Criminal Law Review*, *Issue 3 (March)*, 222–224.

Parker, C.S. (1907). *Life and Letters of Sir James Graham 1792–1861*. London: John Murray.

Royal Commission on Criminal Procedure. (1981). *Report of the Royal Commission on Criminal Procedure (Cmnd 8092)*. London: The Stationery Office.

Ryder, M. (2008, 5 May). RIPA reviewed. *Archbold News*, *Issue 4*.

Secret Committee of the House of Lords. (1844). R*eport Relative to the Post Office*.

Secretary of State for the Home Department (1985). *The Interception of Communications in the United Kingdom: A Consultation Paper (Cmnd. 9438)*. http://www.homeoffice.gov.uk/documents/cons-1999-interception-comms?view=Binary.

Secretary of State for the Home Department (2008). *Privy Council Review of Intercept as Evidence: Report to the Prime Minister and the Home Secretary* (Cm 7324). http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf.

Tapper, C. (2007). *Cross and Tapper on Evidence* (11th edition). Oxford et al.: Oxford University Press.

Williams, V. (2005). The *Surveillance and Intelligence Law Handbook*. Oxford: Oxford University Press.

Chapter 14
Fighting Terrorism – the Unprincipled Approach: the UK, the War on Terror and Criminal Law

Marianne Wade

Few would deny that murder, bodily harm, and the destruction of property are properly the subject of criminal law. Offences bringing such behaviour within the ambit of criminal law are core features of every criminal code across Europe. It would appear rational then that such offences when perpetrated or planned on a large scale – usually central to any definition of what terrorist offences aim to punish for[1] – should be subject to the strong arm of the law on an equally massive scale. Within the continental European context, it is impossible to imagine anyone denying the appropriateness of dealing with terrorism via the criminal law. Although there is rightfully discussion surrounding the definition of terrorism[2] and (where related offences are formulated too widely) controversy whether all forms of behaviour covered by terrorist-related offences are appropriately included (being that they are thus included in this emotive area of the law which aims to punish the most heinous of crimes), prima facia it seems absurd for anyone to seriously deny that acts of terrorism must primarily concern justice systems as a subject of criminal law. Indeed, in the vast majority of cases, one might question the need for any additional "special" criminalising law for terrorism; only rarely does some form of behaviour associated with it not fall within the traditional ambit of criminal law.[3]

M. Wade (✉)
Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: m.wade@mpicc.de

[1] Although the UN definition (in Security Council Resolution 1566) relates to death and serious injury only, Part 1(2)b of the UK TA 2000 refers also to destruction of property – *see*, e.g., Golder and Williams (2004).

[2] For discussion, *see* Rabbat, this volume.

[3] And indeed some commentators assert that it may even be easier to prosecute for the underlying crimes rather than seeking the label terrorist, *see* Beckman (2007) p. 11.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_14, © Springer Science+Business Media, LLC 2010

It may come as something of a shock therefore, to understand that anti-terrorist law has in recent years occupied the courts in England and Wales outside the criminal law – though it is usually discussed as part of the broader criminal justice realm[4] – and that a suggestion to integrate it into the criminal law[5] left the Government "still to be persuaded."[6] Although much has been done to counter the "extra-legal" nature of this area in recent years and it has in many ways been brought into line with the criminal law, it continues to range beyond it as an apparent separate entity.[7]

The broad danger originating from terrorist offences naturally mean that Governments see a deep responsibility to act preventively; actions which are not easily covered by the criminal law which is by nature a post-facto mechanism relating to a past event and able only to prevent future offences committed by persons identified by such an act as dangerous. In the context of the current terrorist threat, related as it is to singular acts of great destruction by persons who will be at pain to ensure they are not identified at all by the criminal justice systems prior to the event it is perhaps not surprising that the criminal law is being stretched and one might expect it to be so particularly in the areas of attempts, conspiracy, and other controversial substantive provisions. Nevertheless, once a planned terrorist crime has been discovered – though it will often be necessary to take more emergency like, short-term preventive steps (in many Continental European systems invoking police and not criminal law to do so. This is particularly true given that modern conspiracy laws can be invoked to ensure a criminal conviction.[8] One would expect the authorities to bring suspected (potential) perpetrators to justice via the criminal justice system.

It is impossible not to view a failure to draw upon the criminal justice mechanism in dealing with such a phenomenon as a fundamental challenge to criminal law: Taking Duff's definition, for example, which regards criminalisation as justified where there is wrong-doing, which merits public calling to account (due to harm/serious unfairness to fellow citizens) and necessitates condemnation and

[4] *See*, e.g., Wilkinson (2006), p. 64 and 205; Warbrick, for example, analyses these developments as part of the criminal law, *see* Warbrick (2004) p. 392.

[5] Lord Lloyd of Berwick (1996).

[6] Home Office and Northern Ireland Office (1998), paragraph 7.16. This proposal was made at a time in which there was perhaps a chance of the emergency law approach – deemed necessary to deal with the Northern Ireland conflict – could have been replaced by a non-emergency scheme; centrally the TA 2000 brought extended police detention following arrest under judicial control (schedule 8, part 3) turning the emergency measure requiring derogation from the Convention [*see* Brannigan and McBride v. United Kingdom, ECtHR, Series A, No. 258-B (19993)] into a "normal" measure – a possibility whose chances of fruition ended on 11 September 2001 – *see* Warbrick (2004), p. 363, 364, and 392. *See also* Warbrick's discussion of the areas providing inspiration for another; if a measure has worked in the anti-terrorist context, it will be adopted elsewhere, p. 390.

[7] Gearty (2007), p. 43 and 47.

[8] Themselves the subject of great controversy in some Continental systems.

punishment, there can be no doubt that the behaviour called to mind by the notion of terrorism (even if this is legally difficult to pin down) falls into this category.[9] US advocates of the War on Terror[10] would deny the efficacy of this category, seeing it as too mild a tool in what they regard as a war, but within Europe and the UK, emphasis has been placed (if the discussion has been entertained at all) on terrorists deserving treatment as criminals, not as soldiers or anything else.[11]

Invoking the criminal law leads to the requirement that criminal procedure is adhered to when imposing its consequences. Across Europe, certain fundamental principles are associated with criminal procedure and these are frequently explored in relation to terrorism, also by contributions to this book. Little effort is required, however, when reviewing the literature to conclude that the challenges currently faced in relation to British criminal procedure are particularly prominent. It is these which are explored in this chapter. The themes of this debate are, however, to a greater or lesser extent relevant for countries throughout Europe, in which governments are considering changing their law to provide for a more effective fight against terrorism.

Nevertheless we have become used to regular reports from England and Wales that suspects of terror-related charges are being treated differently there (see Forster). Some ramifications are explored in the following.

14.1 The Aim of Criminal Proceedings in England and Wales

Whilst England and Wales does not have a code of criminal procedure, recent legislative efforts have resulted in a number of main features of criminal procedure being gathered and codified in the Criminal Procedure Rules.[12] The first section of these refers to their aim or what is known as "the overriding objective." This section 1.1 states that this is to deal with criminal cases "justly… acquitting the innocent and convicting the guilty" dealing "fairly" with the prosecution and the defence and "recognising the rights of a defendant, particularly those under Article 6 of the European Convention on Human Rights." However, this is to be done: "efficiently and expeditiously" taking into account "(1) the gravity of the offence alleged, (2) the complexity of what is in issue, (3) the severity of the consequences for the defendant and others affected, and (4) the needs of other cases."[13] Even after consideration of these final criteria, some of which indicate a more pragmatic approach to certain cases, there is no reason to expect that terrorism-related offences should

[9] *See* Duff.

[10] *See*, e.g., Foreign Policy (2005) and Wolfowitz (2002).

[11] *See*, e.g., Blair (2005); Gregory (2007a) p. 203, and Macdonald (2008).

[12] 2005.

[13] Rule 1.1.g Criminal Procedure Rules 2005 – *see* Ministry of Justice (2008).

be dealt with in any other way than by criminal procedure aiming to convict only the guilty in accordance to the principles of such proceedings. Indeed, the gravity and severity of consequences criteria would appear to favour the prosecution of such crimes, even though this might bind considerable criminal justice system resources.

In emphasising that the needs of justice require the innocent to be acquitted the criminal procedure rules reiterate a long-stated fundamental of criminal procedure in Britain. This was perhaps most famously stated by Justice Holroyd in the case of *Hobson*[14] in which he identified a "maxim of English law that ten guilty men should escape rather than one innocent man should suffer."

It will come as little surprise that changes made to the law in the last decade to provide for the criminalisation of certain behaviour when this is associated with terrorism, as well as immediate means with which to deal with persons suspected of such offences, have caused animated debate as to their compatibility with or weakening of certain fundamental principles of criminal procedure. The aim of this chapter is not, however, to describe the detail of such challenges, for this has been done more effectively and urgently by others.[15] In the course of fierce debate, this has indeed involved the Judiciary accusing the Executive of being a greater danger to democracy than terrorists themselves.[16]

> The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws such as these. That is the true measure of what terrorism may achieve.[17]

The aim here is far more to provide an overview of the overall context of challenge to the fundamentals of criminal procedure in Britain where the fight against terrorism constitutes the spearhead of a far-reaching calling into question of the very structure of the law as we know it.

14.2 Challenging the Fundamentals of Criminal Law

When following the debate surrounding terrorism in the UK and the changes made to the criminal law and the law of criminal procedure because of it, the unavoidable conclusion is that the English and Welsh criminal justice regime is facing unprecedented challenges as the Executive seeks to accommodate new interests in the law as part of its anti-terrorist arsenal. The fierce debate as to anti-terrorist law has raged so strongly because changes made by recent legislation have been fundamental

[14] 1 lew CC 261.

[15] *See*, e.g., Lord Hoffmann in A (FC) and others (FC) (Appellants) *v.* Secretary of State for the Home Department (Respondent) [2004] UKHL 56 and Feldman (2006).

[16] Lord Hoffmann in A (FC) and others (FC) (Appellants) *v.* Secretary of State for the Home Department (Respondent) [2004] UKHL 56.

[17] At paragraph 97.

enough to challenge the very essence of criminal law. When suggestions abound from a series of Home Secretaries, for example, that the burden of proof must be lowered in cases dealing with suspected terrorists (Gibb, Tendler and Ford 2004), one cannot but conclude that the very core of criminal law is being called into question. Whilst Lord Woolf is certainly correct in his assessment that these changes will affect very few people (BBC, 2008), these changes are doubtlessly fundamental no less. If the history of exceptional powers in UK jurisdictions has taught us anything then certainly that those measures which enter discussion intended as absolute exceptions for an emergency have a tendency to become normalised, to stay on the statute books and eventually to be broadened in their application.[18]

This analysis will focus only on those measures that have become law or may yet do so, meaning that more radical suggestions made by Government ministers are not considered.

The criminal law and indeed the wider criminal justice system face a number of challenges: Most prominently, the courts have been at the forefront of efforts to ensure the law remains within acceptable bounds. Since the decision of the House of Lords in *A and others v Secretary of State for the Home Dept*[19] in 2004 the courts have abandoned a more conservative stance and become quite pro-active in their actions to ensure that certain boundaries remain in place, also within the criminal law. Thus, court decisions have been decisive in limiting the scope of attempted reforms of the law by anti-terrorist legislation with a number of cases leading to great tension between the Executive and the Judiciary.[20] The latter have then been cast in the press as hampering effective anti-terrorist work.

14.2.1 Substantive Criminal Law and Criminal Procedure

Perhaps most importantly for the integrity of the criminal law, the Judiciary has been willing to step in to change the *wording of substantive offences* to ensure compatibility with the European Convention on Human Rights, thereby safeguarding not only the standards of substantive criminal law but also of procedural differences. In a reference by the Attorney-General [the UK Government's chief legal

[18] *See* the PTA NI temporary measures anchored into permanent law by the TA 2000, for reflection further afield, *see* Luban (248–249); where taken to far, such an approach can be seen to undermine the legitimacy of a state, *see* Chadwick (1997), p. 341. How quickly such powers are then used in different contexts can be seen in the case of R (Gillan) v. Metropolitan Police Commissioner [2004] E.W.C.A. Civ 1067, summarised by Gearty (2005), p. 30.The scope for misuse has also already been displayed – *see* Green (2008). Zedner (2005), p. 530 argues that it s vital this not be allowed to happen.

[19] in departure from a previously pre – HRA – more deferent stance – Fenwick p. 1336, which saw courts accepting that it is fundamentally for the Government to decide whether national security is threatened – *see Shafir v Rehman* CA – 24 May 2000 and *CCSU v Minister for the Civil Service* [1985] AC 374.

[20] Morris (2007); Steele (2003).

officer, A.G.'s Reference (No 4 of 2002)[21]], the House of Lords used powers lent to the courts by section 3 of the 1998 Human Rights Act to bring the offence of belonging to a proscribed organisation[22] and, with it, all offences which reverse the burden of proof or require a defendant to provide proof refuting a significant element of an offence,[23] into line with standards required by the Convention.[24] Whilst this still means that a fundamental shift is taking place in relation to the national standards placed on the criminal law: the reversal of the burden of proof is a highly contentious point, it does mean that certain boundaries of the criminal law are being defended. The courts have taken charge of ensuring the innocent are not brought within the scope of a substantive criminal offence, thereby countering an imprecise and thus unprincipled attitude to drafting the law. The Government has drawn up legislation that breaches traditional principles of the criminal law but finds itself facing courts imposing a proportionality requirement on that legislation and thus making efforts to ensure even anti-terrorist policy does not become entirely devoid of principle. In doing so, the Judiciary are contradicting Parliament's claim to have paid heed to that very principle,[25] laying down a clear definition of what proportionality means and ensuring that the Government's unprincipled approach faces certain fast boundaries of principle.

The fierce debate currently underway in relation to making *evidence stemming from telephone taps* admissible[26] is a further example of Government anti-terrorist policy paying little heed to the traditional boundaries and principles of criminal law. In fact, the mere fact of admissibility is far less objectionable than the current situation caused by its inadmissibility as we shall see later, but the form in which it is currently proposed is quite another matter. It reflects an attempt by the Government to achieve the admissibility of certain evidence despite the retention of a high level of secrecy above all in relation to the identity and broader investigative practices of the law enforcement or secret service personnel who performed the investigation. This would involve the court accepting classified evidence which it cannot test in accordance with usual standards. This cannot but be seen as an attack on a bastion of criminal procedure. The courts' right and indeed duty to scrutinise evidence is traditionally stringent, and for this reason, classified information tends to be kept out of British courts because the Government is loathe to share its secrets with the courts, let alone the public (*see* Spencer, this volume).[27] The traditional stance is being maintained as far as secrecy is concerned but an exception sought to the usual evidentiary requirements. It is difficult to imagine a further reaching attack on this

[21] [2004] UKHL 43; [2005] 1 AC 264.

[22] s. 3 of the 2000 TA.

[23] *See* the Court of Appeal decision in R v Keogh [2007] All ER (D) 105 (Mar); [2007] EWCA Crim 528, 7 March 2007.

[24] Fenwick 1337.

[25] In accordance with article 19(1)(a) HRA, Fenwick 1337.

[26] Also documented in this volume, *see* Spencer.

[27] Fenwick 1466–1467 (1047–1052).

fundamental principle of criminal procedure. The Government seemingly determined to remain loyal to its principle of unprincipled policy. Surely no one can deny that this increases the risk of the innocent not being acquitted because evidentiary value cannot be properly assessed; only time will tell whether and in what form this kind of development will become a feature of British criminal justice.

A few procedures introduced by anti-terrorist legislation feature the use of classified evidence in non-criminal proceedings. Those relating to determining whether the proscription of an organisation[28] was correct and proceedings before the Special Immigrations Appeals Committee[29] can involve the introduction of classified evidence by the Government which the court views in order to make its judgement. In these proceedings, where such evidence introduced a Special Advocate, who works in the interest of the appellant but is not briefed by him/her/it, views the evidence and makes arguments related to on his/her/its behalf, though naturally never communicates with him/her/it.[30] Since membership of a proscribed organisation is in turn a criminal offence, one may remark that the nature of such proceedings is not decisive in judging them. They will quickly draw on criminal law. Nevertheless as a matter of principle, there is a significant increase in seriousness related to the Government's latest suggestion. Where the punitive aims of criminal proceedings aimed at an individual are involved, blunting the courts, ability to scrutinise evidence is even more serious a matter. It is furthermore noteworthy that whilst in civil proscription proceedings, the court and special advocates were given certain restricted access; in the proposed criminal proceedings, not even the court is to be placed in the privileged position facilitating the ability to judge the reliability of the evidence presented. The criminal law, usually associated with more stringent principles, faces a demand to allow a total exception.[31]

14.2.2 Detention

Perhaps the best known example of challenges to the principles of the British criminal justice system is that related to the *detention of suspects*. Whilst the law is marked by the requirement that police charge suspects very swiftly (thus making them aware of what they are accused of and opening up their possibility to defend themselves against this accusation) if they wish to retain them in detention beyond

[28] In accordance with part 2 of the TA.

[29] *See also* Smith, this volume.

[30] *See also* the court discussion of the role played by Special Advocates and means by which their efficacy can be improved above all by ensuring some kind of exchange between them and the defendant they represent – e.g., Secretary of State for the Home Department v. MB [2007] UKHL 46, paras. 35, 51–54, 62–68, 81–85.

[31] *See* Spencer, this volume.

a few hours,[32] it has also featured a long-standing exception for those suspected of terrorist-related offences.

Under the earlier prevention of terrorism acts, the police were permitted to hold suspects in terror related cases for 7 days without charge[33] and without the suspect gaining a right to inform anyone. These powers were used in particular to hold suspects after bomb attacks had taken place but quite naturally led to discussions concerning police practices during such times.[34]

The recent spate of anti-terrorist law which saw the detention without trial scheme for foreign, non-deportable suspects in force between 2001 and 2005 (regulated by section 23 of the Anti-Terrorism, Crime and Security Act 2001) as well as the debate surrounding 90 days detention without charge for terror suspects[35] have provided for fundamental challenges to the law as well as naturally raising questions about police practice in this area. The newer provisions did mitigate fears to a certain extent by incorporating regular court controls into such schemes, but the concern caused as to where principled criminal procedure was left as a result could not be placated.

Under normal circumstances, section 61 of the Police and Criminal Evidence Act 1984 (PACE) in combination with Code C thereof restricts police detention of a person not yet charged to a maximum of 36 h (this was extended from 24 in 2003 by the Criminal Justice Act section 7). Police must then apply to a magistrate for extensions up to a maximum of 96 h if the latter deems detention necessary within a diligent and expeditious investigation.

Special provision is made for suspects detained in relation to terrorism under schedule 8 of the 2000 TA (amended by section 23 of 2006 TA and Code H of PACE). Detention without charge is possible for up to 28 days with the continued detention subject to regular approval by a magistrate. Until very recently debate focused on Government plans to raise this limit to 42 days though this proposal faced resounding defeat in the House of Lords and has thus been retracted held in reserve should an exceptionally dangerous situation arise.[36] A boundary has thus been drawn upon the Government's plans to extend an exception to a fundamental principle of the criminal law (protected by the powerful and deeply traditional writ of habeas corpus). Nevertheless a breach of principle remains. Although restricted, departure from traditional (in this case pre-1974) standards protecting the principle of liberty of person has been allowed. Previously the law demanded evidence against a person strong enough to provide the basis of a criminal charge before any longer term deprivation of liberty could be imposed. Since 1974, this fundamental

[32] *See* infra.

[33] 48 h and then a further 5 days upon extension by the Secretary of State - section 7 (2) of the Prevention of Terrorism (Temporary Measures) Act (PTA) 1974.

[34] The first detainee was Paul Hill, "pressured" into "confessing" his participation in a pub bombing in Guilford. The Guildford four case remains an extreme example of a miscarriage of justice in the British system – *see* Davenport and Baauw (1995) p. 252.

[35] *See*, e.g., Morris and Russell (2005).

[36] Russell (2008).

stand has been eroded; given the danger posed by terrorists to the British public,[37] it is perhaps understandable that criminal justice institutions have had their powers widened to enable this form of preventive detention which is, after all court controlled, though it is difficult to understand how any system can claim to require 90 days in order to define the crime for which they are holding a suspect. The general rules of criminal procedure provide for securing mechanisms displaying the degree of protection offered to suspects because of the vulnerability of their positions: all detainees must be brought to court as soon as practicable at the latest at the next court sitting and the courts are charged with providing stringent control of police action. Whilst departing from the fundamental need for a strong justification for the detention of suspected terrorists, these new procedures adhere at least to the spirit of these rules. Nevertheless they doubtlessly provide for an increased risk that innocent persons will lose their liberty, currently for up to 28 days and represent a considerable expansion of a long-standing breach of principle.

Weighing against this tendency, one might, however, note a desire to practicably further secure liberty rights as being witnessed by the reform introduced by the SOCP Act[38] which makes provision for civilian custody officers to check whether the police officers desire for detention is justified. Currently, custody officers are also police officers and the desire to introduce someone less influenced by the local "canteen culture" is reflective of a perceived need to provide effective protection of the right to liberty.

Part 4 of the 2001 Anti-Terrorism, Crime and Security Act regulated perhaps the most controversial reform to the law, provided for *detention without charge for foreign nationals* who, in accordance with article 3 ECHR, could not be deported from the UK. The Government acknowledged its fundamental departure from principle associated with these provisions by derogating from article 5 ECHR (as well as from article 9 of the International Covenant on Civil and Political Rights) because of it.[39]

Article 15 of the ECHR allows derogation "in time of war or other public emergency threatening the life of the nation," which the Government obviously judged the UK to be facing. Nevertheless, though acknowledging that the Government had broad discretion to decide what constitutes a state of emergency, because this is a political judgement,[40] the House of Lords famously found these provisions disproportionate[41] and in conflict with articles 5 and 14 of the ECHR when read together.[42] Consequently, this major departure from legal principle was repealed in 2005.

---

[37] Estimated as very high: the current threat level of the UK is severe, the second highest possible. MI5 has identified 2,000 individuals who pose a threat to the country because of their support for terrorism and estimate that as many as another 2,0002008a may not be known (PA).

[38] *See* sections 120 and 121.

[39] Fenwick, p. 1425.

[40] A and others para. 28 et seq.

[41] Para 68.

[42] A and others.

This scheme was replaced by the Control Orders scheme[43] which the Government controversially regards as so much in line with legal principle that it views most orders made in accordance with the scheme as not requiring a derogation from article 5 ECHR.[44] The scheme thus consists of non-derogating control orders that basically make provision for control mechanisms necessary to curtail a person's ability to participate in acts of terrorism, ultimately house arrest, of UK and non-UK nationals suspected of terrorism-related offences. When the most stringent of conditions are imposed by these control orders, they are viewed as going so far as to require derogation from the ECHR, in which case the scheme speaks of derogating control orders.

Non-derogating orders are made by the Secretary of State for the Home Department after consulting a chief officer of the relevant police force[45] to assert whether there is enough evidence for a prosecution for a terrorism-related offence.[46] Their initial issuing involves no court proceedings and the evidentiary standard required is limited. In 2007, 15 such orders were in operation affecting 9 foreign and 6 British nationals. They order mechanisms falling short of detention in a house arrest setting.[47]

These orders must be made in accordance with section 2 that allows the Secretary of State to make non-derogating orders but requires an application for post-facto court approval (in accordance to section 3 – which provides the parameters to examine whether the decision is flawed; in other words, the evidence upon which the decision is based is not strongly tested). Derogating orders must, however, be made in accordance with section 4 that provides for courts to make them on application by the Secretary of State. Orders are supervised in their application by courts in sittings involving the sighting of closed material and special advocates to represent the interests of the detainee.[48] Effort has thus been made to comply with the principles and spirit of criminal law though these measures – marked strongly by the needs of emergency as they are – do not apply them fully. The principles of public trial as well as the defendants own inherent right to challenge evidence against him or her are restricted in line with the need to protect highly sensitive investigative processes whilst protecting the public. Control order proceedings have been held not to amount to criminal proceedings, that is ones concerning the determination of a criminal charge because no risk of conviction and punishment is inherent.[49] The breach of a control order is, however, a criminal offence.

---

[43] For detail, *see* Forster.

[44] *See* Sec. of State for the Home Dept. v JJ, KK, GG, HH, NN, LL [2006] EWHC 1623 (Admin) (QB); 2008?

[45] s 8(2) PTA.

[46] Section 8(1) PTA as defined by section 1(9) PTA.

[47] s.1(3)a PTA any measure which Secretary of State or Court deems necessary to prevent involvement by the person in terrorism related offences as defined by section 1(9) PTA.

[48] *See* section 3 and schedule of the 2005 Act which provides for special court rules for control order proceedings.

[49] *See* the House of Lords judgment in MB, op cit, paras. 16–24, 48–50 and 90.

14.2.3 Policing the Streets

Protection from police powers in the criminal justice context is naturally not only associated with detention. Critical discussion of the UK criminal justice system in general most frequently relates to police powers to stop and search persons in public space. In a radical departure from the usual standards of policing, sections 44 and 45 of the Terrorism Act 2000 provide for *stop and search mechanisms* not tied by the requirement of reasonable suspicion of the police officer performing such stops and searches. Given how controversially policing powers in this context are discussed and the criticism associated with the reasonable suspicion requirement as to its ability to provide effective protection against abuse of police powers,[50] the move to abandon this principle is a radical one.[51] The degree of abandonment of principle associated with this move in this context is further illustrated by the need perceived by the House of Lords in *R (on the application of Gillan) v Commissioner of the Police for the Metropolis* to hold that such stops must be in reasoned connection with the perceived terrorist threat based upon which police officers use such powers.[52] Given that no police force – let alone instance of government – can claim to unaware of the effect that use of stop and search powers in a manner that can be perceived as racist will have on police relationships with communities, it seems astonishing that this point should require such clarification. Even if one saw no alternative to abandoning the reasonable suspicion criteria when drafting the law, it is a cause for concern that the Legislature apparently saw no need to undertake anything to ensure that the law contained some restriction; ensuring that as few innocent people become subject to coercive police measures as possible. Having seen that even the most basic restriction was apparently left to the courts, one might be forgiven for thinking that anti-terrorist policy in Britain thrives on the abandonment of principle above and beyond any reasonable level.[53] The case of Gillan itself sees the courts allocating the police wide scope to determine the correct use of terror-related powers and failing to react to the claim made in the two cases concerned that the powers were used there for public order-related purposes.[54]

---

[50] Sanders and Young (2007) 67 et seq and (2003) 233–237; for the effect on Muslim communities, *see* Choudhury and Milmo (2008a); for more personal accounts, Oborne (2008); for reflection on this by British authorities, Hewitt (2008), pp. 107–118; for the disproportionate targeting of ethnic minorities, *see* the Independent (2005).

[51] Although not as unusual as one might expect, *see* Sanders and Young (2007) p. 76 et seq. for an overview of stop and search powers without the reasonable suspicion requirement and an evaluation thereof. The courts have emphasised the limits applying to such powers (the need for authorisation of their use by a high ranking police officer within a restricted geographical area) – *see*, e.g., *R (on the application of Gillan) v Commissioner of the Police for the Metropolis* [2006] UKHL 12, paras. 31 et seq.

[52] Para. 81 of the House of Lords judgment.

[53] Note also calls by the Government's independent reviewer of anti-terrorist legislation that use of such stop and search powers must be seriously reduced – *see* Lord Carlile of Berriew (2005) para. 106.

[54] *See*, e.g., para. 50 of the House of Lords judgement.

Police practice in relation to terrorism has long seen the UK under fire, above all in relation to interrogation practices used against suspects in Northern Ireland. As details of these emerged in the past they were discussed as being on the boundary of torture.[55]

Controversy over police practice is currently tragically centred upon the police's *shoot to kill* policy[56] centring upon the ongoing inquest into the circumstances of the death of Jean Charles de Menezes, an innocent Brazilian, tragically and falsely identified as a suspected suicide bomber in Stockwell tube station in 2005. The decision to adopt a policy of this kind is controversial above all due to the danger of irreparable police mistakes, like the case in point. The emerging details of the enquiry do, however, raise questions as to the resources available in such situations and thus inevitably as to the dedication of the authorities to do everything in their power to ensure innocent lives are spared.[57]

14.2.4 The Interaction of Substantive and Procedural Law

On the less dramatic point – relatively speaking – of preserving innocent people from prosecution and conviction, certain changes to the substantive law must be noted. In the anti-terrorist realm, a shift has occurred in relation to the duties of investigated and other persons to co-operate with the police. The fundamental right not to be forced to incriminate oneself has formally not been touched and is still upheld as an important principle of British criminal law. Section 38 B of the 2000 TA, however, imposes broad criminal liability on anyone who has information which they know or believe might be of "material assistance" in preventing an act of terrorism or "securing the apprehension, prosecution, or conviction of another person" (within the UK) who was involved in "the commission, preparation, or instigation of an act of terrorism"[58] and do not report this to the police and provide them with the relevant information.[59] In other words, failure to notify police of circumstances which might have helped prevent a terrorist attack or which might lead to the arrest of anyone involved in such acts has become criminalised. This implies a general duty to pro-actively co-operate with the police imposed upon the general population. It further imposes a duty to second guess the status of police

[55] *See* Ireland v. the UK, judgement of the 18th of January 1978 (1979–1980) 2 EHRR 25.

[56] A policy developed of the existing law by the Metropolitan Police based upon section 3 of the Criminal Justice Act in that it provides for the use of proportionate and necessary reasonable force and developed in regular consultation with and approved by the appropriate official bodies – *see* Gregory (2007a).

[57] Milmo (2007, 2008); cf. also with criteria laid down by the European Court of Justice in McCann and Others v. United Kingdom, ECtHR Series A, No 324, Application No 18984/91 (1995).

[58] Section 38B (1)(a)&(b).

[59] *See also* Fenwick (2007) p. 1412.

investigations and knowledge: how else is a citizen to judge what will be of material assistance to the police? Whilst one cannot deny that this may well be in line with the fundamental aim of achieving justice by convicting the guilty and acquitting the innocent, one must further admit that it expands the law so far and provides for such a degree of uncertainty as to what constitutes criminal behaviour, that it is difficult to imagine it not also bringing "innocent" people within the ambit of the criminal law. In practice, one may well tend to expect that police will not use the provision in such cases; it may even be unlikely that they arise, but substantive protection of the innocent is hard to discern in this provision.

The drawing of innocent persons into the ambit of the criminal justice system is, of course, paralleled in moves to place the financial sector under reporting duties – also witnessed in relation to organised crime in many jurisdictions. These provisions aim primarily to secure cooperation by private entities with the police in preventing terrorist attacks. A failure to fulfil such requirements nevertheless exposes persons innocent of any crime to the threat of punishment for a failure to cooperate with the criminal justice system. In England and Wales, this has occurred in relation to anti-terrorist provisions via the 2001 Anti-Terrorism, Crime and Security Act 2001 which embedded active reporting duties to inform upon persons working in the financial sector by inserting sections 21A and B into the 2000 TA.

Centrally, however, section 38B of the 2000 TA by threatening punishment by criminal law of persons who fail to provide the police with material assistance in terrorism cases is fundamentally not aimed at the general public but at suspects on the fringes of suspicious activity. It is a use of the substantive criminal law to circumvent procedural rules.[60] The threat of significant punishment placed on suspects for a refusal to provide information represents an erosion of the central principle of protection from self-incrimination; a principle traditionally at the heart of British criminal procedure.[61] A person may effectively face the choice of exposing himself to criminal liability under this provision or to incriminating himself by making a statement.[62] That substantive provisions like that described above constitute a serious breach of other long-standing fundamental principles of the criminal law pertaining to the rights of the defendant only appears to confirm the current dedication to abandoning all principles which may be seen to help protect the guilty from

[60] Interestingly section 38B is similar to the provision formerly found in section 18 of the 1989 PT (temporary provisions) Act which was replaced by a permanent anti-terror regime in 2001 by the TA. That a provision of this kind was not considered appropriate in the permanent setting and then only reintroduced in 2001 in a perceived emergency situation – though no longer as a temporary measure – is telling.

[61] Darbyshire (2008) 66 et seq.

[62] But compare this to statements made by the European Court of Human Rights in Heaney and McGuiness v Ireland (2001) 33 EHRR 12 – *see* Clark (2004) 25. The impression is certainly that such offences were created in order to be able to proceed against individuals the authorities wished to place in preventive detention because they are regarded as a risk although there is insufficient evidence to tie them to any classic criminal charge – *see* Walker (2004); potentially they, however, apply to a large group of people and the fact that they are strongly under-used (Fenwick (2007) 1333) only confirms such interpretation of their purpose.

conviction in this context. Contrary to the impression lent by this chapter, such divergence from robust defence rights are a betrayal of the fundamental principles of the British criminal law; defence rights first and foremost bearing the function of protecting the innocent from conviction.

Other changes to the substantive criminal law should also be noted in this context. The Terrorist Act 2000 focused on inciting terrorist acts, on providing training in preparation for terrorist acts or providing instruction or training in the use of firearms, explosives, nuclear materials, etc. and the criminalisation thereof. Similarly the 2006 Act again focused on encouragement and dissemination offences and such behaviour linked to promoting terrorism including expanding the type of organisations that can become proscribed. Little knowledge of the criminal law is necessary to understand that these are phenomena which it is difficult to grasp with the means of the criminal law and that such regulation effectively undermines long-standing principles of criminal procedure. Given the political determination to ensure such behaviour can potentially be punished via the criminal law despite all protest that capturing such behaviour in this context goes against its grain, it is little wonder that the criminal law stands before challenges to its fundamental principles.

14.2.5 The Broader Context

Developments related to the fight against terrorism must further be seen in the context of a *shift in British policing*. The last decade or so is often described as one in which a shift in policing to a more pro-active approach has taken place. Above all in relation to anti-terrorist policy in recent years, a fundamental shift to more pro-active policing rather than a focus on punishing past crime has been observed.[63] Since the mid 1990s, a more general trend towards intelligence[64] led policing, which inevitably means more pro-active policing is also to be identified.[65] This is often connected to technological development with the centralising of police databases encouraged and indeed demanded by the Blair government significantly influencing policing structures.[66] The prolific use of CCTV and other surveillance technologies has also meant the police have more and different sources of information upon which to act pro-actively.[67]

In relation to some offence areas, certain coercive measures have ceased to be tied to traditional pre-conditions – reflecting the stop and search related development in

[63] *See*, e.g., Fenwick 1331.

[64] In relation to anti-terrorist activity, intelligence is identified as "the secret of winning the battle against terrorism in an open democratic society" – Wilkinson (2006), p. 62; the failure to use intelligence has been identified as the missed opportunity to prevent the attacks of 11 September 2001, *see* Fijnaut et al (2004), pp. 1–6.

[65] For an assessment of the very specific, strongly secret service driven, anti-terrorist intelligence situation, *see* Gregory (2007).

[66] *See* Faulkner (2000), South (2000), and Home Office (2000).

[67] *See* Gras (2003), also Whitty et al. (2001), and Walker (2004a).

relation to terrorism.[68] This is true of police forces, specialist police agencies, and those working on the edge of the criminal justice system in more administrative agencies. Indeed some of these, like the Asset Recovery Agency (now integrated into SOCA – a specialist police agency) have been created as part of this move towards pro-active law enforcement outside the central criminal justice system.[69] The fact that data found by one agency can be transferred to and thus used by other agencies means that the lack of equivalents outside the criminal justice realm may be allowing certain principles of criminal procedure to be factually undermined.[70]

Pro-active policing measures were also introduced in relation to anti-terrorist activity particularly in 2001 and 2005. Post-2000, anti-terrorist law became far broader in its application. All the "temporary measures" of the past which had been based upon special powers, previously been highly controversial and regarded as "emergency" features with limited application became anchored into the main body of law, applicable UK wide on a permanent basis. Incitement offences were added to this foundation of normalised extraordinary regulations which come together to form the modern anti-terrorist strategy.[71] Interestingly, these powers were then "significantly underused"[72] and the TA 2006 witnessed a return to more traditional measures. The law began once again to focus upon past offences; though the changed nature of such offences (the stature books now feature crimes of indirect encouragement of and glorifying terrorism alongside very wide preparatory offence definitions) as well as the harsher pre-trial detention conditions introduced, mean, however, that one cannot describe this as a reversal of the tendency to abandon long-standing legal principle in this area.

Anti-terrorist policy in the last decade has thus witnessed a fundamental shift with measures and mechanisms being introduced into the criminal law and practice which seem to fundamentally question that system's dedication to ensuring only those guilty of criminal behaviour can become subject to the tools of criminal procedure (or equivalents). Anti-terrorist policy in Britain appears to be fundamentally oriented to different goals than those stated to be the overriding objectives of criminal procedure. Food for thought considering that terrorist activity should surely be a high priority to the English and Welsh criminal justice system.

14.3 Substituting Criminal Law

Challenges to the criminal law as it is traditionally understood are one matter and though they are certainly fundamental enough to warrant a deep and dividing consideration as to whether or not they undermine the legitimacy of the law, they are not alone in potentially doing so. In the fight against terrorism context, the criminal

[68] *See* para. 9 of the House of Lords judgment in Gillan, op cit and Sanders and Young (2007), p. 76 et seq.

[69] *See*, e.g., Verkaik (2003).

[70] *See* network of agencies in which the ARA worked – ARA.

[71] Fenwick (2007) p. 1371.

[72] Fenwick (2007) p. 1332.

law is challenged not only by changes from within but also by an apparent desire to find alternatives to it. British anti-terrorist policy seems to be strongly marked by a wish to use alternative routes to the criminal law to address phenomena which – as was established in the opening paragraphs of this chapter – fall firmly within its ambit. If the Legislature chooses consciously to pick another mode to impose punitive consequences upon those accused of the most heinous of criminal offences, surely one must recognise that they are inherently calling the criminal law into question, either denying its legitimacy or declaring it ineffective or unsuitable. Since murder, bodily injury, and destruction of property cannot, however, be regarded as anything other than the core business of criminal justice systems, this can in turn not be regarded as anything other than a fundamental challenge to criminal law. One commentator identifies the failure to remain within the criminal justice arena as the most serious threat to human rights principles.[73]

Thus although the discussion of detention without charge and control orders used to deal with suspected terrorists is usually discussed within the context of the criminal law – indeed also in this chapter – it is interesting to note that they are means deliberately removed from the criminal procedure setting. Arguably they are designed to deal with a phenomenon not entirely suited to treatment by the criminal law: the Government's pressingly presented need is to find a mechanisms by which the investigative authorities can remove dangerous suspects from public life and protect society from actions they might take because of the devastating nature of what they are suspected of planning.[74] The courts have shown great sympathy with this goal, accepting the Government's claim that they are acting purely preventively.[75] The perceived need is for a form of preventive detention which, in particular with suicide bombers in mind, cannot afford to wait for a specific offence to be committed before the authorities act. Whilst one might of course wish to argue that state action against such persons can only be justified once they have undertaken certain acts in preparation which thus bring them within the ambit of normal criminal procedure, this is seen to expose the public to too great a risk in this context.[76] As the law stands, the need is apparently for a parallel system to the criminal law. This argument is strengthened by the obligation placed upon the Secretary of State before issuing a control order to consult about the possibility of criminal proceedings – there is no obligation to bring a prosecution even if the evidence is sufficient. She can prefer a control order, thus avoiding the "risk" of an acquittal. The courts and independent reporter on anti-terrorist legislation are understandably critical of this possibility calling upon the Government to prosecute wherever feasible.[77]

---

[73] *See* Gearty (2006) p. 126, 137, and 139.

[74] Home Office (d).

[75] *See* the House of Lords judgement in MB accepting that control order proceedings do not expose the affected person to a risk of punishment - paras. 16–24, 48–50, and 90.

[76] Haymann (2005).

[77] *See* the press, e.g., O'Neill (2008) and Walker (2007) but also (the human rights NGO) Liberty's "charge or release" campaign (http://www.liberty-human-rights.org.uk/issues/2-terrorism/index.shtml). *See also* the High Court judgment of the 16 February 2007 in Secretary of State v E.

Given also that the substantive law has been broadened so far in this area to the point of undermining procedural principles (see supra), the claim of an inability to effectively assert a criminal charge becomes particularly unpalatable. To a certain extent, it may be explained by the current inadmissibility of telephone tap evidence in the UK. For this reason, NGOs have been supportive of the proposal to provide for admissibility as in other jurisdictions[78] though the desirability of this being attached to a judicial warrant procedure rather than connected to the degree of secrecy and undermining of evidential standards the Government appears to desire is a major point of contention in this debate.

One may logically expect to find equivalents to criminal law and procedural principles within such alternate systems (as indeed is the case for a defence of sorts via the Special Advocates in terrorism related proceedings), though these cannot be expected or required to entirely equate to the criminal law as the aim of application (both of the system and, within it, the protecting mechanisms) is fundamentally different.

Whilst there is truth in this argument, it is nevertheless necessary to see consequences for the criminal law in the detention without charge and control order debates above all because of the framework of their discussion. If debate centred only on very short term mechanisms aiming to pull particularly heinous and dangerous suspected criminals off the streets and to place them in preventive detention whilst the investigative authorities prepare a classic criminal case against them, that would form a controversial but perhaps understandable case. The discourse has not, however, been only of that nature. Much court discussion has been devoted to the length of acceptability of subjection to the control order regime[79] with the Executive applying pressure for periods of years to be allowed. Whilst the Government repeatedly emphasises that control orders are to be used only where prosecution is not possible,[80] vociferous reminders

[78] *See* Liberty (2007); Warbrick has, for example, commented that detention without trial was necessary because the Government could not seek a conviction because of not wishing to reveal sources in intelligence gathering operations or because evidence was hearsay displaying the severe consequences the current situation may be having – *see* Warbrick (2004) p. 395.

[79] *See* Sec. of State for the Home Dept. v JJ, KK, GG, HH, NN, LL [2007] UKHL 45; [2006] EWHC 1623 (Admin) (QB).

[80] *See* paragraph 14 of Sec. of State for the Home Dept. v E [2007] UKHL 47. Provision is made by section 8 of the 2005 TA to ensure the Secretary of State consults a chief officer of the relevant police force to check whether there is sufficient evidence for a prosecution and for a requirement that that chief officer is informed of any control order made and then responsible for reviewing the potential for prosecution as long as the control order is in force. Tellingly, there is no requirement that a prosecution is brought and the courts concede that this may be a difficult decision for the Secretary of State to make because she cannot control prosecutions - Baroness Hale of Richmond in paragraph 26 of the above judgement. *See also* McNulty (2008a). Gearty (2005a), pp. 527–529, furthermore points to the very broad number of offences available upon which to base a prosecution, making this all the more astonishing. Arguments have been heard from the Government that this is often not possible have come under attack with the Attorney General, the Director of Public Prosecution, and the former Head of MI5 as well as a number of NGOs arguing that intercept evidence should be made admissible in criminal trials to counter this argument [*see* Liberty (2007)].

aplenty[81] indicate that this tends to be forgotten.[82] Discussion of detention without charge is not in terms of a period of time in which investigative authorities can consolidate a case in order to build a case for prosecution. Indeed in both of these discussions, this idea is surprisingly lacking.[83]

Detention without charge is discussed in terms of a tool to allow investigation at all.[84] Meaning that the investigative authorities in essence want a right to detain in order then to investigate; in other words to deprive of liberty without the usual necessary standards of grounds for doing so. The ultimate measure of criminal procedure is to be taken right at the start of what could potentially become one. The statistics as to how often the police are right in their use of this measure – in terms of how often it translates into results which justify the deprivation of liberty – are not encouraging.[85] This measure appears to precede the criminal process imposing far more severe consequences on far lesser grounds. It is an alternative to the criminal law as we know it, perhaps justifiable in acute emergencies but abhorrent in any longer-term setting.

Far less connected to the standards of the criminal law are the detention without trial and now the control order discussion. Again if these were concerned with controlling a suspect, identified by certain means for a short period, one might speak of a preventive measure – unpalatable for traditional principles perhaps but somehow acceptable in exceptional cases. The discourse relating to control orders is, however, in terms of preventing crime and removing people from society in order to protect it, goals also and indeed often associated with the criminal process. Whilst it may well be unreasonable to demand that the committal of an offence is proved before any measures are taken, given the inherent dangers of the fight against terrorism, it is nevertheless astonishing that the discourse fails to address adequately the consideration that these proceedings should be integrated into criminal ones as soon as possible. Indeed the Government's failure to consider bringing persons subject to control orders to criminal trial has been the subject of severe court criticism[86] and leads to justified speculation that the Government is consciously seeking to avoid the criminal process in these cases-cause for fundamental concern as to the legitimacy of the criminal law or such cases. Even in court consideration, the acceptance of discussing this as of a

[81] Among other counterterrorism experts, Lord Carlile – the Government's independent reviewer of terrorism legislation, has called for more prosecution of terrorism suspects rather than the overuse of control orders – *see* Walker (2007).

[82] Interestingly Gearty (2005), p. 32, identified a trend towards increased prosecution in 2005.

[83] *See*, e.g., O'Neill (2008), Walker (2007).

[84] *See* Haymann (2005), The Independent (2005a), and Steel (2005).

[85] Thus, the police made 1,228 arrests between 11 September 2001 and 31 March 2007, 132 were charged with terrorist offences and 76 handed over to immigration authorities; 41 had been convicted under the Terrorism Act by September 2008 with trials of 114 persons – not all charged with terrorist offences – still pending (Home Office 4).

[86] Secretary of State v E [2007] UKHL 47; [2007] EWCA Civ 459.

purely preventive measure has been broad and the argument that the length and severity of control orders reflect nothing short of a punitive intent has not been faced head on.[87] Whilst the Lords acknowledged that those subject to control orders face a state reaction more severe than most criminal penalties, they accepted these as imposed with nothing but a truly preventive purpose (see supra). This stance is not easily ingestible: it is difficult to avoid speculation that the Government is not using control orders (and indeed deportation) also to punish via alternative proceedings with less onerous standards than the criminal law, thus both avoiding and undermining the latter.

Control orders could be seen as a preliminary measure to provide security during a time in which the authorities build a criminal prosecution based upon the evidence they have upon the basis of which, for example, house arrest is ordered. If the suspect is dangerous enough to warrant the kind of treatment ordained by the control orders scheme, surely he is also deserving of punishment by the criminal law and surely such a case can be built – possibly dependant on "phone tap evidence" being openly admissible? Why the Government has chosen to build a longer term scheme which appears to be an alternative to the criminal justice system, deliberately placed as it is outside the criminal justice realm (though retaining its sword for enforcement purposes by ensuring breaches are punishable as criminal offences) is a question which needs to be asked. There are options available which would preserve the integrity of the criminal law in its purpose and procedure far better: the marking of cases in which a control order is used as having priority for trial within the criminal justice system would ensure their use was kept to a minimum and detention transferred into the usual realm of punishment for a proved wrong-doing as soon as possible. The Government's decision to seek an alternative to this system in the control order schemes is an apparent abandonment of the principles of criminal procedure and thus of the dedication to convicting the guilty and acquitting the innocent.

This can be explained, of course, if one treats terrorism purely as a political problem and thus accepts the release of – thus labelled – political prisoners as part of the price of peace,[88] the question is of course as to its legitimacy when it cannot be seen as an element of peace – the conflict is not yet over – and how it can be used on this scale when the criminal justice system remains such a clear alternative.

One might seek to explain this by the origin of the control orders scheme as a follow on to the detention without trial scheme: designed as it was to deal with foreign citizens who the Government wished to deport but could not, given its

[87] *See* the House of Lords judgment in MB, op cit. – the failure to address this argument also means that deeper issues also remain to be addressed, most fundamentally of course the fact that depriving suspects of rights is to fall for the fallacy of presuming guilt, the cardinal sin in undermining the principles of criminal procedure – *see* Luban (2005) 252–254.

[88] In relation to the Northern Ireland Settlement, *see* Warbrick (2004), pp. 375–376.

human rights obligations.[89] Whilst this provides a logical explanation, it is nevertheless astonishing in what it reveals about Government attitudes to the principles of criminal law. The criminal law is intended to punish those who commit crimes. Those suspected of actions serious enough to warrant their deportation or detention from Britain in the anti-terrorist (but also indeed in any) context should surely have been implicated in offences so serious that society has a strong interest in seeing them punished. The idea that the criminal law should not be enforced and no punishment achieved appears a highly pragmatic and unprincipled approach.[90] Surely someone guilty of such a heinous crime is deserving of severe punishment and this should be ensured by inflicting it, not taking the risk that transfer to the country of origin might be an equivalent punishment? Where such breaches have occurred, the rule of law demands that our sovereign ensures that the law is applied equally. This would occur by ensuring punishment via the criminal justice system is enforced. Deportation, in this case, appears to be bowing to more pragmatic considerations; intending to save Britain the cost of trial and of incarceration (the assumption, in good faith, is that the calculation is not to avoid the risk of an acquittal[91]) and the effort of dealing with such persons all together. No matter where one stands on such practices in normal cases,[92] this is unacceptable in such serious cases. Not only must one view matters from a preventive point of view: speculating that the possibility that such dangerous persons re-enter the UK or another EU member state are considerably higher than them posing renewed danger to society by escaping from an incapacitating prison sentence.[93] Above all, it is not the liberal protective

[89] Although there is no fundamental difference in the treatment of British citizens and non-British citizens inherent in the criminal law, the possibility of deportation will certainly mean that factually treatment may differ. This has become particularly clear recently in the discussion of detention without trial (Section 4 of the Anti-Terrorism, Crime and Security Act 2001) and thus in the anti-terrorist context – where an argument of discrimination was brought before the courts and could be made that such specialist mechanisms are a clear indication of a willingness to treat different categories of suspects differently. The House of Lords was critical of this argument stating that the scenario in question related specifically to foreigners who were thus in a situation British citizens could not find themselves in. This scheme was in force from 2001 until 2004 when it was declared in breach of articles 5 and 14 of the European Convention by the House of Lords in *A and others v the Secretary of State for the Home Department* ((2004) UKHL 56;[2005] 2 AC 68; [2005] 2 WLR 87; [2005] All ER 169). The Government then replaced this with the control orders scheme which falls outside of the criminal justice system (*see* part 4 of the 2005 PTA) and is applicable to both British citizens and foreigners.

[90] The depths of this pragmatism and lack of principle can be seen in the UK's intervention in the case of Saadi before the European Court of Human Rights, in which it argued as a third party intervener argued that the risk a deportee faces of being tortured should be balanced against the risk he poses to national security in the state wishing to deport him: *see* Saadi v. Italy, judgement of the Grand Chamber of the 28 February 2008 (application number 37201/06) and Dworkin (2008).

[91] Although this is not always easy to maintain in the face of cases such as Yezza, *see* Osley (2008).

[92] Germany, for instance, requires a sentence to at least 3 years to allow deportation as a consequence – Szyszkowitz (2005), p. 50.

[93] Note, for example, that 3 of 18 men placed under control orders – a scheme firmly in control of British authorities – have absconded: Liberty (2007).

principles of the criminal law which appear abandoned by this approach.[94] Where the state fails to punish a person accused of the most heinous of offences; where it systematically avoids doing so perhaps for pragmatic reasons, this calls the very purpose of criminal law into question. If one does not use the mechanisms of criminal law to deal with persons suspected of planning and preparing mass murder, then when? What legitimacy can a system have which is used to prosecute thieves but considered irrelevant for terrorists?

The decision to use alternative mechanisms, that is, to find substitutes for the criminal law, in the fight against terrorism is an effective questioning of the criminal laws suitability to deal with the most serious of criminals, perhaps the most serious challenge to its legitimacy imaginable.

Interestingly the control order scheme is not the only source of such a challenge. The anti-terrorist resources emphasised in Britain are often not part of the criminal justice system. The Terrorism Act 2000, for instance (in section 28), provides for forfeiture of seized cash by civil proceedings with no requirement of criminal proceedings attached. Furthermore the anti-terrorist realm is not free of the general trend to emphasise asset recovery rather than punishment of individual wrong-doers (the use of the powers lent to criminal justice agencies under the Proceeds of Crime Act 2002 is emphasised by the Home Office, and a specialist Terrorist Finance Investigation Unit[95] concentrates on recovering the funds that could potentially be made available to terrorists;[96] indeed the heart of the Government's counter terrorist strategy is often reported to be to seek to "disrupt and destroy criminal networks without necessarily prosecuting them through the courts"[97] via such mechanisms. The Government faced defeat in the High Court after labelling five men terrorists and apparently trying to deal with them via asset freezing mechanisms.[98]

Of the 1165 arrests made under the TA 2000 and the 63 under other legislation following a terrorist investigation between 11 September 2001 and 31 of March 2007, 132 were charged with terrorist offences (41 convictions resulted to date), 109 with such and other criminal charges, 195 with other offences ranging from murder to fraud and false documentation (171 convictions for such alternative charges so far, 114 still await trial), 76 were handed over to immigration authorities (plus two further remanded awaiting extradition proceedings), and 669 released without charge.[99] On 10 September 2008, 16 non-derogating control orders were in force (4 relating to British citizens).[100] In 2007, 15 were in operation involving

[94] The control orders scheme thus has serious implications for any right to be informed of the case against one – *see* Norton-Taylor (2008).

[95] Reportedly established to prevent anyone associated with terrorism securing any assets at all (The Times 2007).

[96] Home Office.

[97] O'Neill 2008.

[98] *See* the judgement in the A, K, M, Q, and G v HM Treasury case, The Times (2008) – *see* Dodd (2008).

[99] Home Office (c).

[100] McNulty (2008).

9 foreign and 6 British nationals.[101] The written ministerial statement for up until June 2007 stated "A total of 244 separate accounts and approximately £570,000 of suspected terrorist funds have been frozen in the UK since 2001."[102] Whilst it is thus impossible to estimate in which cases the criminal law and its alternatives are being appropriately used to combat terrorism in the UK, there are plenty of grounds to assume that the criminal law may well be being undermined by other procedures and measures available.

14.3.1 Anti-Terrorist Policy Within the Broader Trend

Looked at as a whole, one cannot avoid identifying British anti-terrorist policy as marked at least as strongly by the language of risk assessment and management as by the punitive language of traditional criminal justice.[103] The Government's CONTEST anti-terrorist strategy, in place since 2003, consists, for example, of concerted efforts to prevent radicalisation "by addressing structural problems in the UK and abroad," to pursue terrorists among other means by "disrupting terrorist activity and taking action to frustrate terrorist attacks and to bring terrorists to justice through prosecution and other means, including strengthening the legal framework against terrorism" and protecting potential targets via close co-operation with the private sector.[104] The Anti-Terrorism Crime and Security Act 2001, for instance, concentrated on matters ranging from immigration to securing nuclear power and aviation as well as dangerous substances alongside placing emphasis upon work in the financial sector.[105] The strategy is one of a holistic approach to security management and whilst this seems perfectly reasonable it may explain the number of fundamental challenges the criminal law and justice system faces because of it. The very real needs of prevention cannot be confused with or allowed to intrude upon the territory marked for the criminal law; the consequence is the disintegration of principle we currently witness.

Placing such developments in anti-terrorist law within the broader trend may also provide greater understanding of the developments described here though one may be

[101] Home Office, though according to Liberty (2007) it appears to have been 18.

[102] By 2008, the relevant figures were "263 separate accounts containing over £650,000" – *see* http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080520/wmstext/80520m0001.htm, note that asset recovery and freezing is foreseen in accordance with section 28 of the 2000 TA but that these orders are described as in line with the Terrorism (United Nations Measures) Order 2006.

[103] Beck (1992); Braithwaite (2000) – in this respect, it is also interesting to note that an additional 61 million pounds sterling have been allocated to the responsible police forces to fight terrorism, whilst far greater sums have gone to the health service and fire services to enhance coping capabilities [Home Office (f)]

[104] Home Office 3.

[105] Home Office 2001.

justifiably surprised at their appearance within so serious a policy area. During recent years, Britain has seen an unprecedented search for mechanisms outside the criminal law to deal with undesirable behaviour and, for example, the tendency to focus on mechanisms such as asset recovery, rather than punishment identified above.[106] Perhaps most famously discussion of this has centred around very petty "offences" or nuisance behaviour for which "anti-social behaviour orders"[107] (court orders issued by a civil court, the breach of which is, however, a criminal offence punishable by up to 5 years prison) are available.[108] The fundamental restructuring of anti-terrorist weaponry thus comes at a time which is marked by a tendency to use alternative proceedings – reminiscent of what Continental lawyers would refer to as administrative proceedings – to achieve criminal justice aims. Taken together with the British tradition of using specialist agencies such as the Serious Fraud Office (a policing organisation), the (recent and now debunked) Asset Recovery Agency (which used civil proceedings), or the Health and Safety Executive (a regulatory agency) to pursue goals usually associated with criminal proceedings, the broader setting must be borne in mind for a sense of context. Non-criminal justice mechanisms often flank the criminal law and may provide powerful tools in many other contexts. Thus, it is perhaps not surprising that this development lends impetus to how things are dealt with in this arena. Nevertheless, it seems inappropriate that such mechanisms should be adopted where the criminal law already provides for the desired action and where strong arguments call for it to remain untouched flanked by complementary not replaced by alternative measures. In relation to such serious crimes, the systematic use of such alternatives would appear to challenge the very existence of the criminal justice system.

Beyond purely philosophical consideration, such categorisation has fundamental consequences for those affected by such proceedings. The criminal law is special in particular because of the high standards of protection developed for those subjected to its proceedings and, of course, because of the punitive nature of the consequences imposed upon those found guilty. As the overarching purpose states: the Criminal Procedure Rules provide for justice to be done respecting the rights of the defendant. Thus, for instance, article 76(2)(a) PACE excludes the use of evidence possibly obtained by use of torture abroad in criminal proceedings (though the applicability of this provision becomes more questionable in relation to other proceedings because of the way the balance of proof is regulated in them[109]). Challenges to the use of criminal law are thus not only challenges of form. They go to the very heart of constitutional substance. Furthermore, the punitive imposition of consequences upon an individual by the Executive raises a fundamental issue concerning the relationship between state and citizen and the lines and mechanisms demarking acceptable behaviour within society. Any decision not to adhere to the principles of

[106] *See*, e.g., Summers 2003.

[107] Created by section 1 of the Crime and Civil Disorder Act 1998.

[108] *See* Home Office (e).

[109] Fenwick, p. 1346.

criminal law automatically opens the debate about the standing of other principles. A decision not to use the criminal law is not the bottom but only the top of a very slippery slope indeed.

14.4 Conclusion

Recent development of anti-terrorist law, policy, and practice is irrevocably linked to a number of challenges made to the nature of criminal law and procedure. Government initiatives have resulted in an unprecedented number of changes being made to the statute books which challenged many of the principles regarded as most fundamental to British law for decades if not centuries.

Above all this shift is of great meaning because it involves a shift in relation not only to defendants and their rights and how they should be treated – which can be paralleled to many other changes associated with criminal justice systems turning to more actuarial or managerial forms[110] – but also by a fundamental shift in discourse on the need to punish (or rather the lack of it). It is astonishing to see the Government seeking tools to control those suspected of the most heinous of crimes but satisfying themselves with doing so only for a relatively short period and not transferring this responsibility into the appropriate punitive arena of punishment which also houses the potential to ensure punishment is proportional. Fascinatingly the anti-terrorist discourse altogether is cased not in the language of crime and punishment even in relation to what should happen to suspects, but almost entirely in a risk management vocabulary even when it comes to dealing with individual perpetrators.

One might of course suspect this to be because the Executive recognises its inability to prove the necessity to punish those suspects it holds under alternative regimes but such argument surely lacks credibility even for the most hardened cynic. The apparent will to sideline the traditional mechanisms of criminal law or the protective principles of criminal procedure in favour of easier solutions is not one which will surprise commentators of criminal law. Given the current threat assessment (currently at severe – the second highest level available which defines that "an attack is highly likely"[111]), one would probably find a lack of such challenges to individual fundaments of the criminal law more perturbing. Taken in their current number, together with the alternatives the British Government is consistently favouring to deal with aspects of terrorist crime as well as the apparent abandonment of a longer-term punitive discourse in relation to suspected terrorist, these challenges to criminal law, must however, be viewed as questioning the very basis of criminal law's existence. Whether this is the knee-jerk reaction of a system unable to cope with the problems it faces and thus a temporary, if extreme disregard for a system currently viewed as cumbersome or a more fundamental challenge to the legitimacy and very existence of the criminal law, currently heralded by deliberate disregard for the principles and potential of criminal justice, remains to be seen.

[110] Feeley and Simon (1994).

[111] *See* http://www.homeoffice.gov.uk/security/current-threat-level/

References

ARA Introduction to the Asset Recovery Agency. Available at http://www.assetsrecovery.gov.uk/MediaCentre/Publications/

BBC (2008). Interview with Lord Woolf BBC. Breakfast TV, 1st September.

Beck, U. (1992) Risk Society. London: Sage.

Beckman, J. (2007) Comparative Legal approaches to Homeland Security and Anti-Terrorism. Aldershot and Burlington: Ashgate.

Blair, I. (2005). Speech at Urban Summit Conference. Available online under http://cms.met.police.uk/news/policy_organisationa…general_information/cmsr_s_urban_age_summit_speech

Braithwaite, J. (2000). The New Regulatory State and the Transformation of Criminology. The British Journal of Criminology, 40/2, 222–238.

Chadwick, E. (1997) Terrorism and the Law: Historical Contexts, Contemporary Dilemmas and the End(s) of Democracy in Crime, Law and Social Change, 26, 329–350.

Choudhury, T. Victims of Law? Muslim Communities across Europe (this volume).

Clark, D. (2004) Bevan & Lidstone's The Investigation of Crime. 3rd edition. London et al.: LexisNexis Butterworths.

Darbyshire, P. (2008) England and Wales in Vogler, R. and Huber, B. (eds.) Criminal Procedure in Europe. Berlin: Duncker & Humblot.

Davenport, A. and Baauw, P. (1995) Police Detention in the UK and in the Netherlands in Fennell, P. and Harding, C. (eds.) Criminal Justice in Europe, 251–264. Oxford et al.: Clarendon.

Dodd, V. (2008) Court Criticises more Anti-Terror Legislation. The Guardian, 25 April.

Duff, A. Criminal Law in the Stanford University Encyclopaedia of Philosophy

Dworkin, A. (2008) EU Governments Should Welcome Today's ECHR Ruling on Torture. European Council on Foreign Relations Commentaries. 28 February. Available at http://www.ecfr.eu/content/entry/commentary_dworkin_on_saadi.htm

Feeley, M. and Simon, J. (1994) "Actuarial Justice: the New Emerging Criminal Law," in D. Nelken, ed., The Futures of Criminology. London: Sage.

Feldman, D. (2006), Human Rights, Terrorism and Risk: the Roles of Politicians and Judges, Public Law 364–384.

Fenwick, H. (2007). Civil Liberties and Human Rights. London et al.: Routledge-Cavendish.

Fijnaut, C., Wouters, J. and Naert, F. (2004) Introduction in Finjaut, C., Wouters, J., and Naert, F. (eds.), Legal Instruments in the Fight against International Terrorism. Leiden and Boston: Martinus Nijhoff.

Gibb, F., Tendler, S. and Ford, R. (2004). Rougher justice for Drug Barons and Gangsters: Reasonable doubt should be set aside for worst crimes, says Blair. *The Times*, 10 February.

Gras, M. (2003) Kriminalprävention durch Videoüberwachung – Realität in Großbritannien, Zukunft in Deutschland? Baden-Baden: *Nomos*.

Faulkner, D. (2000) Government, public service and criminal justice in Criminal Justice Matters, Nr. 38, Winter 1999/2000, p. 4.

Foreign Policy and the Fund for Peace (2005) The Failed States Index. Foreign Policy. July/August.

Gearty, C. (2005) 11 September 2001, Counter-Terrorism, and the Human Rights Act in Journal of Law and Society, Vol. 32, No. 1, March 18–33.

Gearty, C. (2005a) Human Rights in an Age of Counter-Terrorism: Injurious, Irrelevant of Indispensable? Essays on Human Rights and Terrorism. Cameron May.

Gearty, C. (2006) Can Human Rights Survive? Cambridge: Cambridge University Press.

Gearty, C. (2007) Civil Liberties. Oxford: Oxford University Press.

Golder, B. and Williams, G. (2004) "What is Terrorism?" Problems of a Legal Definition. 27 University of New South Wales Law Journal, 270.

Green, C. (2008) Anti-terror laws used to spy on family. The Independent, 11 April.

Gregory (2007) An assessment of the contribution of intelligence-led counter-terrorism to UK homeland security post-9/11 within the "contest" strategy, pp. 181–202 in Wilkinson, P. (ed) (2007) Homeland Security in the UK. London and New York: Routledge.

Gregory (2007a) Police and counter-terrorism in the UK, pp. 203–247 in Wilkinson, P. (ed) (2007) Homeland Security in the UK. London and New York: Routledge.

Haymann, A. (2005) Letter from the Assistant Commissioner Andy Haymann to the Home Secretary, 5 October – available at www.statewatch.org/news/2005/oct/met-letter-law.p
Hewitt, S. (2008) The British War on Terror. London: Continuum.
Home Office and Northern Ireland Office (1998) Legislating Against Terrorism: A Consultation Paper, Cm 4178.
Home Office (2000) Home Secretary's Foreword in The Government's Crime Reduction Strategy, S. 1, Home Office, London.
Home Office (2001) Security Anti-Terrorism, Crime and Security Act 2001, http://www.homeoffice.gov.uk/security/terrorism-and-the-law/anti-terrorism-crime-se
Home Office (a) Security Targeting terrorist funds http://www.homeoffice.gov.uk/security/protecting-the-uk/targetting-terrorist-funds/
Home Office (b) About the counter-terrorism strategy http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy/
Home Office (c) Security Terrorism and the Law http://www.homeoffice.gov.uk/security/terrorism-and-the-law/
Home Office (d) Control Orders http://www.homeoffice.gov.uk/security/terrorism-and-the-law/control-orders/?version = 4
Home Office (e) Anti-Social Behaviour Orders http://www.homeoffice.gov.uk/anti-social-behaviour/penalties/anti-social-behaviour-orders/
Home Office (f) How we're protecting the UK http://www.homeoffice.gov.uk/security/protecting-the-uk/
The Independent (2005) Terror Bill: Taking liberties. The Independent, 3 March.
The Independent (2005a) Terror Legislation: The 90 days battle. The Independent, 9 November.
Liberty (2007) Liberty's response to the Joint Committee on Human Rights: "Relaxing the Ban on the Admissibility of Intercept Evidence." February. Available at: http://www.liberty-human-rights.org.uk/pdfs/policy07/liberty-intercept-evidence.pdf
Lord Carlile of Berriew (2006) Report on the operation in 2005 of the Terrorism Act 2000. http://security.homeoffice.gov.uk/news-publications/publication-search/terrorism-act-2000/tact-2005-review?view = Binary
Lord Lloyd of Berwick (1996) Inquiry into Legislation against Terrorism, Cm 6420, October. London: HMSO.
Luban, D (2005) Eight Fallacies about Liberty and Security in Wilson, R.A. (ed.) Human Rights in the "War on Terror." Cambridge: Cambridge University Press.
Macdonald, K. (2008) We must not degrade our liberties in the name of defending them, CPS inaugural lecture, 20th October 2008, reported in the Independent, 21st October 2008.
McNulty, T. (2008) Control Order Powers (11th June 2008 – 10th September 2008), statement to Parliament of the 15th of September 2008. http://security.homeoffice.gov.uk/news-publications/publication-search/control-order-statements/control-orders-statement-100908?view = Binary
McNulty, T. (2008a) Letter to the Editor. The Guardian, 20 June.
Milmo, C. (2007). Officers Involved in De Menezes Killing Escape Disciplinary Action. The Independent, 22 December.
Milmo, C. (2008a) Muslims Feel like "Jews of Europe." The Independent, 4 July.
Milmo, C. (2008). De Menezes Tragedy "Could Happen Again." *The Independent*, 26 September.
Ministry of Justice (2008) The Criminal Procedure Rules. London: The Stationary Office.
Morris, N. and Russell, B. (2005) 90 days: Plans to Lock up Terror Suspects Without Charge Provoke Outcry. The Independent, 13 October.
Morris, N. (2007). Blair Accuses Courts of Putting Rights of Terrorist Suspects First. *The Independent*, 28 May.
Norton-Taylor, R. (2008) Terror Suspects Need not be Told of Evidence. The Guardian, 18 October.
Oborne, P. (2008) The Enemy Within? Fear of Islam: Britain's New Disease. The Independent, 4 July.
O'Neill, S. (2008). Is SOCA just too Soft? The Times, 13 May.
Osley, R. (2008) "Draconian" Home Office Fast-Tracks Algerian's Deportation. The Independent, 25 May.

Russell, B. (2008). Home Secretary Forced into "Humiliating Retreat" over Detention Plans. *The Independent*, 14 October.
PA (2008a). Great Terror Plot Building up. The Independent, 14 October.
PA (2008b). Plan to Name and Shame Barred "Hate Preachers." The Independent, 28 October.
Sanders, A. and Young, R. (2003) Police Powers in Newburn, T. (ed) Handbook of Policing, 228 – 258. Willan: Culhampton.
Sanders, A. and Young, R. (2007) Criminal Justice, 3rd ed., Oxford: OUP.
Sengupta, K. (2008). Spies Take War on Terror into Cyberspace: New Approach Tackles "Severe Threat" of Attacks by Funding Monitoring Network. The Independent, 3 October.
Smith, A.T.H. Balancing Liberty and Security? A legal analysis of United Kingdom Anti-Terrorist Legislation (this volume).
Spencer, J. Telephone Tap Evidence and Administrative Detention in the United Kingdom. (this volume).
South, N (2000) Late-Modern Tension not Post-Modern Transformations in CJM, no. 38, Winter 1999/2000, p. 5.
Steel, M. (2005) The Compelling Case for more Police Powers, The Independent, 10 November.
Steele, J. (2003) Blunkett Takes Swipe at Judges, The Daily Telegraph, 15 May.
Summers, J. (2003). We're Innocent Until Proved Guilty… or Until Our Assets Are Seized. The Times, 25 November.
Szyszkowitz, T. (2005) Germany in von Hippel, K. (ed.) Europe Confronts Terrorism. Basingstoke: Palgrave Macmillan.
The Times (2007). Terrorism Assets Unit "Flawed." The Times, 2 March.
The Times (2008). Anti-Terror Asset-Freezing Order Improperly Made. The Times Law Reports, 5 May.
Verkaik, R. (2003) Gangsters' Assets to be Seized by New Agency. The Independent, 24 February.
Warbrick, C. (2004) Emergency Powers and Human Rights: the UK Experience in Finjaut, C., Wouters, J., and Naert, F. (eds.) Legal Instruments in the Fight against International Terrorism. Leiden and Boston: Martinus Nijhoff.
Walker, C. (2004) Political Violence and Commercial Risk, 56 Current Legal Problems 531
Walker, C. (2004a) Terrorism and Criminal Justice: Past, Present and Future, Crim LR, May 311.
Walker, P. (2007) Control Orders Breach Human Rights, Law Lords Say. The Guardian, 31 October.
Wilkinson, P. (2006) Terrorism versus Democracy - the Liberal State Response. 2nd ed. London and New York: Routledge.
Whitty, N., Murphy, T. and Livingston, S. (2001) Civil Liberties Law: The Human Rights Act Era. Butterworths;
Wolfowitz, P (2002) Interview with the San Francisco Chronicle, February 23.
Zedner, L. (2005) Securing Liberty in the Face of Terror: Reflections from Criminal Justice, Journal of Law and Society, 32/4, 507–533.

Chapter 15
Balancing Liberty and Security? A Legal Analysis of UK Anti-Terrorist Legislation[1]

Tony Smith

Nobody could doubt that the events of 11 September 2001 in New York and Washington have had an enormous impact on our social, political, and legal existences – and no doubt either that the world has changed irrevocably as a result. We will continue to feel the aftershocks for decades to come, as the most powerful nation on earth and its allies come to terms with the fact that they are not immune from the scourge of terror. The international, border-crossing nature of terrorism is illustrated by further incidents since then; bombings in Bali (October 2002), the trains in Madrid (March 2004), and the underground and bus bombings in London (7 July 2005). There can be no escaping the fact that there are some who will continue to seek to target civilian populations indiscriminately, using the suicide bomb, chemical weapons, and possibly worse without warning. How then should the legal system respond?

One of the principal aims of terror is to destabilise by creating uncertainty, and to make its targets question whether their institutions and practices (including laws) are any longer fit for the purpose for which they were created, and forcing those targets to re-think questions that were long thought to have been resolved. Has the time come to require UK citizens to adopt a practice common to its European partners and possess identity cards?[2] Are the courts that administer the ordinary law of the land adequate to deal with the various legal disputes that arise from such atrocities – whether they be criminal prosecutions or the deportation of those suspected

T. Smith (✉)
Pro Vice-Chancellor (Government Relations) and Dean of Law Director,
NZ Centre for Public Law School of Law, Victroia University of Wellington, New Zealand
e-mail: Tony.Smith@vuw.ac.nz

[1]Originally published by Springer Science + Business Media in the *European Journal on Criminal Policy and Research*, issue 13:1–2 (April 2007), pg. 73–83.

[2]See the response of the Director General of Liberty, Shami Chakrabarti, "Nothing to Hide, Nothing to Fear" (2004) *Counsel*, May, p.10; A. Khan, "Identity cards: the final nail in the coffin of civil liberties?" (2006) *J. Crim. L.* 139–146. In spite of considerable opposition, the Identity Cards Act 2006 received the Royal Assent on 30 March 2006, but no date appears to have been set for its implementation.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_15, © Springer Science+Business Media, LLC 2010

of terrorist activity – or must some other, special tribunal be found? How does the law of self-defence and prevention of crime (not a very certain branch of the law at the best of times) apply to the prevention of the suspected suicide bomber?[3] More fundamentally, can torture ever be justified as an acceptable response to terror?[4] Those who resort to the methods of terror have, after all, no regard for the rights and interests of their innocent victims. Why should democracy be forced to fight with one arm tied behind its back?[5]

Whatever the answers to these difficult questions might be, there can be no real doubt but that governments have the constitutional duty to take countermeasures to ensure the safety of their citizens and others. Whether that duty extends so far as to permit the American decision to start a faux "war on terror"[6] in collaboration with such of its allies who were prepared to give it credence, and in pursuit of that to start a genuine military war on Iraq[7] has heightened the strains and given the matter a global (and so far as the UK is concerned a far less controllable) dimension. On the legitimacy of employing one particular countermeasure, namely imprisonment at Guantanamo Bay, the Bush and Blair governments have been consistently at odds. It will have given some satisfaction to those heading British attempts to exert a restraining influence[8] that the

[3] The police have shown a degree of uncertainty about this issue. Witness in particular the shooting of the Brazilian electrician (Mr Jean Charles de Menezes) apparently suspected of being a suicide bomber in the Stockwell London underground station on 22 July 2005. Was this sort of anxiety what prompted the Metropolitan Police Commissioner to begin taping his telephone conversations with the Attorney-General? *See* Nolten (2005) 156 New Law Jo 693.

[4] The House of Lords has answered this question with a resounding no, in *A v Secretary of State for the Home Department (No 2)* (2005) UKHL 71, [2005] 3 W.L.R. 1249, as to which see my note in the Smith [2006] C.L.J. 252. And *see* Lord Hope, "Torture" (2004) 53 I.C.L.Q. 807. But the then Home Secretary told Parliament, "I say that the right to be protected from the death and destruction caused by indiscriminate terrorism is at least as important as the right of the terrorist to be protected from torture and ill-treatment"; Hansard, H.C., 26 October 2005, cc 325–328.

[5] As it was so memorably put by the President of the Supreme Court of Israel A. Barak in *Public Committee Against Torture v Israel*, 26 May 1999, H.C. 5100/94.53(4) P.D. 817, 845. *See also* his "Foreword: A Judge on the Role of the Supreme Court in a Democracy" Barak (2002) 116 Harv. Law R. 16.

[6] For an interesting exploration of the consequences of regarding terrorists as being combatants in a war rather than as ordinary criminals who should be dealt with by the ordinary processes of the domestic criminal law, *see* Vaughan Lowe, "'Clear and present danger': Responses to Terrorism" (2005) 54 I.C.L.Q. 185.

[7] *See* generally, Phillippe Sands, *Lawless World* (2006), chapter 8 for a passionate elaboration of the argument that the war was unlawful.

[8] See in particular the Attorney General Lord Goldsmith's (2005) speech to the CBBE (Paris) "Balancing Security and Fundamental Rights – the EU Presidency view" 19 November 2005. Lord Goldsmith was complaining in particular about the inappropriate partiality of the Military Tribunals through which it was intended to prosecute the detainees, a view later vindicated by the decision of the US Supreme Court in *Hamdan v Rumsfield* (decided 29 June 2006)

US Supreme Court decided[9] several important cases on the legality of detention in Guantanamo Bay against the arguments of the Bush Administration. It is noteworthy (not to say encouraging) that one member of that court, at least, had given some indication that she thought it appropriate to look beyond the confines of the USA for supplementary reassurance as to how[10] such issues might be resolved.

In seeking to appraise the measures that might appropriately be adopted to cope with the challenges of terrorism, it is important to keep perspective[11] and proportion.[12] As I have pointed out on a previous occasion,[13]

> … it would be a mistake to suppose that the United Kingdom law devoted to the suppression of terrorism is entirely modern, let alone the reaction to the events that convulsed the world following the attacks in the USA in September 2001. Continuing problems in Northern Ireland meant that the statute books were replete with offences directed against terrorist groups and their activities.[14] Some time before the American events and in the light of a continued improvement of the situation in Northern Ireland, it had been decided to place the legislation hitherto designated as "Temporary" with a revised framework. The opportunity was to be taken at the same time to acknowledge that there was an increasingly international dimension to terrorism, and the result was the Terrorism Act 2000.[15]

The Terrorism Act 2000 was intended to be the final British statement of the law relating to terrorism. But 9/11 changed all that and fresh legislation was immediately forthcoming. The quoted passage continued:

---

[9]The cases were *Rasul v Bush* 124 S. Ct. 2686 (2004) (Sup Ct (US) on whether the US courts have jurisdiction to hear habeas corpus claims brought by non-US nationals with respect to their detention at the Guantanamo Bay centre; *Hamdi v Rumsfeld* 124 S. Ct. 2633 (2004) (Sup Ct (US) on whether the Government had the authority to detain a US citizen as an enemy combatant on the ground that he had allegedly engaged in military action against US forces in Afghanistan; *Rumsfeld v Padilla* 124 S. Ct. 2711 (2004) (Sup Ct (US) on whether the detention of a US citizen, who had been unarmed on capture and was not accused of involvement in the Afghan conflict, was unconstitutional. For discussion, *see* David Golove, "United States: the Bush administration's "war on terrorism" in the Supreme Court" (2005) I.J.C.L. 128–146. *See also* O. Fiss, "The War Against Terrorism and the Rule of Law" (2006) 26 O.J.L.S. 235.

[10]Ruth Bader Ginsberg, "'A Decent Respect to the Opinions of [Human] kind': The Value of a Comparative Perspective in Constitutional Adjudication" [2005] C.L.J. 575.

[11]Including, it might be said, historical perspective. It is not complacent to point out that the British experience in the course of the twentieth century included two world wars, and the second of these involved assaults upon the civilian population of London and other cities such as Coventry and Plymouth causing far greater casualties that anything yet inflicted by Al Quaeda.

[12]Lord Bingham, "Personal Freedom and the Dilemma of Democracies" (2003) 52 I.C.L.Q. 841.

[13]Ed. D. Feldman, *English Public* Law (2004) p. 1334. The passage was cited in full by Lord Walker of Gestinghope in *A v Secretary of State for the Home Department* [2004] UKHL 56, [2005] 2 A.C. 68, at [199].

[14]One might instance in particular the Explosive Substances Act 1883 as an example of this. *See* C.A. Gearty and K.D. Ewing, *The Struggle for Civil Liberties: Political Freedom and the Rule of Law* (2000).

[15]For the criminal law aspects of which, *see* J.J. Rowe, "The Terrorism Act 2000" [2001] Crim. L.R. 528.

> Further initiatives were taken in response to the American atrocities, in the Anti-terrorism, Crime and Security Act 2001.[16] These confirm and extend the measures relating to proscribed organisations, for example, membership or support for which – Irish and other domestic or foreign groups – is a criminal offence. The Acts additionally offer extended police powers, including powers to set up cordons, compulsory obtaining of testimony and evidence, additional disclosure powers in connection with financial organisations, account monitoring information, arrest without warrant, stop and search, search of premises[17]; search of persons, parking restrictions, port and border controls, retention of communications data, electronic surveillance, curtailment of access to legal advice and the right to silence and prohibitions on torture.[18]

All of these measures have manifestly given the state huge powers to intervene in the lives of subjects and citizens, nominally in the interests of preventing terrorism. In an article of this length, it will not be possible to examine each of these developments in any depth. But there are some overarching issues that arise when executive governments, faced with what they perceive to be a time of crisis, seek (and not infrequently manage) to stampede Parliament into passing legislation that goes far beyond the exigencies of the moment. It takes enormous political courage to resist being swept along on tides of populist sentiment that, if succumbed to, will risk trampling on the very liberties that western democracies are seeking to protect.

What principles are to be offered by way of guidance when terrorism stalks and legislative (and other) change is proposed? David Feldman has suggested[19] a formulation that might be adopted when anti-terrorism measures are under scrutiny.

> There is an urgent need for everyone who has to determine the scope of anti-terrorism measures, their justification or the method of their implementation to bear in mind the need to uphold four principles if democratic values are to survive. *First*, there must be a clear necessity for any restrictive measures. *Secondly*, the restrictions must go no further than is required. *Thirdly*, the measures must be controlled by law. *Fourthly*, the law must be cast in such a way has to make sure that any interference with liberty is clearly and rationally related to the aim of protecting security.

Although it was not necessary for Professor Feldman's purposes to identify the origins of these principles, they have in fact been distilled from the jurisprudence

---

[16]The Bill was presented to Parliament on 12 November 2001, and received Royal Assent on 14 December 2001. Its operation has been reviewed by a Committee of Privy Counselors, chaired by the Rt. Hon Lord Newton of Braintree (18 December 2003). The Government reply is to be found as "Counter Terrorism Powers: Reconciling Security and Liberty in an Open Society (2004) Cm 6147.

[17]It is at least arguable that Parliament has thereby reinstated a version of the General Warrant/writ of assistance in a way that would have John Wilkes revolving at high speed in his grave. They are not identical, since "…they specify the suspects, but not the premises, and they permit multiple searches of those unspecified premises. They seem intended to permit fishing expeditions; they seem to risk encouraging harassment. Most ethnic Englishmen's homes will no doubt remain their castles, but rather fewer Muslim homes." *See* John Barrell, London Review of Books, 6 July 2006.

[18]*Ireland v. UK* (1978) 2 EHRR 25.

[19]"Human Rights, Terrorism and Risk: The Roles of Politicians and Judges" [2006] P.L. 364 at p. 371.

of the European Court of Human Rights. One significance of this point is that, if the principles are ignored by those who are responsible for devising and implementing anti-terrorism measures, it is altogether possible that they will fall foul of the judicial arm of government. But this will not always be so. There are (at least) two ways in which rapidly drafted and implemented legislation can have a greater impact than was ostensibly intended but will nevertheless remain immune from checks through the judicial process. In the first place, the law may have been drafted in such a way that its language (and therefore impact) is not confined to the control of terrorism. A good example of this phenomenon[20] is to be found in the Extradition Act 2003 that alters the law of extradition by dispensing with the requirement that the requesting state should demonstrate that a *prima facie* case exists against those whom it seeks to deport. At the time when this legislation was promoted, the point was made that this would be of great assistance in the fight against terrorism. In fact, the powers have been used in cases of fraud having nothing to do with terrorism,[21] and, so far as the USA is concerned, there is a lack of reciprocity in the arrangements, since the USA will not extradite its own citizens in the absence of the *prima facie* case.

Second, where the law on terrorism leads, Parliament will feel able to go further on later occasions.[22] In the Terrorism Act 2006, the power to hold suspects without charge has been extended from 14 days to 28 days, in spite of the arguments of opponents of the Bill that there was nothing that differentiated terrorist offences from others such as drugs running or people smuggling. How long will it be, one wonders, before those arguments are turned against those who used them and in favour of extending the law to other areas of criminality? Again, it may well be the

[20] Another example is to be found in the stop and search powers to be found in the Terrorism Act 2000, s. 44. This authorises the Metropolitan Police Commissioner to make an order identifying an area within which he may authorise officers to stop and search members of the public for articles that could be used in connection with terrorism. Unlike the ordinary powers, there need be no proof of reasonable grounds to suspect those who are stopped and searched. The order's existence must be confirmed by the Home Secretary and may last for no longer than 28 days. In fact, ever since the Act came in to force, the Commissioner has exercised the power in such a way that an order has been continuously in force. In *Gillan v Metropolitan Police Commissioner* [2005] EWCA Civ 1067, [2005] Q.B. 388, a court took the view that the continuous use of the orders was justified in the circumstances, but that on the facts the Commissioner had not succeeded in showing that the use of the power was lawful on this occasion.

[21] *R (on the application of Bermingham, Mulgrew and Derby v Director of the Serious Fraud Office* [2006] EWHC 200 (Admin), [2006] 3 All E.R. 239. The incident has caused considerable alarm in the business community, as evidenced by the full-page open letter to the Home Secretary in *The Daily Telegraph* of 5 July 2006, signed by many leading businessmen, in which the claim is made that the arrangements are "manifestly unfair" and that although this "was done with good intentions – to help the fight against terrorism," the outcome has been highly damaging to the national interest. No criticism is made of the courts for interpreting the legislation in such a way as to apply to non-terrorism cases.

[22] *See* Helena Kennedy, *Just Law* (2004), who gives as an illustration the fact that the right to silence was first curtailed (by permitting adverse inferences from silence) as a response to the emergency in Northern Ireland, before being introduced on to the mainland by the Criminal Justice and Public Order Act 1994, ss 34–38.

case that such legislation would not be vulnerable to judicial challenge on Human Rights Acts grounds. All the more important, then, that it is scrutinised with enormous care before it reaches the statute book with Professor Feldman's limiting principles in mind.

What Parliament has done through legislation probably represents the most visible and fundamental of the legal changes resulting from the body blow of 9/11. But any change is likely to produce other changes that are less predictable and less visible – once unleashed, the forces of change can act in a kaleidoscopic fashion that can produce at a shake a very different and unfamiliar picture. Conventions of the constitution can be placed under strain, and at a time when there is a reformist Government in power,[23] this places the whole constitutional structure under yet more pressure. At the very time when the legal system was coming to terms with fundamental changes such as those introduced by the Human Rights Act, the Government chose to make potentially fundamental changes in the relationships between the judiciary and the executive. Two Consultation Papers were issued. One[24] canvassed views about the abolition of the judicial role of the House of Lords and creating a new Supreme Court in its place. The second[25] canvassed view on the creation of a new Independent Judicial Appointments Commission. The government was plainly aware of the potentially destabilising effect of these proposals. In a Foreword to the first of them, Lord Falconer (the Lord Chancellor) said: "Separately and together they deal with issues of great constitutional importance because they focus on changes to the Judiciary's relationship with the Executive and the legislature." Both of these were ultimately brought about by the Constitutional Reform Act 2005. So far as the appointments of the judges is concerned, the Act (and the constitutionally curious "concordat"[26] which preceded it) in part supersedes a range of conventions (habits, practices, and understandings) surrounding judicial appointments and the preservation of judicial independence, with who knows at this stage what are consequences?[27]

15.1 Extended Powers of Pre-Trial Detention

Professor Feldman's principles were nowhere in sight at the outset of the discussions about the possibility of extending police powers of pre-trial detention, although they did inform the later treatment of the government's proposals. In early

[23] Lord Wilson, "The Robustness of Conventions in a Time of Modernisation and Change" [2004] Public Law 407.

[24] "Constitutional Reform: A Supreme Court for the United Kingdom" July 2003.

[25] Constitutional Reform: A New Way of Appointing Judges, July 2003. Replies to both papers were sought by 7 November 2003.

[26] *See* Lord Woolf, "The Rule of Law and a Change in the Constitution" [2004] 63 C.L.J. 317.

[27] The issue is explored further below.

drafts of what eventually became the Terrorism Act 2006, the government sought to extend the power to detain without charge persons suspected of being engaged in terrorism-related activities for up to 90 days. This would have been a huge extension from the 14 days which the law then permitted. In support of the case for an extension, the government relied on a police briefing paper which, in the words of Professor Feldman, "clearly had the character more of a piece of campaigning literature than an informative and balanced assessment of the available intelligence."[28] This sought to argue that the nature of the terror by which the nation was confronted was entirely different from anything encountered in the past.[29] In the relatively recent past, the government might have been able to persuade its followers using such meagre methods; but no longer. One of the ways in which the loss of confidence arising from the decision to go to war with Iraq has manifested itself is in the relative lack of trust now accorded to the present government, even by its own supporters. A very last minute compromise was achieved, extending the time available to the authorities from 14 days to 28 days. It might be thought that this represents a very real victory for Parliament in its oversight of the legislative process. But the fact is that by making a claim to require a new power that, in the absence of the threat of terrorism would have been absolutely unthinkable,[30] the government has managed to double the period of time for which a person might be detained without charge.

15.2 "Special Advocates" and SIAC

In the war on terrorism, a question arises concerning the role of the established courts in dealing with the problems that it generates. If any change were thought to be desirable, a precedent was to be found in the so-called "Diplock" courts, which were established in Northern Ireland at the height of the troubles there.[31] These were trials held by judges alone, without a jury, and they had extensive powers to receive evidence in secret. President Bush's attempts to outflank the established courts of the USA through the use of Military Tribunals have eventually been

[28] [2006] P.L. at p. 380.

[29] See the Report of the Home Affairs Committee, 2 July 2006.

[30] The technique is one frequently adopted by the current Government. On-the-spot fines for certain public order offences, for example, made their first appearance in the form of a suggestion by Mr Blair that the police might be given powers to march offenders up to the cash-point till to obtain money with which to pay for offences committed. Recently, the power to fine on-the-spot for offensive conduct under the Public Order Act 1986 resulted in a £80 fine being levied upon a person selling T-shirts bearing the legend "Bollocks to Blair." *See The Times*, 4 July.

[31] So called because they were introduced on the recommendation of a Report of a Commission chaired by Lord Diplock, Cmnd 5185) (1972). It was introduced by the Northern Ireland (Emergency Provisions Act 1973). *See* B. Dickson, "Northern Ireland's Emergency Legislation" [1992] P.L. 529.

prevented by the US Supreme Court.[32] No suggestion has been made in the UK that it should follow suit – the presumption has always been that those suspected of terrorist offences would be tried in the Crown Court.[33]

The Special Immigration Appeals Commission (SIAC) was established in 1997[34] to deal with an increasingly creaky immigration and asylum system, and attempts to permit procedural safeguards of the individual with the national security interests of the state. Its aspects undoubtedly do cause concern. This body hears appeals from decisions of the Home Secretary in immigration and asylum matters. The legislation provides that in certain circumstances, some of the ordinary rules of evidence and procedure have been displaced. Where, for security reasons, the Secretary of State decides that it would be unsafe to allow an appellant to see the evidence against him, the appellant may be represented by a "special advocate," a senior, security vetted barrister who acts on behalf of the appellant.[35] Once the evidence is given to the special advocate, he may no longer communicate with his "client" or his legal representatives, who remain therefore in ignorance of the full weight of the case against them. He is forced to rely instead on the integrity and resources of the tribunal itself to arrive at the proper conclusion. These are the sorts of compromises with principle into which the war on terrorism appears to have forced us.

15.3 The Role of the Judiciary[36]

Of altogether greater constitutional significance than anything thus far canvassed is the fact that the perceived need to protect national security through the use of exceptional legal measures has given rise to increasing possibilities for misunderstandings and mutual irritation between judges and politicians. This raises the question – what is the role of the judiciary when faced with laws that appear to infringe

[32] In *Hamdan v Rumsfield* (decided 29 June 2006).

[33] It may be noted that such courts have extensive powers to order that trials, and ancillary hearings should take place *in camera* where this may be necessary in the interests of national security and the avoidance of harm to the due administration of justice. Although provision is made for notice to be given in advance that a prosecutor intends to ask for an *in camera* order, and the press and other "persons aggrieved" have a right of appeal against such an order, rules of court stipulating that an application for leave to appeal and the appeal itself "shall" be heard in camera does not fall foul of the requirements of Article 6 of the Convention right to a "fair and public hearing." *See Re A* [2006] EWCA Crim 04, [2006] 2 All E.R. 1.

[34] By the Immigration Appeals Commission Act 1997. This was introduced as a result of the decision of the ECHR in *Chahal v UK* (1996) 23 E.H.R.R. 413, which had expressed doubts as to whether the non-statutory procedures of the non-statutory panel could be accounted "fair" for the purposes of Article 6 of the Convention.

[35] See *R v H and C* [2004] Crim. L.R. 861 (public interest immunity) (2005) 154 New Law Jo. 233; [2005] P.L. 195, (2005) 149 S.J. 842 (Parole Board).

[36] *See* R. Stevens, *The English Judges: Their Role in A Changing Constitution* (2002).

fundamental civil liberties? In an unwritten and flexible constitution such as that of the UK, that is not at all an easy question to answer. Lord Steyn pointed to the risk that "in troubled times there is a ever present danger of the seductive but misconceived judicial mindset that 'after all, we are on the same side as the government' … It is a slippery slope which tends to sap the will of judges to stand up to a government guilty of abuse of power."[37] In short, the independence of the judiciary, whose existence depends on a series of measures and conventions for its existence and protection, is put under real pressure by the advent of terrorism.

Before the enactment of the Human Rights Act 1998 (which came in to force in October 2000), the English courts were inclined to defer to the Executive, taking the view that accountability to Parliament rather than the courts was the more appropriate constitutional check, and that politicians rather than judges were likely to be best placed to assess the risks that terrorism presents. It may be said that the English courts have had a rather patchy record in protecting human rights when the Executive has waved the banner of "national security."[38] The constitutional relationship between the judges and the Executive from the start of the Blair government's term of office was not in any event particularly settled or clear, and certainly not cordial[39] (partly as a result of the government's unbelievably amateurish attempt to abolish the Office of Lord Chancellor).[40] The enactment of the Human Rights Act 1998 gave a clear signal that the courts were to act as the guardians of rights and civil liberties. The courts were given, for the first time, a power to declare that Acts of Parliament were incompatible with the European Convention.[41] This was bound to lead, sooner or later, to a conflict between the two branches. The constitutional convention of mutual respect between executive and judiciary for the territory and appropriate role of the other was to be sorely tested in relation to "detention orders," and then in relation to "control orders."

---

[37] Lord Steyn, "Deference: A Tangled Story" [2005] P.L. 346, at 359.

[38] *See* A.T.H. Smith, "Dicey and Civil Liberties: A Comment" [1985] P.L. 608; Lord Steyn, "Democracy, the Rule of Law and the Role of Judges" (2006) E.H.R.L.R. 243; *see also* D. Feldman "Human Rights, Terrorism and Risk: the Role of Politicians and Judges [2006] P.L. 364.

[39] Disputes have tended to arise in the context of judicial review of administrative action (in which Sir William Wade was the acknowledged founding father), and in connection with the exercise of sentencing powers in criminal cases. As to the former, *see* Lord Woolf, "Judicial Review – the Tension between the Executive and the Judiciary" (1998) 114 L.Q.R. 579. *See also* D. Bonner, "Human Rights; Criminal Law; Checking the Executive (2006) E.P.L. 45. Vera Baird Q.C., a Government Minister in the Department for Constitutional Affairs, was obliged to withdraw her criticism of a judge's exercise of his sentencing powers. *See* Frances Gibb, *The Times*, 27 June 2006.

[40] See the remarkable lecture of the then Chief Justice of England in which Lord Woolf describes the Lord Chancellor as "that engagingly friendly and cheerful chappie" (320), "The Rule of Law and a Change in the Constitution" [2004] 63 C.L.J. 317 and the events leading up to the Constitutional Reform Act 2005.

[41] Human Rights Act 1998, s. 4.

Matters came to a head in the case of *A v Secretary of State for the Home Department*.[42] Part IV of the Anti-Terrorism, Crime, and Security Act 2001 gave the Home Secretary the power to issue a certificate where he reasonably believes that a specified person's continued presence in the UK is a risk to national security and reasonably suspects that that person is a terrorist. He can then make a deportation order. But, if the person subject to the deportation order would face torture or inhuman treatment in the country to which he or she was about to be deported, it would be contrary to the European Convention to deport such a person.[43] The Act therefore provided that such a person could be detained indefinitely, without trial. An appeal process (habeas corpus not being available) was created that involved an appeal to SIAC. The Government had accepted that these measures were not compatible with Article 5 of the Convention, and it therefore decided to derogate from the Convention, Article 15 of which provides for derogation "in time of war or other emergencies." A number of persons were so detained, and it was their cases that formed the subject of the decision of the House of Lords in the case under discussion.

Although there was a challenge to the decision to derogate, the House of Lords refused to interfere with the decision of SIAC that there was indeed sufficient evidence of an emergency to permit the derogation. But the House held that the legislation violated Article 14 of the Convention, in that it discriminated against non-UK nationals. It also held that the Act was irrational in that it permitted the detention of foreign nationals who could not be deported, when it could not be said that they were the only source of threat to the nation's security. The number of individuals involved as being subject to these orders was not great. But this was an instance where the Government's attempt to deal with what it believed to be potentially dangerous people had been thwarted by the judiciary. There is wide scope here for disagreement about the true legal and constitutional significance of the decision. Lord Bingham in the course of his speech had defended the position of the courts by saying that "… the function of independent judge charged to interpret and apply the law is universally recognised as a cardinal feature of the modern democratic state, a cornerstone of the rule of law itself."[44] Dame Mary Arden has insisted that "The decision in the *A* case should not be misinterpreted as a transfer of power from the executive to the judiciary. The position is that the judiciary now has the important task of reviewing executive action against the benchmark of human rights. Thus, the transfer of power is not to the judiciary but to the individual."[45] But politicians, perhaps inevitably, thought otherwise. Mr Blair hinted that it might be necessary to re-think aspects of the Human Rights Act if it should prevent the government from affording its citizens adequate protection.

---

[42] (2004) UKHL 56, (2005) 2 A.C. 60. The case and its implications are discussed more fully by Dame Mary Arden, "Human Rights in the Age of Terrorism" [2005] 121 L.Q.R. 604.

[43] *Chahal v United Kingdom* (1996) 23 E.H.R.R. 413.

[44] At [42].

[45] [2005] 121 L.Q.R. at pp. 623–624.

The Government decided to deal with the setback by repealing the relevant sections of the 2001 Act, and replace them with "control orders" which it did in the Prevention of Terrorism Act 2005. The control orders, which permit the setting of conditions making the order a kind of house arrest, are of two kinds. If the order is of a kind that would violate article 5 of the Convention, there must be a derogating order in force and the control order can be made only by a court. If the control order is thought not to be in violation of Article 5, the Secretary of State can himself make the order, but only with the permission of the court. But even that regime has not found favour with the courts. In *Re MB*,[46] J. Sullivan came to the conclusion that the procedures provided for in the Prevention of Terrorism Act 2005 whereby the court merely reviews the lawfulness of the Secretary of State's decision to make a control order … are conspicuously unfair. "The thin veneer of legality that is sought to be applied by section 3 of the Act cannot disguise the reality. That controlees' rights under the Convention are being determined not by an independent court in compliance with Article 6.1 but by executive decision making, untrammelled by any prospect of effective judicial supervision [103]."

Shortly after this, the same judge decided[47] that a control order purporting to be non-derogating imposed such strict constraints that they offended the requirements of Article 5 and were therefore derogating orders and as such unlawful. The control orders were quashed, but that order was stayed pending an appeal by the Government.

This decision was not met with quite the same equanimity as the first decision had been. The Chairman of the House of Commons Home Affairs Committee, Mr John Denham, complained that the judges were threatening to provoke a "constitutional crisis."

There has always been an element of tension between the courts and the executive, the height of which varies from time to time.[48] Some regard such tension as indicative that the system is in a healthy state. But talk of "crisis" suggests that the judges are behaving in a way that is somehow constitutionally improper, and that they are somehow exceeding the judicial remit. Such assertions are not new either. Particularly in the area of judicial review of administrative action, claims have been made that judges are guilty of substituting their own views as to the wisdom of adopting a particular policy, which is more appropriately the province of the ministers. Judges defended themselves by the assertion that they were concerned with legality rather than policy – it being an inherent part of the constitutional settlement that it was for the courts to ensure that the administration was acting within the confines of the law. It is suggested that the same setting of the constitutional boundaries is at stake underneath the current constitutional arguments.

---

[46] [2006] EWHC 1000 (Admin).

[47] *Re JJ, KK, GG, HH, NN, LL.* (28 June 2006).

[48] *See*, for example, A. Le Sueur, "The Judicial Review Debate: From Partnership to Friction" (1996) 31 Government and Opposition 8.

When the system of judicial review of administrative action was in the process of maturing at the hands of the judges, Lord Diplock characterised its essentials as involving irrationality, illegality, and procedural impropriety, genuflecting at the same time in the direction of proportionality.[49] As with most overviews, this formulation abbreviated the issues at stake, and the constitutional status of judicial review that it described was a matter of considerable debate.[50] But it was a very useful formula around which to discuss the principles and practices that went to make up the institution of judicial review of administrative and executive action and to justify those practices as being part of the separation of powers and the rule of law.

The time has come for a similar formula to be distilled in the case of the interrelationship between human rights principles and the interests of security in the face of terrorism's threats. It will inevitably be more complex than that outlined by Lord Diplock. But its seeds are to be found, I suggest, in the principles articulated by Professor Feldman, who speaks for the need "… for the judiciary to re-conceptualise its position in the constitution."[51] It is not so much that terrorism has created a new need to arrive at this re-conceptulaisation. It is simply the arena in which the inevitable re-thinking that arose from the enactment of the Human Rights Act and the Constitutional Reform Act 2005 must now be played out.[52] The rule of law, its concomitant, and the independence of the judiciary are as important now as they have ever been. When the stakes are so high as they are for all concerned, it is important that we get it right.

[49] These were articulated in *Council of Civil Service Unions v Minister for the Civil* Service [1985] A.C. 374.

[50] *See* generally, Mark Elliott, *The Constitutional Foundations of Judicial Review* (2001). On judicial Independence, *see* R. Stevens, *The Indepencence of the Judiciary: The View From the Lord Chancellor's Office* (1997).

[51] [51] At p. 383.

[52] The Act makes reference to the importance of both the rule of law and the independence of the judiciary, but it is beyond the scope of this chapter to subject it to a detailed examination. Balancing Liberty and Security? A Legal Analysis of United Kingdom Anti-Terrorist Legislation.

References

Arden, D. M. (2005). Human Rights in the Age of Terrorism. *The Law Quarterly Review, Volume 121*, 604–627.

Bader Ginsberg, R. (2005). A Decent Respect to the Opinions of [Human] kind: The Value of a Comparative Perspective in Constitutional Adjudication. *The Cambridge Law Journal*, *64/3*, 575–592.

Barak, A. (2002). Foreword: A Judge on the Role of the Supreme Court in a Democracy. *Harvard Law Review*, *116/1*, 16–162.

Barak, A. in *Public Committee Against Torture v Israel*, 1999, H.C. 5100/94.53(4) P.D. 817, 845.

Barrell, J. (2006). Unwarranted–Review about 'John Wilkes: The Scandalous Father of Civil Liberty' by Arthur Cash. *London Review of Books*, *28/13*, 6 July.

Bingham, T. (2003). Personal Freedom and the Dilemma of Democracies. *International and Comparative Law Quarterly*, *52/4*, 841–858.

Blunkett, D., Secretary of State for the Home Department (2004). *Counter Terrorism Powers: Reconciling Security and Liberty in an Open Society.*http://www.homeoffice.gov.uk/documents/cons-count-terror-powers-310804?view = Binary

Bonner, D. (2006). Checking the Executive? Detention Without Trial, Control Orders, Due Process and Human Rights. *European Public Law*, *12/1*, 45–71.

Chakrabarti, S. and Gallagher, C. (2004). Nothing to Hide, Nothing to Fear. Counsel,Volume 5 (May 2004), 10–12.

Department for Constitutional Affairs (2003a). *Constitutional Reform: A Supreme Court for the United Kingdom*. http://www.dca.gov.uk/consult/supremecourt/supreme.pdf

Department for Constitutional Affairs (2003b). *Constitutional Reform: A New Way of Appointing Judges*. http://www.dca.gov.uk/consult/jacommission/judges.pdf

Dickson, B. (1992). Northern Ireland's Emergency Legislation. *Public Law, Issue 4 (Winter 1992)*, 592–624.

Dinton, Wilson (2004), The Robustness of Conventions in a Time of Modernisation and Change. *Public Law, Issue 2 (Summer 2004)*, 407–420.

Lord Diplock (1972). *Report to the Commission to Consider Legal Procedures to deal with Terrorist Activities in Northern Ireland*. Her Majesty's Stationery Office: London.

Elliott, M. (2001). *The Constitutional Foundations of Judicial Review*. Oxford: Hart Publishing.

Fiss, O. (2006). The War Against Terrorism and the Rule of Law. *Oxford Journal of Legal Studies*, *26/2*, 235–256.

Feldman, D. (2004). *English Public* Law. Oxford: Oxford University Press.

Feldman, D. (2006). Human Rights, Terrorism and Risk: the Role of Politicians and Judges. *Public Law, Issue 1 (August–November 2005)*, 364–384.

Gearty, C. A and Ewing, K. D. (2000). *The Struggle for Civil Liberties: Political Freedom and the Rule of Law in Britain, 1914–1945*. Oxford: Oxford University Press.

Gibb, F. and Charter, D. (2006). Cameron's Bill of Rights Leaves Lawyers Baffled–The Tory Leader Runs into a Little Legal Difficulty over His Plan to Copy the US. *The Times*. http://business.timesonline.co.uk/tol/business/law/public_law/article679810.ece

Lord Goldsmith (2005). Balancing Security and Fundamentals Rights – the EU Presidency View. *Speech of the Attorney General to the CBBE (Paris)*. http://www.attorneygeneral.gov.uk/attachments/19_11_05_speech_to_CCBE_sec_fund_rights.doc

Golove, D. (2005). United States: the Bush administration's "war on terrorism" in the Supreme Court. *International Journal of Constitutional Law*, *3/1*, 128–146.

Hansard, H. C., 2005, cc 325–328.

Hope, D. (2004). Torture. *International and Comparative Law Quarterly*, *53/4*, 807–832.

House of Commons: Home Affairs Committee (2006). *Terrorism Detention Powers. Fourth Report of Session*. Volume I.

Kennedy, H. (2004). *Just Law: The Changing Face of Justice–And Why It Matters To Us All*. London: Random House UK.

Khan, A. (2006). Identity Cards: The Final Nail in the Coffin of Civil Liberties?. *Journal of Criminal Law*, 70/2, 139–146.
Le Sueur, A. (1996). The Judicial Review Debate: From Partnership to Friction. *Government and Opposition: An International Journal of Comparative Politics*, *31/1*, 8–26.
Lowe, V. (2005). Clear and Present Danger: Responses to Terrorism. *International and Comparative Law Quarterly*, *54/1*, 185–196.
Nolten, S. (2005). Personal Injury Update. New Law Journal, Volume 155/No. 7175, 693–695.
Privy Counsellor Review Committee (2003). *Anti-terrorism, Crime and Security Act 2001 Review: Report*. London: The Stationary Office.
Rowe, J.J. (2001). The Terrorism Act 2000. *The Criminal Law Review, Issue 7 (July 2001)*, 27–542.
Sands, P. (2006). *Lawless World: America and the Making and Breaking of Global Rules*. London: Penguin.
Smith, A.T.H. (2006). Disavowing Torture in the House of Lords. *The Cambridge Law Journal*, *65/2*, 252–254.
Smith, A.T.H. (1985). Dicey and Civil Liberties: A Comment. *Public Law, Issue 4 (Winter 1985)*, 608–611.
Lord Steyn (2005). Deference: A Tangled Story. *Public Law, Issue 2 (Summer 2005)*, 246–359.
Lord Steyn (2006). Democracy, the Rule of Law and the Role of Judges. *European Human Rights Law Review*, *11/3*, 243–253.
Stevens, R. (1997). *The Independence of the Judiciary: The View from the Lord Chancellor's Office*. Oxford: Clarendon.
Stevens, R. (2002). *The English Judges: Their Role in a Changing Constitution*. Oxford et al.: Hart.
Lord Woolf, H. (1998). Judicial Review – the Tension Between the Executive and the Judiciary. *The Law Quarterly Review, Volume 114*, 579–593.
Lord Woolf, H. (2004). The Rule of Law and a Change in the Constitution. *The Cambridge Law Review*, *63/2*, 317–330.

Chapter 16
Limiting Fundamental Rights in the Fight Against Terrorism in Spain[1]

Víctor Moreno Catena and Mariangeles Catalina Benavente

16.1 Introduction

In this study, we wish to offer the reader a general analysis of the main anti-terrorist procedural measures that have been introduced in Spain since the passing of the 1978 Constitution, an event that marked the end, finally, of the era of the dictatorship in Spain, establishing in its place a social, democratic Rule of Law (sect. 1 CE).[2] We will also examine the impact of these measures on fundamental rights, and offer some reflections in that regard.[3]

When it comes to creating anti-terrorism policy, the State must keep in mind the democratic principles imposed on it by the terms of its Constitution and act in accordance with its position as a country governed by the fundamental principles of the social and democratic Rule of Law, designed to make it a model of freedom and respect for human rights. First and foremost, therefore, any measure introduced in the fight against terrorism should respect the democratic principles of freedom, which must be maintained at all times, even in the face of terrorism (Moreno Catena 2006; Mestre Delgado 1987).

V. Moreno (✉) and M. Catalina
Alonso Martinez University Institute for Justice and Litigation,
Carlos III University, Madrid, Spain
e-mail: victor.moreno@uc3m.es, angeles.catalina@uc3m.es

[1] This chapter is part of a research Project, "Limitations of freedom in the terrorism procedure", financed by the spanish Science Ministry, Ref: DER 2008–06178

[2] CE is the abbreviation used to refer to the Spanish Constitution (*Constitución Española*).

[3] The fundamental rights of citizens are contained in sections 14–29 of the 1978 Constitution, including, among others: the right to life and to physical integrity, with the express prohibition of torture or inhuman or degrading punishment or treatment (sect. 15); the right to freedom (sect. 17); the right to honour, to privacy, to the inviolability of the home and secrecy of communications (sect. 18); the right to effective protection from the judges (sect. 24.1); the right to the ordinary judge predetermined by law, to defence and the assistance by a lawyer, to be informed of the charges brought against them, to a public trial without undue delays and with full guarantees, to the use of evidence appropriate to their defence, not to make self-incriminating statements, not to plead guilty and to be presumed innocent (sect. 24.2); and the right to penitentiary legality (sect. 25).

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_16, © Springer Science+Business Media, LLC 2010

The criminal justice system should be the keystone of a public safety policy capable of combating a terrorist phenomenon whose aim is to bring down the legitimate structures of power and peaceful coexistence.[4] The criminal justice system establishes the Judiciary as the body responsible for administering the only authorised system of sanctions against individuals according to the criminal act they have committed. As the final link in the public safety policy chain, the criminal process must be designed with the utmost care and attention, in order to guarantee maximum control over criminal conduct without detriment to individual rights and freedoms. The attempt to make the fight against crime and, in this instance, terrorism, more effective can never become an excuse for the diminution of individual rights and guarantees that have taken decades of hard work to achieve.

16.2 Section 55.2 of the Spanish Constitution

Section 55 CE (from Chapter V, section-heading I: "Suspension of rights and liberties") states that: "An organic act may determine the manner and the circumstances in which, on an individual basis and with the necessary participation of the courts and proper parliamentary control, the rights recognised in sect. 17, subsection 2 and section 18, subsections 2 and 3 may be suspended for specific persons in connection with investigations of the activities of armed bands or terrorist groups". The rights referred to here are: the right for preventive arrest to last "no longer than the time strictly necessary in order to carry out the investigations aimed at establishing the events; in any case, the person arrested must be set free or handed over to the judicial authorities within a maximum period of seventy-two hours" (sect. 17.2); the right to the inviolability of the home (sect. 18.2), and the right to secrecy of communications (sect. 18.3). Outside of these cases, no exception from the protection of all other fundamental rights is permitted, not even for the investigation and prosecution of terrorist crimes (Moreno Catena 2006; Bartolomé Cenzano 2003; Pérez Tremps 2000; Remotti Carbonell 1999).

Section 55.2 is an attempt, on the one hand, to facilitate the investigation of terrorist activity but, on the other hand, to limit the powers of law and government in order to avoid any unacceptable violation of fundamental rights (Remotti Carbonell 1999). To understand this last statement properly, it should be recalled that, within the Spanish legal system, the limitation of fundamental rights is surrounded by the maximum possible guarantees, hence for any interference in this area to be considered legitimate, five a posteriori "requirements" must be fulfilled (Moreno Catena 2006): (1) firstly, the restriction must be authorised by an organic act, which is a law whose passing, modification, or repeal requires an absolute majority in the Chamber of Deputies in a final vote on the bill in its entirety (sect. 81.2 CE).

[4] This has been the experience in Spain where, for longer than 40 years, the people of the country have been forced to live under the shadow of terrorism, at a cost of nearly 1,300 lives, including those claimed by the attacks in Madrid on 11 March 2004 (Pulgar Gutiérrez, 2004; http://www.mir.es).

Moreover, in addition to the requirement that any limitation of a fundamental right must be stated in an organic act, this condition also demands that a separate organic act should be created for each specific use of the suspension powers contemplated by sect. 55.2 CE; (2) the organic act should determine the *manner* and *circumstances* in which the limitation of a fundamental right will be considered legitimate; (3) the restriction of fundamental rights may only be applied on an *individual basis* and *for specific persons*; the suspension of constitutional guarantees in relation to the three fundamental rights contemplated in sect. 55.2 should not, therefore, be taken as a general order of exception against all persons implicated directly or indirectly in an investigation concerning terrorist activities; (4) interference with the fundamental rights of an individual requires the participation of the judiciary. This does not mean that the judge's authorisation must always precede the interfering action; however, whether before or after, a judicial order or confirmation of the action must be issued in the form of a resolution outlining grounds sufficient and necessary to comply with the conditions demanded by the Constitution; (5) lastly, the Constitution requires *parliamentary control* of these measures.[5]

The limitation of fundamental rights is still an exceptional measure, however. In other words, it is confined to cases in which there is reasonable evidence of the existence of certain exceptional circumstances that make the introduction of such a limitation absolutely necessary (Remotti Carbonell 1999). The limitation of fundamental rights provided for in sect. 55.2 CE is not implemented automatically in all cases of terrorism, but on an individual basis and where there are sufficient grounds.

Whether or not the limitation of fundamental rights in the context of the criminal process is legitimate depends on whether or not the procedures envisaged by the Constitution are implemented properly. What is involved here, basically, is the two sides of a single reality, so that when those two sides come into conflict, it becomes necessary to weigh the protected interests of one against those of the other: on the one side, the preservation of the fundamental rights of the person; on the other, the defence of society that calls for criminal actions to be met with their appropriate punishment (STC[6] 199/1987 and STC 25/1981).

Today, the restrictions envisaged under sect. 55.2 CE are regulated by the Code of Criminal Procedure (*Ley de Enjuiciamiento Criminal* [*LECrim*]), according to the reforms introduced to it by organic act 4/1988 (25 May). Before moving on to analyse in more detail the current legislation governing the limitation of fundamental rights in cases of terrorism, we should point out that between the

[5]Parliamentary control is not defined by an organic law and is not provided for specifically in the Codes of either the Chamber of Deputies or the Senate. It has become accepted practice among the two Houses that the requirement of parliamentary control is fulfilled by the appearances of the Minister of the Home Office in the Chamber to report to the parliamentary groups regarding the progress of the fight against terrorism; as yet, no parliamentary initiative has emerged to demand any alternative form of control.

[6]STC is the abbreviation used to refer to sentence of the Constitutional Court (*Sentencia del Tribunal Constitucional*).

passing of the Constitution in 1978 and the introduction of LO[7] 4/1988, there was already specific legislation in existence in Spain for dealing with the problem of terrorism: LO 11/1980 (1 December), concerning the exceptions envisaged by sect. 55.2 CE; and LO 9/1984 (26 December), concerning the activities of armed bands and terrorist groups and the implementation of sect. 55.2 of the Constitution.[8]

LO 11/1980 was a very short act, comprising only eight sections, and the regulations contained in it regarding the limitation of fundamental rights were not very detailed (Vercher Noguera 1991; Fernández Segado 1983; Miguel Zaragoza 1981). The only additional provision it contained stressed the importance of processing terrorist cases as a matter of urgency, and stated that in such cases a special indictment procedure lasting no more than 60 days should be inserted in the Code of Criminal Procedure. No such procedure was ever established. Preventive arrest by government order was allowed for a maximum period of 10 days, with the option of ordering that the subject be detained in isolation for that period (sect. 3). The Security Forces and Services of the State were permitted to enter and search the home or location of individuals suspected of terrorist activities without the prior authorisation of a judge (sect. 4). Similarly, in an emergency situation, the Minister of the Home Office or, in his/her absence, the Director General of State Security could sanction the intervention of communications of persons suspected of membership of or connection with armed bands or terrorist groups (sect. 5). LO 11/1980 was the object of an appeal brought against it by the Basque Regional Parliament, but the appeal was rejected by the Constitutional Court under ruling 25/1981[9]

LO 9/1984 was, in contrast, a much more detailed and far-reaching act than the one it had just replaced (Vercher Noguera 1991; López Garrido 1987; Mestre Delgado 1987; Lamarca Pérez 1985). The new legislation contained 25 sections but it was not confined to the limitation of fundamental rights, as its predecessor had been; instead, what it provided was a more complete set of regulations dealing specifically with terrorism. As regards procedure, the new act moved away from the attempt by the 1980 legislator to create a "special indictment procedure", preferring instead the ordinary procedural norms provided for under the Code of Criminal Procedure (sect. 12.1). It retained, however, the earlier act's provision regarding the processing of certain cases as a matter of priority, establishing a 90-day period as the maximum time allowed between a subject's committal for trial and his/her appearance before the trial judge (sect. 23). On the whole, there were few substantial differences between the two acts in terms of the way they regulated the limitation of fundamental rights envisaged by sect. 55.2 CE. For instance, preventive arrest by order of the government was still allowed for up to 10 days, provided the measure received the

[7]LO is the abbreviation used to refer to the organic act (*Ley Orgánica*).

[8]LO 9/1984 replaced LO 11/1980, and was in turn replaced by LO 3/1988 (25 May).

[9]The Basque Regional Parliament appealed its constitutionality on the grounds that LO 11/1980 impinged on the autonomy of the Basque Country, because the suspension of rights provided for under the act would apply primarily to citizens residing in that autonomous community. In its rejection of the appeal, the Constitutional Court alleged, among other reasons, that LO 11/1980 "does not relate to any particular part of the country, but applies to the State as a whole". It also added that fundamental rights "are not affected by the federal, regional or autonomous community structure of the State", but rather "belong to all citizens, individually and collectively".

required authorisation of the courts (sect. 13); unlike LO 11/1980, though, the 1984 act demanded that incommunicado detention should be confirmed by the appropriate jurisdictional bodies (sect. 16.2). The provisions regulating search and entry were identical to those contained in LO 11/1980; regarding the intervention of postal, telegraphic, and telephonic communications, however, there was a change to the earlier text where in sect. 17 it now referred to communications as "possible evidence of criminal responsibility", and not "suspicious", as sect. 5 LO 11/1980 had stated. Aside from this point, though, the other provisions concerning the intervention of communications were identical to those of 1980. The 1984 act was the object of two constitutional challenges, brought against it by the Regional Parliaments of the Basque Country and Catalonia. The Constitutional Court ruled that certain elements of the act were unconstitutional, but not the act itself (STC 199/1987).

Finally, then, the following regulations were introduced into the Code of Criminal Procedure by LO 4/1988: sect. 520 bis, providing for the extension of preventive arrest by 48 h in cases of terrorism; sect. 553, providing for entry and search of any location used to hide or take refuge in, when the individuals suspected of the crime being investigated are terrorists, rebels, members of an armed band, or in some way connected with an armed band; and, lastly, sect. 579.4, according to which the Minister of the Home Office or, in his/her absence, the Director of State Security may order the monitoring of postal, telegraphic, or telephonic communications where the subject is suspected of involvement in terrorist crimes, provided immediate notification is submitted in writing to the proper court authority, who must within a maximum period of 72 h rule either to revoke or to confirm the measure. This is how the interpretation of sect. 55.2 CE stands at present. The fact that the limitation of fundamental rights in cases of terrorism has been incorporated into the Code of Criminal Procedure has led certain authors to cast doubt on the exceptional nature of the measure in such instances (Terradillos Basoco 1988).

Our analysis of the theme will be organised as follows: firstly, we will analyse the sections in the Code of Criminal Procedure referred to above in order to highlight what, in our view, are the main flaws in the current interpretation of the law. Once we have examined the three fundamental rights in question, we will focus our attention on the right to defence and the right to the ordinary judge predetermined by law (sect. 24.2 CE), as the restriction of these rights in the context of the fight against terrorism has been a cause of some concern among legal theorists and members of the Constitutional Court itself. Finally, we will look at the right to be presumed innocent (sect. 24.2 CE), a right that can prove the ultimate guarantee for an alleged terrorist whose conviction will be based on whether or not the evidence against him/her has been obtained without prejudice to his/her fundamental rights.

16.3 The Fundamental Right to Freedom

The Spanish Constitution establishes the right to freedom as one of the essential values of the Rule of Law (sect. 1.1) and as a fundamental right: "Every person has the right to freedom and security. No-one may be deprived of his or her freedom

except in accordance with the provisions of this section and in the cases and the manner provided for by the law" (sect. 17.1).

16.3.1 Extending the Time Limit for Preventive Arrest

According to sect. 17.2 CE, preventive arrest should last no longer than is strictly necessary to allow the police to carry out the investigations aimed at establishing the events surrounding the crime (first time limit), and must not, in any case, continue for any longer than 72 h (second limit). Before these limits expire, the detainee must be set free or handed over to the judicial authorities.

This fundamental right may be only suspended if the case under investigation relates to terrorism (García Morillo 2000). Section 520 bis 1 LECrim, for example, provides for the extension of the period of detention by the police by 48 h. This means that a person detained in the context of investigations relating to terrorist crimes may be deprived of his/her freedom on this basis for up to 5 days in total. When it came to establishing the maximum period of preventive attest in cases of terrorism, the legislator had to follow the example set by the Constitutional Court decision (STC 199/1987) regarding the unconstitutionality of sect. 13 LO 9/1984, which allowed, in cases of terrorism, for police detention to last for up to 10 days (in other words, that the 3 days permitted under the Constitution could be extended by a further 7 days).[10] The Constitutional Court's ruling on this matter stated that the extension of the period of detention to 10 days signified "extra hardship and unjustified additional moral coercion against the detainee, that are not compatible with his or her rights not to make self-incriminating statements and not to plead guilty". Basing its judgement on sect. 9.3 International Covenant on Civil and Political Rights and 5.3 European Convention of Human Rights, the Constitutional Court rejected that the legislator was at liberty to establish such a long period of preventive detention, and so pronounced a ruling of unconstitutionality against sect. 13 LO 9/1984.[11]

[10]The detention period allowed under the 1984 act was the same as that provided for under sect. 3.1 LO 11/1980. The fact that the detention period was so long suggests that what the legislator may have been hoping to achieve was to obtain from the detainee, before bringing him/her before the judge, certain disclosures or a self-incriminating statement which he/she would otherwise probably not have made (Moreno Catena, 1987).

[11]Another of the arguments cited by the Constitutional Court was that no country with a similar system of law to Spain's has established such a long period of preventive arrest in cases of terrorism. While the number of victims claimed by terrorist attacks should not influence the decisions of the legislator when formulating legislative policy, and legislation should not be created "in the heat of the moment" (because this usually gives rise to much more restrictive measures than would be preferable), there is no escaping the fact that between 1980 and 1984, terrorism in Spain claimed 223 victims (Pulgar Gutiérrez 2004). At the end of the day, however, the Constitutional Court is always there to keep the legislator from committing any excesses.

The important point is that the extension of the detention period by 48 h is not something that can be introduced automatically or implemented across the board in all cases of terrorism; it may only be introduced on an individual and exceptional basis (the same as any measure that implies the limitation of a fundamental right). What this means, therefore, is that the extension of the time limit is only allowed when, owing to exceptional circumstances, the police are unable to complete their inquiries and investigations concerning the person in custody within the first 72 h. The individualisation of the exception also means that the police have to demonstrate the existence of reasonable evidence linking the person under investigation with participation of some description (perpetrator, accomplice, instigator, collaborator, etc.) in specific terrorist acts.

The extension of the time limit by 48 h is, moreover, subject to judicial controls because, according to sect. 520 bis 1 LECrim, the police are required to apply to a judge within the first 48 h of detention for the 48-h extension permitted by the law in cases of terrorism. The judge's decision regarding that application must be reached within a further 24 h. If, after the first 72 h of detention, the police have not received the judge's authorisation to extend the period of detention by a further 48 h, the alleged terrorist must be handed over to the judicial authorities. The police have to receive judicial authorisation before the first 72 h expire in order to extend the detention.

16.3.2 Incommunicado (Isolation) Detention

Another distinctive aspect of preventive arrest in cases of terrorism is the option to order the isolation of the subject for the duration of his/her detention (sect. 520 bis 2 LECrim, in reference to sect. 384 bis LECrim). In the event of such an order being issued, and until such time as it is lifted again, the person may only be assisted by a court-appointed lawyer, whom he/she will not be entitled to meet confidentially after the order has been lifted. In addition, the subject is not permitted to inform a family member or whomever he/she may wish to inform of the fact of his/her detention or regarding the location in which he/she is being held (sect. 527 LECrim).[12]

Sections 520–526 LECrim, and sect. 520,[13] in particular, explain the rights of detainees in greater detail. Firstly, sect. 520.1 paragraph 1 states that the detention "must be carried out in such a way as to minimise the damage to the subject's personal reputation and property".[14] The purpose of this provision is to guard against the use of unnecessary force, thus making it illegal to employ coercive measures

[12] Introduced under LO 14/1983 (12 Dec).

[13] Introduced under LO 14/1983 (12 Dec).

[14] In this regard, sect. 3 of the State Security Forces and Services Act states that the security forces of the State "will ensure the life and physical integrity of persons detained by them or in their custody, and will respect the honour and dignity of all people".

against the person being detained if he/she offers no physical resistance (Moreno Catena 2008). However, the act of detention is, of itself, clearly a violent act; therefore, in most cases, the police authorities are likely to find some use of force necessary in order to effect an arrest of this kind.

Section 17.3 CE establishes as a fundamental right the right of every person arrested "to be informed immediately, and in a way understandable to him/her, of his/her rights and of the grounds for his/her arrest, and may not be compelled to make a statement" (too sect. 520.2 LECrim). These entitlements may not under be restricted any circumstances, not even in the context of investigations relating to terrorism. It represents a solid guarantee to all detainees and an example to other countries whose antiterrorist measures permit, not only the extension to scandalous limits of the maximum legal period of detention, but also the refusal to inform detainees of the reasons for their detention (García Morillo 2000).

The other rights guaranteed by the Code of Criminal Procedure in all detention cases are: (1) the right to remain silent and not to make a statement if he/she does not wish to do so; not to answer any or all of the questions he/she may be asked; and to declare that he/she will only make a statement before a judge (sect. 520.2.a). (2) The right not to make self-incriminating statements or to plead guilty (sect. 520.2.b). (3) The right to appoint a lawyer of his/her choice and the right to have that lawyer present throughout all police and judicial proceedings, and to have him/her present during all identification procedures the detainee may be required to undergo. If he/she does not appoint a lawyer for him/herself, counsel will be appointed for him/her by the court (sect. 520.2.c). (4) The right to inform a family member or whomever he/she may wish to inform of the fact of his/her detention and his/her custodial location at all times. If the person being held is a foreign national, he/she is entitled to inform the Consular Office of his/her country of the situation (sect. 520.2.d). (5) The right to be assisted for free by an interpreter (sect. 520.2.e), applicable also to Spanish citizens who do not understand or speak Castilian Spanish (STC 74/1987). (6) The right to be examined by a medical doctor (sect. 520.2.f).

Returning once more to the limitation of the rights of the detainee under sect. 527 LECrim, it is hard to argue with the assessment of the removal of the subject's right to appoint a lawyer of his/her choice during the period of incommunicado detention as clearly the most serious limitation of a fundamental right (that of defence – sect. 24.2 CE) entailed by the prohibition of contact order. According to Gómez Colomer (1988), the limitation of the right to defence is one of the State's "essential weapons in the fight against terrorism"; more will be said about that statement later on. For now, we are going to focus on the procedure followed in cases of incommunicado detention and the objectives such a measure is intended to achieve. The question is as controversial as it is interesting.

The decision to detain a subject in isolation must be confirmed by a judge's order (in the form of a resolution, accompanied by a statement of grounds) within 24 h of his/her receiving the police's application (sect. 520 bis 2). As soon as the police request the judge's order to sanction the isolation of the detainee, from the moment the request is made to the moment the judge makes his ruling, the subject

is considered officially incommunicado. For the 24 h during which the judge must reach a judgement, the police have the obligation to guarantee the detainee's constitutional and legal rights and, in view of his/her situation of isolation, must follow all the necessary procedures to guarantee that court-appointed counsel is present throughout all police proceedings. A prohibition of contact order may be requested at any time during the period of detention, although the most common course of action is for the application to be made soon after the initial detention, at the same time as the request for the judge's order to extend the detention period.

The principal conditions a prohibition of contact order must meet in order to satisfy the Constitutional Court are as follows (Catalina Benavente 2007): (1) the order should reveal the purpose served by holding a subject in isolation (ATC[15] 155/1999); (2) it should explain why, for that purpose to be met, the prohibition of contact is necessary in the specific case in question (STC 127/2000); (3) it should provide evidence to demonstrate the connection between the person being held incommunicado and the crime under investigation (STC 169/1999); and (4) the judge's resolution may also make reference to the arguments presented by the police authorities in their original request for a judicial order (STC 7/2004).

The question of how long incommunicado detention is permitted to last is dealt with in sect. 509 LECrim.[16] According to the provisions of this section, concerning the isolation of both detainees and prisoners, the first time limit should observe the "time strictly necessary to allow urgent proceedings to take place with a view to avoiding the dangers stated in the previous section"; in any case, though, the prohibition of contact "may not be extended beyond five days". These are the only parts of 509 LECrim that are relevant to our analysis of preventive incommunicado detention; the rest of the section relates exclusively to the isolation of prisoners on provisional imprisonment.[17]

One final aspect of this issue to which we wish to devote some attention is the question of the purpose incommunicado detention is intended to serve; the only way to make some sense of the measure is in terms of the objectives it is designed to achieve. According to the terms of sect. 509.1 LECrim, the fundamental objectives sought by incommunicado detention are three: (1) to prevent individuals suspected of involvement in the events under investigation from escaping; (2) to prevent those

[15] ATC is the abbreviation used to refer to the decision of the Constitutional Court (*Auto del Tribunal Constitucional*).

[16] Introduced under the LO 13/2003 (24 Oct) reform of the Code of Criminal Procedure in regard to preventive imprisonment and later modified by LO 15/2003 (25 Nov), necessitating the additional modification of LO 10/1995 of the Code of Criminal Procedure.

[17] This section contains provision for the extension of the deprivation of contact order by a further maximum period of 5 days in cases in which the arrest is made on the basis of one of the crimes contemplated in sect. 384 bis LECrim. Once the prisoner has been taken out of isolation, a second period of incommunicado detention may be declared, lasting no more than 3 days. According to these provisions, therefore, a person accused of one of the crimes contemplated in sect. 384 bis may ultimately find him/herself being isolated for up to 13 days: the potential deprivation of contact during the initial detention (5 days), the extension of that order once the detainee has been remanded (5 days), and its re-ordering after the expiry of that extension (3 days).

individuals from harming the legal interest protected of the victim, or from hiding, altering, or destroying evidence relating to such an action; (3) to prevent the commission of further criminal acts.

The aims sought by the isolation of detainees can only be understood in reference to the rulings made on this matter by both the Constitutional Court and the Supreme Court. The Constitutional Court has stated that incommunicado detention is an "exceptional short-term measure aimed at isolating the subject from contact of a personal nature which could be used to transfer information pertaining to the investigation and thereby jeopardise that operation" (STC 196/1987).[18] The aim of the measure is, therefore, to maintain peace in society and the safety of its citizens (sects. 10.1 and 104.1 CE). In 1997, the Constitutional Court found once again that the legislator's objective in providing for the isolation of detainees was to avoid putting an investigation at risk by allowing details of its progress to become known to persons other than those involved directly (STC 200/1997).

The Supreme Court, on the other hand, appears to have a slightly different take on the issue. Its judgement of 8 October 2001, for example, ruled that incommunicado detention is an exceptional measure that may be adopted "to isolate certain suspects in order to gain as clear a picture as possible of the events in which they are alleged to be involved". In the same way, in its ruling of 3 October 1998, the Supreme Court referred to the need for incommunicado detention as a way of "guaranteeing the efficiency of the investigation". We do not believe that the isolation of detainees should be used to facilitate the establishing of the facts of a case against a particular individual, but rather that it should be used to guarantee the greatest possible efficiency of a police investigation, which at any given moment may be operating on several different fronts and hence require a level of coordination on the part of the police that could be placed in serious jeopardy by the leaking of information of any kind. With that in mind, and bearing in mind, also, the need to avoid a detainee's using the rights guaranteed to him/her by law (assistance of a lawyer and contact with a person of trust) to "warn" other implicated parties (the crimes in question have, after all, been committed under the auspices of a terrorist organisation), what incommunicado detention allows is for the police to operate for a short time with a certain "advantage" – something the Rule of Law needs sometimes in order to deal with terrorist activities. Neither the isolation of detainees nor the extension of the detention period by 48 h, therefore, will be necessary in all instances, both measures depending on the individual case. The legislation attempts for a short time to assist the operations of the police by putting off for as long as possible the moment when other individuals implicated in the investigation are apprised of their colleagues' situation. Nevertheless, even granting that the objective being pursued involves placing social peace and citizen safety on one side of the scales, and the fundamental rights of detainees on the other, with a definite bias towards the former, it does not justify the use of all possible means to achieve it.

[18]It also states: "The Constitution does not prevent the State from protecting constitutionally recognised legal entitlements at the cost of other equally recognised entitlements, whether in relation to fundamental rights or to other constitutionally protected values and entitlements".

To conclude this analysis of incommunicado detention, we would like to highlight one of the most polemical aspects of this form of detention, which is the way it encourages, or can lead to, the practice of police torture (Human Rights Watch 2005). The Rule of Law does offer safeguards to protect against such a situation, however: principally, the training received by the Security Forces and Services of the State and, where that security fails, the definition within the Criminal Justice Code of what constitutes illegal detention so that any excesses on the part of the police authorities receive their proper punishment as required by law.

Before we end this section, we would like to make some brief comments on two of the rights available to detainees: the right to be assisted by an interpreter (sect. 520.2.e LECrim), and the right to be examined by a medical doctor (sect. 520.2.f LECrim). The involvement of the interpreter during the making of statements to the police is necessary in all cases in which the person being held claims not to know the Spanish language, even if that person is a Spanish national (STC 74/1987). However, the right applies only to those who claim not to know Spanish, not to detainees who know Spanish but prefer not to use it, whether with the intention of obstructing their interrogation by the police or the court, or of delaying the process as a whole (Rebato Peño 2006). The right to be examined by a medical doctor, then, is to do with ensuring the physical and mental integrity of the person being held. As soon as the subject has been taken into police custody, before he/she is placed in a cell, the doctor appointed should conduct the necessary medical examination and issue the appropriate medical certificate. The medical check will be repeated before the detainee is released from custody or before he/she is handed over to the judicial authorities. In the case of investigations relating to terrorism, and especially in cases of incommunicado detention, the doctor's presence is obligatory. To understand why, one need only look at some of the judgements of both the National Criminal Court and Court Number II of the Supreme Court, which show that allegations of torture and abuse during detention are not uncommon.

16.4 The Right to the Inviolability of the Home

The second of the rights mentioned in sect. 55.2 CE, in reference to the possibility of its being suspended in the case of investigations into terrorism, is the right to the inviolability of the home. According to the provisions of sect. 18.2 CE: "The home is inviolable. No entry or search may be made without the consent of the householder or a legal warrant, except in cases of *flagrante delicto*". As the Constitutional Court has shown, the right to the inviolability of the home is relative and limited, and the restrictions on it are envisaged within the Constitution itself. However, the suspension of the right to the inviolability of the home on an individual basis, provided for under sect. 55.2 CE, raises the problem of how to make the efficiency of the suspension compatible with the involvement of the courts. Section 55.2 only authorises the legislator to moderate judicial involvement in the action of entering and searching the home, but not to eliminate it completely in the interest of making the suspension process more efficient (STC 199/1987).

Sections 545–578 LECrim establish the procedures that must be observed in an entry and search operation. In cases in which the householder has not granted his/her consent and *flagrante delicto* is likewise absent, the police need a judicial order in the form of a resolution ordering them to enter and search. The resolution should include precise information regarding the following points (Moreno Catena 2005): (1) the location of the action; (2) the person or thing being sought; and (3) evidence that the accused is present at the stated location, or that the scene contains instruments and effects relating to the crime, or books, papers, or other objects that may help to uncover or corroborate its existence. The procedure for entry and search is, moreover, subject to the following conditions: (1) the operation may only be ordered as part of an open criminal process; (2) the court secretary, the party implicated or his/her legal representative, a family member of the implicated party, or two witnesses must be present (sect. 569). If the witnesses refuse to take part, the search will be carried out without them and they may be held criminally responsible for their attitude (sect. 556 Penal Code).

In investigations into the activities of terrorist groups, the limitation of sect. 18.2 CE may take place without the prior obtaining of a court order. For this to happen, the situation should be one of urgency; in other words, that if the entry and search measure were not allowed to proceed there and then, its whole object would be defeated since the person in question would have time to escape or to destroy or hide evidence (Remotti Carbonell 1999). Section 553 LECrim authorises entry and search when the person being pursued is a member of or related to an armed band or terrorist or rebel group, "whatever the location or home in which they have hidden or taken refuge". Although the prior authorisation of the judge is not needed in these cases, the Code of Criminal Procedure does require police officers to "inform the competent judge immediately, including in the report an outline of why the measure was adopted and what results were obtained, with specific reference to any detentions made in the course of the operation. In addition, the police report should account for all the people involved in the operation and any incidents which may have occurred" (sect. 553 II).

An emergency entry and search, carried out without a judicial order and in violation, in many cases, of other conditions demanded by law, may produce incriminating evidence against the accused. A measure of this kind should, therefore, use all means possible to ensure that, under the pretext of combating terrorism, the police are not given unlimited powers to enter and search a location without the necessary judicial authorisation. It is, for the same reason, also vital that the police authorities be obliged to submit a report in these cases, after the entry and search operation, explaining their reasons for adopting such a measure. The reasons cited in the report will be used by the judge to determine whether the limitation of sect. 18.2 CE in each case is justified or not according to the Code of Criminal Procedure and, consequently, whether the results of the entry and search may be included in the body of evidence against the accused. In other words, in cases of terrorism, the authorisation of the judge is not required before the entry and search takes place, but it must be obtained a posteriori in order to confirm the validity of the operation.

In any case, though, the law in regard to this measure needs to be made more precise. The legislator should establish a more detailed procedure for entering a home without the authorisation of a judge and for the subsequent searching of the premises, likewise in the absence of a court order. In view of the fact that the operation is one which takes place over an extended period of time, lasting several hours in some cases, the proper course of action would be for the police authorities to request the judge's authorisation to proceed with a search as soon as emergency entry has been made, in order to guarantee the future validity of all evidence found in the home or at the scene in question. As Remotti Carbonell (1999) points out, emergency entry should be communicated to the judge immediately, thus ensuring that the search can be controlled and if necessary suspended if, in the judge's opinion, the required conditions for the operation have not been met.

16.5 The Right to Secrecy of Communications

The third and final right whose possible suspension is authorised by sect. 55.2 CE is the right contained under sect. 18.3 CE, which guarantees "the secrecy of communications, particularly regarding postal, telegraphic and telephonic communications, except in the event of a court order". The potential limitation of the fundamental right to the secrecy of communications in the context of a criminal process is regulated under sects. 579–588 LECrim. Depending on the medium involved, the form of intervention varies. For example, in the case of a postal communication, the procedure consists of its interception, detention, opening, and examination; the same procedure applies when the information being transmitted is in telegraphic form, although the judge in this instance may also confine him/herself to ordering copies of the telegrams from the Telegraph Office, so that the communication is still received by its addressee. Finally, in the case of telephonic intervention, the intention is not to interrupt or obstruct the line of communication, but rather to inspect, supervise, or listen to what goes on over the telephone, using surveillance, tapping, and recording equipment.

The intervention of the communications of one or more subjects must be ordered by a judge. However, "in an emergency situation, when investigations are being undertaken to establish the circumstances of crimes relating to the activities of armed bands or terrorist or rebel groups", the surveillance of postal, telegraphic or telephonic communications may be ordered by "the Home Office or, in it place, the Director of State Security. The competent judge should be notified in writing of the action and the reasons for the action immediately and, within seventy-two hours of the order being issued, make a ruling as to whether to revoke or confirm the measure" (sect. 579.4 LECrim).

Without the authorisation of the judge, therefore, the communications of a subject can only be intervened for up to 72 h. Because the relevant judicial body has to state in its decision whether or not the emergency intervention of communications is in accordance with the law, in part guided by the reasons declared by the authority

responsible for ordering the measure, the decision by the judge to confirm or rescind that order will have a direct bearing on the use in evidence subsequently of any incriminating information obtained in the course of the intervention. Once judicial approval has been granted, the action can continue according to the procedures outlined in the Code of Criminal Procedure.

Right now, the trickiest aspect of this question relates to surveillance of communications via telephone electronic mail, internet, etc. The current regulation of the intervention of communications under the Code of Criminal Procedure is by no means exhaustive. A ruling by the Constitutional Court in 1999 (STC 49/1999), for example, set out the critical areas that it thought should be included in the proper regulation of the limitation of the right guaranteed by sect. 18.3 CE. Similarly, according to the Constitutional Court an act providing for the intervention of communications should contain: "the definition of the types of individuals whose communications the courts may order to have placed under surveillance; the nature of the offences that may be used to justify such a measure; the establishment of a time limit on the duration of the action; the procedure for transcribing intercepted conversations; precautions to be taken to ensure that all recordings make it into the hands of the judge and those of the defence in a full and intact state; the circumstances under which recordings may or should be deleted or destroyed, particularly in the event of the charges being dismissed or the subject being set free".[19] It may seem an obvious statement but it is worth remembering that proper legislative regulation is essential in order to ensure against excesses of all kinds, whether perpetrated by the police authorities or on the part of the courts.

One of the most controversial aspects of this measure is the question of its duration. Section 579, subsection 3 LECrim states that the intervention of communications may be approved "via a motivated resolution, for a period of up to three months, extendable for additional periods of the same duration". For the measure to be effective, it is essential that its target remains unaware of the action; however, given that sect. 302, paragraph 2 of the LECrim states that an indictment may be kept secret for no more than 1 month, in the case of intervened communications that guarantee appears simply to have been dispensed with (by the extension from 1 to 3 months), yet without any prior reform of the law (Moreno Catena 2006). The legislator cannot keep avoiding this problem.

Once the judge has issued a writ authorising the intervention of communications, an official letter must be sent immediately to the company responsible for the telephonic services used by the subject, instructing them to put the measure into effect. Alternatively, the task may be entrusted to officers of the court using the appropriate warrant. Whichever one receives the task, the party responsible for intervening the subject's communications must report regularly regarding the results of the operation to the judge named in the order and is expected, ultimately, to submit all the documentary material and information obtained. This material is included in evidence, while the tape recordings are transcribed in a sworn affidavit

[19]Cf. STC 184/2003.

by the secretary whose function it is to receive and transcribe the recordings and to help the judge to decide which fragments are relevant to the case.

The intervention of communications in the case of Islamic terrorism can introduce a further complication, depending on the language used. When the court authorises an intervention, it must do so with the certainty that it will be possible to carry out the measure; in other words, that there are sufficient human and material resources to translate the content of the intercepted conversations and make them available for use during criminal proceedings to both prosecution and defence counsel. For instance, the judgement of sect. 3 of the National Criminal Court (Sentence Number 36/2005, 26 September),[20] mentions that the contents of the material sent by the Central Unit of External Information was "frankly overwhelming, owing as much to the volume of the material sent as to its lack of specificity".[21]

Another important issue in relation to the limitation of the right to secrecy of communications is the question of how to regulate access to the information relating to the intercepted telephonic communications. The object of the measure is not supposed to be to supervise the content of each communication, but to record the fact that it has occurred. In an appearance before the Chamber of Deputies on 27 October 2005,[22] the then Minister of the Home Office, José Alonso, defended the need to create new legislative provisions to make State storage of telephone records acceptable under the law. He also stressed the need to establish the legal terms of data storage, and the need for the identity of people buying pre-paid mobile phones to be registered. The purpose of all this would be to facilitate future investigations involving communications between terrorists. The aim, the Minister concluded, was to ensure that police in the middle of an investigation of a terrorist crime would not find themselves in the situation of requiring "a particular piece of telephonic information which could be of great importance, only to discover that the information has been destroyed in the absence of any obligation to preserve it for a minimum period of time, which, as you know, will be 12 months".

Despite the argument that supervision of communications applies only to the fact of the call itself and not to its content, this intervention grants the police and the judiciary extensive powers of control over the citizens of the State, which, if abused, could signify a serious breach of the right to intimacy. For that reason, every precaution should be taken to ensure that the measure is not used inappropriately.

---

[20]The ruling made against the leaders of al-Qaeda in Spain.

[21]From p. 115 of the judgement. The sentence continues: "There were a total of 75 boxes, measuring 24 cm (height) × 30.5 cm (length) × 22 cm (width), all filled with master tapes which were labelled according to the conversations contained on each and the dates on which those conversations took place. However, what each of the 'tapes' identified by the Attorney General's Office in its preliminary summary of conclusions with the instruction that it be played to the court in full session, was in fact in reference to hundreds of master tapes, contained in various different boxes and organised according to a uniform system of numbering (i.e. C-1020, C-320, C-1014, C-21, C-30, D-28)".

[22]Home Office Commission. Parliamentary Debates (*CC.GG. Diario de sesiones*): Chamber of Deputies, session number 24 (Thursday, 27 October 2005), under the presidency of Mrs. Carmen Hermosín Bono (pp. 9–10).

The intervention of communications is a very valuable measure vis-à-vis the obtaining of information and the prevention of certain criminal acts. Nevertheless, the government or legislator cannot justify its application solely on preventive grounds. The intervention of communications should be ordered against subjects who have already been charged with committing or participating in some kind of criminal act. It should not, however, be used on a more general basis against individuals with suspected links to terrorist organisations. The legal system as it stands already contains the instruments necessary to convert that suspicion into an accusation. The transformation from suspect to accused will have no effect on the investigation, in the sense of making it less efficient. What it will do is endow the operation with every possible safeguard to ensure the structural principles of due criminal process and the social and democratic Rule of Law remain intact, even when faced with especially critical or difficult circumstances. The only way to prevent the police authorities from making abusive use of the intervention of communications, safe in the knowledge that their actions can always be endorsed a posteriori by the courts, is to institute precise procedural criteria regulating its application.

16.6 The Right to Defence

Section 24.2 CE guarantees the right to defence and assistance by a lawyer. The right to defence is the right of the passive subject of the proceedings (the accused or the person being charged) to obtain effective protection from the judges and the courts based on a proper defence. In other words, the subject's defence acts as a legitimating factor of the accusation against him/her and its criminal sanction (Moreno Catena 2008). According to the Constitutional Court, the right to defence contained in sect. 24.2 signifies the freedom to be assisted by a lawyer of one's choice.[23]

In addition to sect. 24.2 CE, sect. 17.3 CE guarantees "the assistance of a lawyer during police and judicial proceedings, under the terms laid down by the law". In view of the judgements of the TC on this matter (STC 196/1987 and STC 38/2003), Grima Lizandra (2005) summarises what, according to the Constitutional Court, the triple purpose served by the presence of the lawyer during the detention process consists of: (1) guarantees that the constitutional rights of the person being held are respected; (2) guarantees the reliability of the evidence collected, because the lawyer will be able to confirm whether the transcript included in the statement brought before him to sign is a true representation of what was said during the interrogation; and (3) guarantees that the person being held is defended properly so that, for example, he/she receives technical advice regarding his/her rights during interrogation, such as the right to remain silent or the right to the active presence of counsel throughout.

According to the Constitutional Court's interpretation of the right to defence, the right to be assisted by the lawyer of one's choice applies even at the earliest stages

[23] SSTC 339/2005, 130/2001, 18/1995, or 216/1988.

of the criminal proceedings undertaken against a person. On that basis, the appointment of counsel by the court during the period of incommunicado detention in cases of suspected terrorism represents an unauthorised limitation of the right to defence according to sect. 55.2 CE and is, therefore, unconstitutional.

The appointment by the court of counsel for the detainee during the period of isolation is yet another measure that the legislator has deemed necessary in order to accomplish the objectives sought by incommunicado detention. Counsel for the detainee has regularly been used as a way of controlling or issuing orders or information to other elements of the organisation or band of which the person being held is a member.[24] As Gómez Colomer (1988) points out, the court appointment measure is based on the hypothesis that any lawyer freely chosen by a person detained for terrorist activities will purposely attempt to defy the deprivation of contact order.[25]

The inevitable question raised by all of this is whether the ordering of incommunicado detention constitutes an unauthorised limitation of the fundamental right to defence under sect. 55.2 CE. The Constitutional Court has based its rulings on the final part of sect. 17.3 where it states that the lawyer's assistance during police and judicial proceedings should occur "according to the terms established by law", meaning that, if the law considers that in a case of incommunicado detention the lawyer present should be court-appointed, the subject's right to defence has not been violated.[26] The constitutionality of sect. 527.a LECrim was appealed on the grounds that it was in contravention of the right guaranteed under sect. 17.3 CE. The case was resolved by STC 196/1987 with the rejection of the action, based on the Constitutional Court's finding that the provision in question was not in breach of the detainee's fundamental right to legal counsel. The Constitutional Court's basic argument was that, in the criminal process, a distinction should be made between the right to be assisted by a lawyer during police and judicial proceedings (sect. 17.3 CE) and the right to defence, stated in sect. 24.2, as part of the right to due process with full guarantees: "sect. 17.3 CE recognises this right of the 'detainee' during police and judicial proceedings as one of the entitlements guaranteed by the right to freedom protected under subsection 1 of the same section; section 24.2 CE, on the other hand, recognises this entitlement in the context of the right to effective protection from the judges and the courts and the associated guarantee of due process, particularly in relation to criminal proceedings".[27] In our opinion, the distinction proposed by the Constitutional Court is a highly questionable one.

---

[24] The magistrates who signed the dissenting vote to STC 196/1987 summarised the position of the court as follows: "The measure is designed to prevent the lawyer freely chosen by the detainee from conspiring with third parties to obstruct the investigations of the police or the judicial authorities".

[25] Likewise, as the dissenting vote of Magistrate Carlos de la Vega Benayas (seconded by Magistrate Luis Díez-Picazo y Ponce de León) points out: "it would make more sense and be more effective, ultimately, to charge and prosecute the lawyer who breaks the law".

[26] SSTC 199/1987 and 25/1981.

[27] SSTC 339/2005, 7/2004, 188/1999, 48/1982, and 121/1981.

What the Constitutional Court's ruling would seem to suggest is that, whether appointed by the detainee or by the court, the purpose of the lawyer's presence during the making of statements to the police is confined to guaranteeing the detainee's right to freedom. His/her role, after all, essentially consists in ensuring the subject's legal entitlements are met and that all the rights and protections pertaining to his/her detention are observed. The function attributed by the Constitutional Court to legal counsel for the detainee during the first hours of detention is not, in our opinion, an accurate interpretation of the law and represents a limitation of the detainee's right to defence. Our conclusion is based on the premise that the subject's defence is a legitimating factor of the accusation against him/her and its criminal sanction in law, and also that the defensive strategy of the accused clearly begins at the moment of detention (Moreno Catena 2008). It could be concluded, therefore, that, failing any explicit legal authorisation for it (because sect. 55.2 CE does not authorise the restriction of sect. 24.2), the procedural regulation regarding the presence of counsel, as it stands, does represent a limitation of terrorist subjects' fundamental right to defence (Moreno Catena 2006).

The allocation of court-appointed counsel has a fixed duration, though: as soon as the isolation order is lifted, the person in custody may proceed, if he/she so wishes, to appoint a lawyer of his/her own choice to take over his/her case for the remainder of the process.

16.7 The Right to the Ordinary Judge Predetermined by Law

Section 24.2 CE guarantees the right to the "ordinary judge predetermined by law", the essential content of which consists, in the words of the Constitutional Court, of three basic pillars: (1) prohibited the institution of jurisdictional bodies except by a specific act to this effect, though not by organic act as such[28]; (2) prohibited the creation of special courts; and (3) possibility of specifying with absolute certainty the court designated to rule on a criminal act from the moment of its commission. These three standards are, according to the Constitutional Court, what guarantee the system against the creation of ad hoc courts.[29]

The Code of Criminal Procedure (sect. 14) gives competence over the investigation and prosecution of all crimes to the judge in the place where those crimes have been committed (*forum delicti commissi*). However, in cases of terrorism, the investigation is overseen by a Central Court of the First Instance (*Juzgado Central de Instrucción*), regardless of where the crime was committed, whereas the trial itself is dealt with by the Central Criminal Court (*Juez Central de lo Penal*), Central Juvenile Court (*Juzgado Central de Menores*), or National Criminal Court (*Sala de lo Penal de la Audiencia Nacional*). All of these jurisdictional bodies have their

[28] SSTC 95/1988 and 101/1984.

[29] SSTC 171/1994, 199/1987, and 47/1983.

base in Madrid and jurisdiction over the whole of Spain, which means that, regardless of where a terrorist attack takes place, the competence for trying the crime will fall to one of them.

The National Criminal Court was set up by decree on 4 January 1977. From the outset, both it and the Central Courts of the First Instance were accused by certain sectors of being unconstitutional (Lamarca Pérez 1989; Gimeno Sendra 1983). Over time, however, and after the Constitution was voted in 1978 and, subsequently, the organic act concerning the Powers of the Judiciary (1985), the National Criminal Court and Central Courts of the First Instance gradually became accepted as ordinary courts (Mestre Delgado 1987). Their status as ordinary courts was recognised, for example, both by the Report of the European Commission on Human Rights (16 October 1986) and by the Constitutional Court, which ruled that "the constitutional prohibition of exceptional non-ordinary judges does not mean that the legislator may not in certain cases be justified in providing for the investigation and prosecution of those cases by a centralised judicial organ without this signifying a contradiction of sect. 24 CE" (STC 199/1987).[30]

The transitional provision in LO 4/1988 instructed that jurisdiction over the investigation and prosecution of criminal proceedings against members of armed bands or persons connected with terrorist or rebel groups would continue to correspond to the Central Court of the First Instance and the National Criminal Court (as had been the case under LO 11/1980 and LO 9/1984). The jurisdiction of the National Criminal Court over terrorist crimes, therefore, comes under the general provision in sect. 65.7 LOPJ, which uses the phrase "any other matter of competence assigned to it by law". Therefore, although there is no danger of mistaking the courts of the National Criminal Court for the other judicial organs, owing to the territorial factor governing the latter, the competences assigned to the former could be considered unconstitutional if the determining principles outlined in the Constitution are followed to the letter (Moreno Catena 2008; Gimeno Sendra 1977).

Among the arguments in favour of maintaining the competence of the National Criminal Court to try terrorist crimes (and also that of the Central Court of the First Instance, the Central Criminal Court, and the Central Juvenile Court), there are two that stand out: firstly, the greater efficiency of these centralised organs and, secondly, the greater resources available to them. Neither of these arguments, however, is completely sound. The Constitutional Court, in an attempt to justify the competence of the National Criminal Court in cases of terrorism, has recalled that the purpose of crimes of this nature is "the disruption of constitutional order" (STC 56/1990). However, according to the constitution itself, the motive for a crime cannot be used as a reason to alter the general regime of jurisdiction and hence the fundamental right to the ordinary judge predetermined by law (Moreno Catena 2006).

The real reason for assigning terrorist crimes to the jurisdiction of these centralised courts appears to have been the need to remove trials for terrorism from the Basque Country. The terrorist organisation ETA has, after all, been the group

[30] SSTC 56/1990 and 153/1998.

responsible for the greatest number of attacks and victims in Spain; the conducting of trials against these terrorists within the Basque Country did not, therefore, seem the best possible course of action. Something that is frequently slipped into the debate is the notion that a judge in the Basque Country in charge of the trial of a member of a terrorist organisation will find his/her task obstructed by all but insurmountable difficulties (e.g. threats against his/her life and the lives of those close to him/her). There is no solid reason to justify the present attribution to the organs of the National Criminal Court of competence over the prosecution of terrorist crimes, other than the traditional inertia of the system and greater convenience from an administrative point of view. In fact, if the argument in favour of maintaining the competence of the National Criminal Court really is based on the reasoning that judges in the place where the crime has been committed will find themselves unable to carry out their duties, that makes the measure an emergency one designed to compensate for the State's inability to guarantee the normal functioning of its institutions (Moreno Catena 2006). It means acknowledging the impossibility of controlling the problem within the established borders of the constitution.

Calls for the National Criminal Court to be dissolved and for terrorist crimes to be tried in the proper courts according to the *forum delicti commissi* territorial principle are growing all the time. The matter, however, is undeniably complex and it seems unlikely, at least in the short term, that the legislator will withdraw the National Criminal Court's competence in cases of terrorism.

16.8 The Ultimate Guarantee: The Right to Be Presumed Innocent

The fundamental right to be presumed innocent (sect. 24.2 CE) is, without question, one of the core differences between the adversarial and inquisitorial systems: the accused remains innocent until a guilty verdict is pronounced against him/her (sect. 6.2 European Convention of Human Rights and sect. 14.2 International Covenant on Civil and Political Rights). Since 1981 (STC 31/1981), the Constitutional Court has been working to define in exactly what the right to be presumed innocent consists. For a presumption of innocence to be invalidated, there must be minimum evidence of actions to support the charges being made, on the basis of which the guilt of the accused may be deduced. The case against the accused should be brought at the instance of the prosecution with the full procedural and legal guarantees of the law, taking special care to ensure that evidence is not obtained by unlawful means; in other words, that it respects the principles of publicity, immediacy, contradiction, and orality, and that its relevance is clearly stated in the judgement (Moreno Catena 2008). As the Supreme Court ruling of 25 February 2008 states, "evidence is considered admissible when it has been obtained in accordance with the structural principles governing evidence-gathering procedures, so judged by the jurisdictional courts. Evidence is considered sufficient when its content is clearly incriminatory".

The court is not permitted to base a conviction on evidence that has been obtained in violation of a fundamental right (sect. 11.1 LOPJ) (González-Cuéllar Serrano 1990). That rule applies to all cases, including, naturally, trials for terrorism. The right to be presumed innocent is, therefore, the last guarantee available to terrorists as grounds for the exclusion from evidence of probative material obtained in violation of one of their fundamental rights: for example, self-incriminating statements made to the police following subjection to torture; material obtained during an entry and search operation carried out without all the necessary legal conditions; or incriminating material obtained through the intervention of the subject's communications.

In the case of the self-incriminating statements that an alleged terrorist may make to the police while being held in isolation, the crucial point to make certain of is that the statements could not have been made as a result of torture or inhuman or degrading treatment, prohibited under sect. 15 CE. This control requires the special collaboration of the examining magistrate, before whom the alleged terrorist will appear following the termination of his/her time in police custody. In STC 7/2004, the Constitutional Court found itself called on to rule on the probative validity of the first statements made by appellants to the examining magistrate. On that occasion, the statement to the examining magistrate was made immediately after the lifting of a 5-day incommunicado detention, during which period, the National Criminal Court heard, the detainees had suffered torture and abuse. As soon as the detainees were brought before the judge, they were properly informed of all their rights and were assisted throughout the proceedings by a lawyer appointed by them. However, the Constitutional Court ruled that the testimony heard by the examining magistrate was not valid because, although there was nothing formally to fault in the actions of the judge, the examining magistrate should have taken into account the fact that only a few hours earlier the detainees had been subjected to torture and abusive treatment. The Constitutional Court ruled that statements made by the detainees immediately after their release were influenced by the treatment they had received in custody and its impact on their physical and mental state. The examining magistrate should have delayed the hearing to allow for prior consultation between the detainees and their lawyers, or should have obtained some kind of additional medical or psychological report in regard to the situation in question. In the opinion of the Constitutional Court, therefore, statements made to the examining magistrate are not considered to be valid.

A situation that occurs on a very regular basis is that in which a person charged with a terrorist crime makes self-incriminating statements to the police and examining magistrate, but subsequently, during the trial, either denies the statements, alleging they were made under torture, or refuses to testify. This leaves the sentencing court with the problem of how to determine the value, if any, of self-incriminating statements made by the accused while being held in isolated custody during the investigation phase. The statements may be submitted in evidence provided their introduction is accompanied by sufficient guarantees to preserve the contradiction (Moreno Catena 2008; Tomé García 2007; Guzmán Fluja 2006). According to STC 127/2000, for pre-trial statements to be used in evidence, they must have

been made in full accordance with the guarantees required by law: they must be made before the examining magistrate in the presence of counsel, and must be read into record at the administrative hearing. For statements made to the police to be submitted, the police officers in charge of the interrogation must appear before the court and confirm the evidence recorded there. However, self-incriminating pre-trial statements are only admissible if they have not been obtained as a result of torture or inhuman or degrading treatment. When evaluating statements made before the examining magistrate, the sentencing court should, in addition, take into account the rest of the evidence against the accused.

The right to be presumed innocent also means that the results of an entry or search or intervention of communications carried out under the legal powers granted by sects. 553 and 579.4 LECrim (that is, without the prior order of a judge), will be excluded from evidence if the operation has not received subsequent confirmation from the appropriate judicial authority.

The ruling of sect. III of the National Criminal Court (sentence number 36/2005, 26 September), concerning the intervention of communications and the corresponding limitation of sect. 18.3 CE, recalls the existence in law of general conditions for the adoption and implementation of the measure (reasonable grounds, specificity, and judicial control), failure to observe which will lead to the telephonic interventions involved being declared illegal on the grounds of unconstitutionality, along with all other sources of proof deriving from them. That ruling also points out, however, that there are other conditions proceeding from ordinary law whose non-observance does not constitute the violation of a fundamental right. In that situation, the infringement of the subject's legal rights would affect the validity of the results of the intervention as admissible evidence, but would not have any impact on the rest of the prosecution's case.[31]

The three binding conditions demanded by the Supreme Court for the limitation of sect. 18.3 CE are: (1) authorisation of a judge; (2) exceptionality of the measure; (3) proportionality of application. Hence, for the intervention of communications in the course of an investigation in the case of terrorism to be constitutionally admissible, a judicial order confirming the measure will always be necessary, whether issued by the Home Office or by the General Direction of State Security.

16.9 Conclusion

Using sect. 55.2 CE as a point of reference, the Spanish legislator has created measures to limit the fundamental rights of freedom (sect. 17.2 CE), the inviolability of the home (sect. 18.2 CE) and secrecy of communications (sect. 18.3 CE), in its efforts to combat terrorism. In 1978, the parties involved in drawing up the Constitution foresaw that it would be necessary to restrict fundamental rights in

[31] Cf. Ruling of the Supreme Court of 21 July 2004 and 15 December 2004.

order to defend against crimes of this kind, but they also wished that such restrictions should be safeguarded by the maximum protections. The antiterrorist measures adopted in many countries in the wake of the 11 September attacks on the US in 2001 have made it clear that, when it comes to fundamental rights, the risk of regression is always present. At this juncture in history, sect. 55.2 CE sets an important standard and an example for other states to follow.

None of which means, of course, that there is nothing to criticise in the manner in which the legislator has interpreted sect. 55.2 CE. Following several attempts to regulate the limitation of fundamental rights via specific acts based on sect. 55.2 CE (organic acts 11/1980 and 9/1984), with LO 4/1988 the legislator finally opted to include in the Code of Criminal Procedure (LECrim) the limitations on the fundamental rights listed above (sects. 520 bis, 553 and 579.4). As we have sought to demonstrate throughout this chapter, there is still a need in certain areas for more precise and exhaustive legislative regulation of the limitations imposed on specific fundamental rights (as in the case of extending the time limit on the period allowed for preventive arrest). The police and the judiciary, indeed, appear to have accepted already that, as a general principle, the limitation of fundamental rights should only occur on a case-by-case basis and under exceptional circumstances.

Nevertheless, sect. 55.2 CE has not managed to prevent other fundamental rights from being restricted in trials for terrorism. This is what has happened, for example, in the case of the right to the ordinary judge predetermined by law and the right to defence (sect. 24.2 CE). The creation of the National Criminal Court (*Audiencia Nacional*) in 1977 is still a source of debate and demands for it to be dissolved continue to be raised. In relation to the right to defence, the fact that a terrorist is not permitted to appoint a lawyer of his/her choice to be present throughout all police and judicial proceedings represents, in our view, a clear limitation of that right and one that is not sustained by sect. 55.2 CE – in spite of the Constitutional Court's ruling to the contrary.

There are still many questions that must be addressed in regard to current Spanish legislation, in order to ensure that the limitation of the fundamental rights of terrorists (or alleged terrorists) is only sought as a last resort; the Rule of Law requires that it be so. We are still confident, however, that, in the Spanish legal system, the criminal justice process will remain the cornerstone of public safety policy making against the threat of terrorism.

References

Bartolomé Cenzano, José Carlos DE, *Derechos Fundamentales y Libertades Públicas*, Tirant lo Blanch, Valencia, 2003.

Catalina Benavente, Mª Ángeles, "La restricción de derechos fundamentales en el marco de la lucha contra el terrorismo", Estudios de Progreso, Madrid, núm. 21/2006, pp. 31 y ss. También disponible en www.falternativas.org

Catalina Benavente, Mª Ángeles., "Los supuestos de detención en los casos de terrorismo: propuestas para una reforma", en Faraldo Cabana (Coord.), *Derecho Penal de Excepción Terrorismo e inmigración*, Tirant lo Blanch, Valencia, 2007.

Fernández Segado, Francisco, "Naturaleza y régimen legal de la suspensión general de los derechos fundamentales", en *Revista de Derecho Político*, núms. 18–19, 1983.
Gómez Colomer, Juan Luis, *La exclusión del abogado defensor de elección en el proceso penal*, Bosch, Barcelona, 1988.
González-Cuéllar Serrano, Nicolás, *Proporcionalidad y derechos fundamentales en el proceso penal*, Colex, Madrid, 1990.
Grima Lizandra, Vicente, "El derecho de defensa y el derecho de asistencia letrada en las detenciones policiales", tol. 526382, www.tirantonline.com.
Guzmán Fluja, Vicente, *Anticipación y preconstitución de la prueba en el proceso penal*, Tirant lo Blanch, Valencia, 2006.
Lamarca Pérez, Carmen, *Tratamiento jurídico del terrorismo*, Ministerio de Justicia, Madrid, 1985.
López Garrido, Diego, *Terrorismo, Política y Derecho*, Alianza, Madrid,1987.
Mestre Delgado, Esteban, *Delincuencia terrorista y Audiencia Nacional*, Ministerio de Justicia, Madrid, 1987.
Miguel Zaragoza, Juan de, "La Ley Orgánica 11/1980, de 1 de diciembre, sobre los supuestos previstos en el artículo 55.2 de la Constitución", en Documentación Jurídica, Madrid, núms. 29–32, 1981.
Moreno Catena, Víctor, "Garantía de los derechos fundamentales en la investigación penal", en *Justicia Penal*, Revista Poder Judicial, núm. Especial II, 1987.
Moreno Catena, Víctor, "El enjuiciamiento de delitos de terrorismo y el derecho de defense", en Gómez Colomer, J.L., González Cussac, J.L.,(coord.), *Terrorismo y proceso penal acusatorio*, Tirant lo Blanch, Valencia, 2006.
Moreno Catena, Víctor, *Derecho Procesal Penal* (con CORTÉS DOMÍNGUEZ, V.), (3ª. Edición). Tirant lo Blanch, Valencia, 2008.
Ovejero Puente, Ana María, *Constitución y derecho a la presunción de inocencia*, Tirant lo Blanch, Valencia, 2006.
Pulgar Gutiérrez, Mª Belén, *Víctimas del Terrorismo: 1968–2004*, Dykinson, Madrid, 2004.
Remotti Carbonell, José Carlos, *Constitución y medidas contra el terrorismo. La suspensión individual de derechos y garantías*, Colex, Madrid, 1999.
Terradillos Basoco, Juan, *Terrorismo y Derecho. Comentario a las Leyes Orgánicas 3 y 4/1988, de reforma del Código Penal y de la Ley de Enjuiciamiento Criminal*, Tecnos, Madrid, 1988.
Tomé García, José Antonio (y otros), *Derecho Procesal Penal*, (8. edición). Ramón Areces, Madrid, 2007.
Vercher Noguera, Antonio, *Antiterrorismo en el Ulster y en el País Vasco*, PPU, Barcelona, 1991.

Chapter 17
The Fight Against Terrorism and Human Rights: The French Perspective

Olivier Cahn

17.1 Introduction

Fighting terrorism that threatens its institutions and citizens is not a recent concern for the French government. The history of terrorist attacks goes back to the mid nineteenth century and "the French capacity to fight terrorism [is] the result of hard-won lessons […] (as) France has always been on the 'bleeding edge' of terrorism, confronting terrorism in all its guises".[1]

Historically, the first statutes specifically aimed to fight terrorism passed by the French Republic are the four enacted between December 1893 and July 1894 to combat anarchist activists. Legislators then resorted to special legislation, interfering with some of the civil liberties granted when the Third Republic was founded, which immediately caused a virulent reaction from both Liberals and Parliamentary opposition.[2] Apart from the Vichy government sequence, the Algerian war of independence (1954–1962) constitutes the second circumstance in which French authorities implemented exceptional legislation to fight what they regarded as terrorist acts. Acts of violence committed by soldiers then put in charge of counter-terrorism policing eventually gave rise to offended rejection from part of the civil society. Furthermore, such policy rapidly proved in the meantime amazingly expensive and not apparently efficient. These two setbacks explain that when the French governments had to face a resurgence of terrorist attacks in the mid 1980s, they showed reluctance to enact special legislation.

O. Cahn (✉)
School of Law University of Cergy-Pontoise, Cergy-Pontoise, France
e-mail: oliviercahn@orange.fr

[1] J. Shapiro and B. Suzan, *The French Experience of Counter-terrorism*, Survival, vol. 45, n° 1, Spring 2003, p. 68.

[2] These statutes were called the "*lois scélérates*" (which can be translated as "the villainous statutes") and eventually fell into abeyance before being overruled in 1992.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_17,

The current French counterterrorism law is the outcome of 20 years of evolution. After a period of time of approximately 15 years during which terrorist attacks relatively spared France, the mid 1970s marked the resumption of terrorism – protean in its motives and exerted both within and outside French borders – that has never stopped since. Although only Corsican separatists have perpetrated attacks on French territory since 1996, French citizens and interests abroad have recently been targeted and counterterrorism services have thwarted few planned attacks. Thus, the terrorist threat is still prominent in France.[3] As a consequence, the necessity to fight terrorism remains meaningful.

In the mid 1980s, both the lack of preparation of the police and judicial institutions and the inadequacy of the enforcement tools they enjoyed to fight terrorist attacks appeared blatantly. In the meantime, the failure of diplomatic attempts, consisting of seeking arrangements with terrorist-supporting States, led the French government to modify radically its counterterrorism policy to concentrate on increasing deterrent and enforcement capacities of the penal apparatus. The first antiterrorism statute was thus passed in 1986. As resorting to special legislation was excluded for the reason above mentioned, legislators opted for an adaptation of ordinary criminal law and procedure based on the implementation of specific rules. The 1986 statute was complemented in 1996 by a further statute meant to adjust the French legislation to the evolution of the terrorist threat and/or forms of action. It explains why the general framework of the French counterterrorism apparatus[4] was not substantially reformed following 9/11. Indeed, according to the conclusions of the assessment carried out by the General Secretariat of the European Union Council in 2004, its economy, internal structure, and philosophy, both as regards general organisation and operational pertinence, already proved to be appropriate and to provide enforcement agencies with the required repressive means.[5] This absence of resort to exceptional legislation is probably the distinctive mark of the French counterterrorism system and it should certainly be regarded as an achievement for the protection of fundamental rights and civil liberties.

Nonetheless, since 9/11 – and furthermore since the Madrid and London bomb attacks – the French government has put before Parliament four Bills containing provisions intended to improve counterterrorism that have all been passed. Some of the new provisions undeniably contribute to the adaptation of the antiterrorism legislation as they allow internal security services to benefit from technological improvements or as they enforce new powers required to combat modern forms of

[3]According to a recent Government White Paper, more than 20 planned attacks on French soil have been foiled since 1998 (Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006), and the Europol assessment proves that France is probably, after Spain, the Member State of the European Union that is the most concerned by the terrorist threat (Europol, *TE-SAT 2008, EU Terrorism situation and trend report*, 2008, p. 16).

[4]No exceptional legislation was passed on to substitute for authorities in charge or the principles governing investigations and trials.

[5] G. de Kerchove, EU Counter-terrorism Coordinator, interview with the author, 4th March 2008, EU Council.

terrorism. On the other hand, there are reasons to suspect that the necessity to set up effective counterterrorism legislation has been exploited by the Executive and security forces to provide police services with widely enforceable coercive and intrusive powers. The latter threatens the fundamental rights of people who cannot be suspected of any involvement whatever in terrorism.

We shall therefore distinguish within the French counterterrorism system, on the one hand, the achieved balance with human rights consisting of having managed to keep the fight against terrorism within the frame of ordinary criminal law; and, on the other hand, the deficiencies of the system to guarantee effectively fair protection of human rights.

17.2 The Achieved Conciliation Between Counterterrorism and Human Rights: Keeping the Fight Against Terrorism within the Frame of Ordinary Criminal Law

Since the first antiterrorism statute was passed on 9 September 1986,[6] the French antiterrorism legal framework has been constantly adapted to improve the general efficiency of the repressive apparatus on both the national and the international scene and to implement multilaterally made norms or decisions.[7] This longstanding experience made possible the development of wide-ranging counterterrorism strategies involving all relevant ministries and security forces, capacities to assess and prevent the terrorist threat and efficient intelligence gathering and enforcement capabilities.

International law constraints and limited capacities of national military forces have led the French Administration to disregard counterterrorism enforcement activities outside its national boundaries, to concentrate on working out a penal apparatus aimed to, in the meantime, prevent terrorists from entering French territory, and to anticipate, as much as legally admissible, curbing to neutralise terrorists at the preparatory stage of their actions. Efficient counterterrorism culture and mechanisms were thus implemented from 1986. The pre-existence to 9/11 of this structured antiterrorist apparatus helps to explain why France was only slightly impacted by the elimination of conceptual borders between war and counterterrorism

---

[6] Loi n° 86-1020 du 9 septembre 1986 *dite Chalandon, sur les repentis, relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'Etat*, JORF, 10th September 1986, p. 10,956.

[7] Loi n° 96-647 du 22 juillet 1996 *tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire*, JORF, 23rd July 1996, p. 11104; loi no 2001-1062 du 15 novembre 2001 *relative à la sécurité quotidienne*, JORF, 16th November 2001, p. 18215; loi n° 2003-239 du 18 mars 2003 *pour la sécurité intérieure*, JORF, 19th March 2003, p. 4761; loi n° 2004-204 du 9 mars 2004 *portant adaptation de la justice aux évolutions de la criminalité*, JORF, 10th March 2004, p. 4567; loi n° 2006-64 du 23 janvie r 2006 *relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, JORF, 24th January 2006, p. 1129 ; loi n°2008-1245 du 1er décembre 2008 *visant à prolonger l'application des articles 3, 6 et 9 de la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, JORF, 2nd December 2008, p.18361.

that have affected some of its allies' legal systems.[8] To that extent, the French experience should certainly be considered as a model of protection of fundamental freedoms in the fight against terrorism.

French legislators thus managed to avoid the pitfall of resorting to special or emergency legislation involving a temporary dispensation from the European Convention on Human Rights. The improvement of the ability of the criminal justice system to fight terrorism is intended to result from the coordination of the activities of all actors involved. Besides, counterterrorism legislation is characterised by a specialisation of both the institutions involved and the enforceable rules of criminal law and criminal procedure.

17.2.1 The Coordination of Counterterrorism

The coordination of the exchange of intelligence and of enforcement activities is identified as an issue of crucial importance by the European Union experts.[9] As a matter of fact, it is a permanent priority that has led French antiterrorism policy since 1986.

Indeed, one of the main reasons identified to explain the French criminal justice system's incapability to prevent and rapidly stop the wave of terrorist bombings and murders perpetrated in the mid 1980s was the total lack of coordination between the services involved.[10] Being a centralised State, no alternative was offered to the French government but finding a way to gather and rationalise the competences *rationae loci* and *materiae* of the various police forces and jurisdictions involved in the fight against terrorism with a view to compel them to collaborate. The solution found was to create, at all stages of the administrative apparatus, centralised and integrated ad hoc organisations that are in charge of coordinating the criminal justice process.

17.2.1.1 Centralisation

According to French counterterrorism doctrine, centralisation is regarded as a prerequisite for specialisation of investigation, prosecution, and trial authorities. Centralisation in Paris is certainly a manifestation of French Jacobinism but it is also the result of a pragmatic choice. As judicial police services vested with

---

[8] H. Tigroudja, *Quel(s) droit(s) applicable(s) à la* "*guerre antiterrorisme*"*?*, AFDI, XLVIII, 2002, pp. 81–102.

[9] Council of the European Union, Presidency in co-operation with the Counter Terrorism Coordinator, *Final report on the Evaluation of National Anti-Terrorist Arrangements: Improving national machinery and capability for the fight against terrorism*, 12168/3/05 REV 3, 18 November 2005, p. 2.

[10] J.-F. Gayraud et D. Sénat, *Le terrorisme*, PUF, coll. Que sais-je?, 2ème éd., 2006, p. 54.

national territory-wide competence were already attached in Paris, it was thought more appropriate to promote operational and efficient coordination between police and judicial authorities, to concentrate them within the same area.

Therefore, article 706-16 of the Criminal Procedure Code (CPC) provides that terrorist offences punishable by articles 421-1 to 421-5 of the Penal Code committed on the French territory or, when French law is applicable, abroad,[11] are prosecuted, investigated, and tried according to the specific rules provided in the CPC. According to article 706-17, "for the prosecution, investigation and trial" of acts of terrorism, "the Paris public prosecutor, investigating judge, correctional court and assize court hold a jurisdiction concurrent to that deriving from" ordinary jurisdiction law and, further, that "where they hold jurisdiction", Paris magistrates exercise their "authority over the whole national territory".[12] Articles 706-18 to 706-22 provide for conflict of jurisdiction settlement rules "in favour of the Paris judicial investigation authorities". As a consequence, the vast majority of terrorism cases are in practice now centralised and dealt with in Paris at any stage of the criminal justice process.[13]

With the purpose of guaranteeing the effectiveness of counterterrorism coordination, the centralisation of the authorities has been coupled with the setting up of integrated ad hoc structures in which the various administrations involved in anti-terrorism are merged.

17.2.1.2 Integration

Increase and transformations of the terrorist threat and forms of attacks faced by France in the mid 1980s and the incapacity of the then-divided penal apparatus to effectively deal with them have made the French government aware of the fact that terrorism could not be fought by isolated policing and/or judicial administrations acting on their own. It led to the doctrine of the mobilisation of all security forces to prevent and repress acts of terrorism through a global and coordinated action which should involve all administrative levels of the State organisation. As a consequence, an integrated organisation of the fight against terrorism was designed and is carried out both at the central level and through intermediate ad hoc institutions. Such an organisation is purposed to ensure the coherence of the State's penal answer, to avoid loss or dilution effects that could impair efficiency and to allow the organised mobilisation of all State means required for the investigation, prosecution, and trial of terrorism cases.

---

[11] Articles 113-6 to 113-12 of the Penal Code and article 689-9 CPC. See also: A. Huet and R. Koering-Joulin, *Droit pénal international*, PUF, coll. Thémis droit, 3è ed., 2005, pp. 194–199.

[12] The legality of such an adaptation of ordinary jurisdiction rules has been confirmed by the Constitutional Council (Conseil Constitutionnel, Décision n° 86-213 DC du 3 septembre 1986, *Loi relative à la lutte contre le terrorisme et aux attentats à la sûreté de l'Etat*, Recueil, p. 122, §.12).

[13] V. Bianchi, La loi du 23 janvier 2006 ou l'extension à l'application des peines de la compétence nationale en matière de terrorisme, Gazette du Palais, Recueil mai-juin 2006, p. 1570.

At governmental level, the coordination of the fight is primarily devoted to the Internal Security Council (CSI),[14] which is chaired by the President of the Republic. It aims to draw up the headlines of the counterterrorism policy and to define the political priorities operational services will have to implement. Its action is taken over by two inter-ministerial committees. In accordance with the recommendations contained in the White Paper on Defence and National Security 2008,[15] an Intelligence National Council (CNR), chaired by the President of the Republic, has been set up in September 2008 to replace the former Inter-ministerial Intelligence Committee (CIR). It is in charge of inter-ministerial coordination of the sharing out of intelligence and of the prospective through permanent specialised working groups. The Antiterrorist Inter-ministerial Liaison Committee (CILAT) is in charge of inter-ministerial operational aspects of counterterrorism. Its aim is to decide the measures required to respond to the terrorist threats, facilitate exchange of intelligence between security services, and coordinate operations.

The coordination and regulation between decisions taken at the governmental level and all security forces involved in the fight against terrorism are undertaken by the General Secretariat of the National Defence (SGDN) and, furthermore and primarily, by the Anti-Terrorism Fight Coordination Unit (UCLAT). The UCLAT is a permanent ad hoc structure, set up in 1984 within the ministry of the Interior, aimed to ensure inter-agencies co-operation by promoting a joined-up approach to terrorism and counterterrorism and a fully coordinated response to terrorism activities. It is mainly in charge of the permanent and specific coordination of the centralisation and circulation of intelligence between the various police services, intelligence agencies, and all other forces involved in counterterrorism both nationally and internationally (which explains why antiterrorism foreign liaison officers are attached to this service). It is also vested with the direction of the Joint Investigation Teams implemented to fight cross-border terrorism and involving French and other EU Member State authorities,[16] and it coordinates the exchanges with Europol.

International police co-operation is also integrated to maximise its efficiency through the *Service Central de Coopération Opérationnelle de Police* (SCCOPOL).[17] Not dedicated to counterterrorism, this unit is the contact point for international co-operation, in which are gathered the Paris NCB – Interpol, the French N-SIS and SIREN, and the Europol National Unit. It also receives the foreign liaison officers. Thus, the SCCOPOL is the interlocutor of the investigators and magistrates who require information from foreign police forces or judicial system with a view to use them in Court.

---

[14] Décret n° 2002-890 of 15th May 2002, JORF, 16th May 2002, p. 9246.

[15] Commission chargée de l'élaboration du Livre Blanc sur la Défense et la Sécurité Nationale, *Défense et Sécurité Nationale - Le Livre Blanc*, Odile Jacob - La Documentation française, juin 2008.

[16] Following the adaptation of article 13 of the *European Union Convention on Mutual assistance in Criminal Matters between the Member States of the European Union* of 29th May 2000 through articles 695-2 and 695-3 CPC, JIT have been created in France in antiterrorism cases, mainly with the Spanish authorities.

[17] Police Operational Co-operation Central Service.

Finally, a crisis management centre, called *Centre Opérationnel Beauvau* and chaired by the General Director of the National Police, has been installed within the ministry of Interior. It is in charge in case of a crisis situation (for example, a terrorist bomb attack) or of an important event involving a threat of being targeted by terrorists, to coordinate the police and gendarmerie on the field operations.

Integration is made easier as a result of the French penal culture, which is distinguished by the strong interdependence that exists between police services activities and the work of the magistrates.[18] The legislator establishes crossed institutional interfaces linking the services involved[19] and the existing interface between intelligence and enforcement implies strengthening co-operation between police forces and the judiciary.[20]

Such a counterterrorism framework is entirely consistent with, and satisfies all of, the recommendations made by the experts of the European Union.[21]

The coordination of the activities of administrations involved in the fight against terrorism is coupled with a specialisation of the counterterrorism arsenal.

17.2.2 Specialisation

The purpose pursued through specialisation is, on the one hand, to improve the repressive efficiency of the criminal justice system and adapt the State response to the evolutions of terrorism activities and, on the other hand, to adapt French law to the provisions of international norms, mainly European Union rules. Nonetheless, as regards the subject of this study, the noticeable achievement is the endeavour made by the legislator to keep the antiterrorism system within the ordinary criminal justice system.

---

[18] In the wording of the French Constitution (Title VIII), the Judiciary is not a separate power but an authority whose independence is guaranteed by the President of the Republic. As a consequence, article 30 CPC provides for the subjection of Public Prosecutors to the Minister of Justice. Although hardly consistent with the principle of separation of powers, police forces (civil servants) and public prosecutors (magistrates) are thus under the immediate authority of the Executive.

[19] For example, the SGDN is in charge of the Secretariat of the CILAT and takes part to the CSI, the UCLAT is associated to the works of the CSI; civil servants from the ministries of Defence and Interior are attached to the SGDN and to the Under-Direction of Security of the Foreign Office; officers of the Gendarmerie and of the Customs are assigned to the UCLAT, magistrates and officers of the gendarmerie, national police, and customs are attached to the SCCOPOL, etc.

[20] O Dutheillet de Lamothe, Member of the Constitutional Council, Conference, *French legislation against terrorism: constitutional issues*, 11th November http://www.conseil-constitutionnel.fr/divers/documents/constitutionalterrorism.pdf"2006www.conseil-constitutionnel.fr/divers/documents/constitutionalterrorism.pdf.

[21] Council of the European Union, Presidency in co-operation with the Counter Terrorism Coordinator, *Final report on the Evaluation of National Anti-Terrorist Arrangements: Improving national machinery and capability for the fight against terrorism*, 12168/3/05 REV 3, 18 November 2005: especially recommendations 1, 2, and 4.

The successive statutes enacted have provided for a specialisation of offences and of the enforcement apparatus.

17.2.2.1 Terrorist Offences

The specialisation of counterterrorism criminal law first appears when considering the pertinent offences. Since the reform of the penal code carried out in 1992, terrorist offences are gathered in Book IV, Title II, articles 421-1 to 422-7 of the Penal code*. The French legislator thus anticipated the requirements of the EU Council Framework Decision of 13 June 2002 *on combating terrorism*[22] by providing for autonomous incriminations of terrorism acts but managed, in the meantime, to keep this penal arsenal within the frames of the principle of legality.[23] Strictly speaking, incriminations are not the result of dispensatory legislation, but terrorism offences consist of a combination of common criminal offences, defined in the Penal code, and a specific *means rea* consisting in the aggravated specific motive of being "committed intentionally in connection with an individual or collective undertaking the purpose of which is seriously to disturb law and order through intimidation or terror".[24] It allows applying the case law relating to the definition of the constituent elements of the *actus reus* of these offences to terrorist offences.

Most of the acts of terrorism are defined in article 421-1,[25] whereas article 421-2 aims at acts of environmental terrorism. Article 421-2-2 prohibits knowingly taking part in the financing of a terrorist organisation[#]. The offence defined in article 421-2-1 deserves to be particularly mentioned. It provides for an autonomous criminalisation of the participation to a criminal group in relation with a terrorist undertaking, which is aimed to anticipate the State reaction and prevent terrorist attacks by intercepting the

---

* Y. Mayaud, *Terrorisme*, Rep. pén. Dalloz, 1997, n°6-80; J.-M. Gonnard, *Terrorisme-Art. 421-1 à 422-5*, Jurisclasseur Droit pénal, 1994; J. Alix, *Terrorisme et droit pénal - Etude critique des incriminations terroristes*. Thèse pour le doctorat en droit, Dir. G. Giudicelli-Delage, Université de Paris 1 Panthéon-Sorbonne, 2008

[22] Articles 1–5 and 7–8, 2002/475/JHA, OJEC L164, 22nd June 2002, p. 3.

[23] Conseil Constitutionnel, Décision n° 86-213 DC, 3rd September 1986, Rec. p. 120.

[24] H. Labayle, *Terrorisme et droit communautaire*, Cour de cassation, cycle droit européen 2007, 8ème conférence, 12 novembre 2007.

[25] Wilful attacks on life and on the physical integrity of persons, abduction and unlawful detention, hijacking of means of transport, theft, extortion, destruction, defacement and damage, computer offences, offences committed by combat organisations and disbanded movements, production or keeping of machines, dangerous or explosive devices, purchase, keeping, transport, or unlawful carrying of explosive substances or of devices made with such explosive substances; detention, carrying, and transport of weapons and ammunition; designing, production, keeping, stocking, purchase, or sale of biological or toxin-based weapons; developing, producing, stocking, and use of chemical weapons and on their destruction, money laundering, and insider trading.

[#] Ordonnance n°2009-104 du 30 janvier 2009 *relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et de financement du terrorisme*, JORF, 31st January 2009, p. 1819.

criminal process at the preparatory stage.[26] The sentences incurred by people who commit acts of terrorism previously listed are detailed in articles 421-3 to 421-6. Since 1986, custodial sentences have been constantly aggravated, making them particularly severe, often closer to the *maxima* provided by the French criminal sentences scale.

Chapter II contains the Miscellaneous and Supplemental. Articles 422-1 and 422-2 respectively deal with the exemption or reduction by half of punishment awarded to criminal turned informers.[27] Articles 422-3 and 422-4 enumerate additional penalties incurred whereas article 422-5 provides for legal persons criminal liability. Articles 422-6 and 422-7 provide for the complementary penalty of confiscation of properties. Finally, since the *loi* n° 95-125 of 8 February 1995, the statute of limitation periods for prosecuting acts of terrorism or enforcing sentences imposed are postponed, de facto implying the statute of limitation has become almost theoretical regarding such offences.

17.2.2.2 The Enforcement Apparatus

The specialisation of the counterterrorism enforcement apparatus proceeded from both (1) a rationalisation of the use of the administrations involved according to their particular capacities and (2) in the granting to these services of powers aimed to meet the necessities of the fight against such particular forms of criminal activities. Again, the legislator managed to implement an appropriate State response without resorting to exceptional legislation.

(1) Rationalised use of security forces. As regards the forces involved, the counterterrorism structure provides for a combination of the capacities of military and civil administrations.

The involvement of military forces in counterterrorism[28] comes from the provisions of the ordinance of 7 January 1959,[29] which states that military forces are in charge of maintaining the security and the integrity of the French territory at any time, in any circumstances, and against any form of aggression. Nonetheless, except in situations of state of siege, they are not allowed to carry out acts of judicial police.

---

[26] J. Shapiro and B. Suzan, *The French Experience of Counter-terrorism*, Survival, vol. 45, n° 1, Spring 2003, p. 82; L. Bonelli, *Les caractéristiques de l'antiterrorisme français:* "*Parer les coups plutôt que penser les plaies*", in D. Bigo, L. Bonelli et T. Deltombe (dir.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, pp. 170–172 and 184–185. For a critical point of view, see: Human Rights Watch, *La Justice court-circuitée–Les lois et procédures antiterroristes en France*, Report 1-56432-350-1, July 2008, pp. 20–61

[27] This provision satisfies the requirements of article 6 of the EU Council framework decision of 13th June 2002 *on combating terrorism*, above mentioned.

[28] See: E.-P. Guittet, *L'implication de l'armée dans la lutte antiterroriste: le cas français*, in D. Bigo, L. Bonelli et T. Deltombe (dir.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, pp. 188–193.

[29] Ordonnance n° 59-147 du 7 janvier 1959 *portant organisation générale de la défense*, JORF, 10 janvier 1959, p. 61.

Following the Algerian war experience, which has proved a disaster for the international image of France, French authorities now show reluctance to entrust military forces with policing missions. Apart from the gendarmerie,[30] the involvement of military forces in the fight against terrorism is therefore rather limited and precisely confined with a view to complete the activity of civil forces by providing them with specific capacities only possessed by military forces. Nonetheless, this contribution cannot be neglected and it is now part of the implementation of the doctrine of globalisation of security, integrated by the government following 9/11.[31]

According to the ministry of Interior,[32] this contribution is threefold. First, soldiers take part in the patrols set up according to the plans of prevention of the terrorist risk on the national territory (Vigipirate, Biotox, and Piratox). Second, the collection of intelligence outside the national frontiers is entrusted to two army services: the *Direction Générale de la Sécurité Extérieure* (DGSE)[33] and the *Direction du Renseignement Militaire* (DRM).[34] The French government associates these two services in external operations[35] with a view to sustain return in internal security. In addition, the DGSE has through history developed satisfactory networks in the Middle East and the Maghreb, which proved useful to prevent terrorist attacks and, as a consequence, it is now represented within UCLAT. Third, in case of an emergency situation resulting from a terrorist attack, military forces could be engaged either to restore law and order or to deal with particular situations, such as nuclear or biological attacks, that they are the only forces trained and equipped to face.[36]

Besides the involvement of military forces, which remains anecdotal, the policing of counterterrorism is mainly entrusted to specialised services within the police forces.

The fight against terrorism is mainly left in the care of two national police services, namely the *Direction Centrale du Renseignement Intérieur* (DCRI)[37]

---

[30]Which, although a military status force, is now placed under the authority of the Interior Minister and is subsequently in charge of similar missions as those carried out by the National Police (Projet de loi n°499 *portant dispositions relatives à la gendarmerie nationale*, 21st August 2008; currently under passing: adopted by the National Assembly on 7th July 2009).

[31]J.-J. Gleizal, *Sécurité et globalisation*, Revue de Sciences criminelles 4/2004, pp. 952–953.

[32]Conseil des ministres, press release, 26th May 2004, *Droit pénal, n° 7/2004, p. 5, alertes n° 28.*

[33]External Security General Direction. Article 3, Décret of 2nd April 1982, JORF, 4th April 1982, p. 1034.

[34]Military Intelligence Direction; see: M. Garrigos, *Les aspects procéduraux de la lutte contre le terrorisme – Etude de droit interne et de droit international*, Thèse de doctorat, Université de Paris I – Panthéon Sorbonne, 2004, pp. 130–131.

[35]Either military or peace keeping and crisis management operations launched either under EU common foreign and security policy or UN mandates.

[36]Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006, pp. 61–63.

[37]Internal Intelligence Central Direction; Décret n° 2008-609 du 27 juin 2008 *relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur*, JORF 28th June 2008, text n° 4.

and the *Sous-direction Anti-terroriste de la Direction Centrale de la Police Judiciaire*.[38]

Since March 2008, the former *Renseignements Généraux* (RG)[39] and *Direction de la Surveillance du Territoire* (DST)[40] are merged within the *Direction Centrale du Renseignement Intérieur* set up to improve the coordination and efficiency of the French police intelligence.[41] As far as the fight against terrorism is concerned, this fusion must be approved because it allows combining the territorial network developed throughout the country by the RG with the professional expertise of the DST.

The enforcement of counterterrorism policing activities is mainly carried out by the Anti-Terrorism Under-Direction of the DCPJ. This unit works closely with the specialised section of Paris prosecution service and the specialised squad of investigating judges. Officers of this force enjoy a nation-wide jurisdiction and are

[38] Anti-terrorism Under-Direction of the Central Direction of the Judicial Police, formerly the DNAT (Anti-Terrorism National Division). Arrêté du 19 mai 2006 *relatif aux missions et à l'organisation en sous-directions de la direction centrale de la police judiciaire et portant création de services à compétence nationale*, JORF, 2nd June 2006, articles 5 and 13.

[39] Police General Intelligence Service. This powerful domestic intelligence agency of more than 4,000 police officers had built up over the years an extensive and effective system of population monitoring (O. Touchot, *Etude comparée des législations antiterroristes en France, au Royaume-Uni et aux Etats-Unis*, Thèse de doctorat, Université de Paris II – Panthéon Assas, 2004, p. 66). In the early 1990s, the Government has redefined their activities (Décret n° 95-44 of 16th January 1995 *portant création de la Direction centrale des Renseignements Généraux*, JORF, 17th January 1995, p. 836, article 3; Arrêté du 6 novembre 1995 *relatif à l'organisation et aux missions de la direction centrale des renseignements généraux et de ses services déconcentrés*, JORF 8th November 1995 p. 16367). The activity of the RG has been turned to the fight against potential national terrorist activities (M. Le Fur, *Rapport n° 3363 sur le projet de loi de finances pour 2007, annexe 30* "*sécurité*", Assemblée nationale, octobre 2006). Officers of the RG are not habilitated to undertake judicial police acts.

[40] Surveillance of the Territory Direction. Until the end of the Cold War, the DST was mainly concerned with activities of foreign agents on French territory (Décret of 22nd December 1982 *fixant les attributions de la Direction de la Surveillance du Territoire*, JORF, 26th December 1982, p. 3864, articles 1 and 2). The disappearance of the communist bloc allowed the increasing importance of counterterrorism activities and the appointment of more agents. The DST Fight against International Terrorism Under-direction, mainly in charge of the fight against radical Islamism and other forms of international/cross-borders terrorism, was set up in 1989 (L. Caprioli et J.-P. Pochon, *La France et le terrorisme international – Les racines historiques et organisationnelles du savoir policier*, Cahiers de la Sécurité intérieure, n° 55, 1/2004, p. 163). The distinctive feature of DST officers is that they are both intelligence and judicial police officers. It has allowed setting up an operational and analytical interface between the force and the antiterrorism-investigating magistrates. Furthermore, it facilitates the use of intelligence, even collected through international networks, as evidence in Court, satisfying thus the EU requirements (Council of the European Union, Presidency in co-operation with the Counter Terrorism Coordinator, *Final report on the Evaluation of National Anti-Terrorist Arrangements: Improving national machinery and capability for the fight against terrorism*, 12168/3/05 REV 3, 18 November 2005: Recommendation 10).

[41] L. Bonelli, *Les caractéristiques de l'antiterrorisme français:* "*Parer les coups plutôt que penser les plaies*", in D. Bigo, L. Bonelli et T. Deltombe (dir.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, pp. 176–187.

addressees of all information collected by other services that interest the operational aspects of the fight against terrorism. They are in charge of both actions of preventive enforcement to avoid the commission of acts of terrorism and of post-attacks investigations. This unit is also involved in international co-operation and takes in foreign counterterrorism liaison officers.

On the other hand, two specialised intervention units can be deployed to undertake operations which imply specific operational capacities, namely the *Groupe d'Intervention de la Gendarmerie Nationale*[42] and its equivalent within the National Police, the RAID.[43] These groups enjoy an operational competence both on interventions to end taking of hostages' operations and hijackings, and on operational investigations requiring specific competences (surveillance in hostile environments, arrest of highly violent groups…).[44] Furthermore, all other internal security forces can accessorily be associated to the fight against terrorism when their specific areas of competence are interested and/or required (mainly the Central Direction of the Borders Police and the Customs). All these services are legally bound to report to the specialised services intelligence on terrorism issues or cases they might collect in their day-to-day practice, and they can be associated to some enforcement operations.

Apart from the police apparatus, magistrates involved at all levels of the penal process are also specialised.

Although the 1986 statute did not establish a special court to deal with terrorist cases, it provides that the Paris Tribunal of Grande Instance enjoys a primary nation-wide jurisdiction to deal with terrorist cases. It establishes within Paris Tribunal's bosom a specific section of the Public Prosecution Service, the *Service Central de Lutte Antiterroriste*,[45] made up of eight dedicated public prosecutors and a specialised squad of investigating judges, known as the "*juges antiterroristes*"[46]. The establishment of equivalent institutions in all member States is

[42] National Gendarmerie Intervention Group.

[43] Research, Assistance, Intervention, Deterrence.

[44] M. Garrigos, *Les aspects procéduraux de la lutte contre le terrorisme – Etude de droit interne et de droit international*, Thèse de doctorat, Université de Paris I – Panthéon Sorbonne, 2004, pp. 141–144.

[45] Fight against Terrorism Central Service – SCLAT – formerly known as the *14ème section du Parquet de Paris*.

[46] On request of the President of the Republic (Speech at the *Audience solennelle de rentrée de la Cour de cassation*, 7th January 2009), a bill is currently under consideration that should put forward the disappearance of the French investigating judge (Comité de réflexion sur la justice pénale, *Rapport d'étape sur la phase préparatoire du procès pén*al, 6th March 2009; P. Conte, *Les propositions du pré-rapport du comité de réflexion sur la justice pénale*, Droit pénal, 6/2009, *Etudes*, n°11). The investigation of criminal cases would be entirely entrusted to public prosecutors and, under their control, to police officers, whereas investigating judges would become "judges of the investigation", in charge of controlling the legality of inquiries and of authorizing the enforcement of coercive police powers.

recommended by the experts of the European Union.[47] The specialisation of investigating magistrates importantly contributed to improving the efficiency of the French counterterrorism apparatus,[48] after the antiterrorist magistrates started to work closer with the DST at the end of the 1990s. Their direct collaboration allows avoiding interference in the transformation of preventive and/or preliminary investigations into judicial ones.[49]

Besides, apart from the provisions of article 706-17, article 706-25 CPC provides for a specialised Assize Court, set up only with professional judges, to try terrorism cases in order to prevent pressure and threats to members of juries. The Constitutional Council has validated this provision[50] and the Criminal chamber of the Court of Cassation has stated that the procedure applied by this jurisdiction respects the rights of the defence.[51]

The granting to specialised administrations of powers aimed to meet the necessities of the fight against terrorism is the other expression of the specialisation of the penal apparatus.

(2) Enforcement of specific powers. France only managed to preserve a judicial treatment of terrorism cases through a regular adaptation of the criminal procedure rules. The statute of 9 September 1986, which is the foundation stone of antiterrorism legislation, has thus been completed and adapted by five subsequent statutes[52] since, which have all increased and strengthened the powers granted to the administrations vested with the prevention, investigation, and prosecution of terrorism cases. Counterterrorism enforcement forces can obviously resort to the already substantial powers of investigation vested with French police officers.[53] Furthermore, taking the argument of the necessities of the fight against terrorism, the French governments have constantly extended the area of application of police powers together with providing the forces with specific prerogatives aimed to fight terrorism as a type amongst others of organised crime. As a result, an important set of powers is available to police forces in charge of counterterrorism.

---

[47] Council of the European Union, Presidency in co-operation with the Counter Terrorism Coordinator, *Final report on the Evaluation of National Anti-Terrorist Arrangements: Improving national machinery and capability for the fight against terrorism*, 12168/3/05 REV 3, 18 November 2005: Recommendation 3.

[48] J. Shapiro and B. Suzan, *The French Experience of Counter-terrorism*, Survival, vol. 45, n° 1, Spring 2003, p. 82.

[49] The dual competence of some DCRI officers permits enforcement operations led under the authority of the investigating magistrate by the officers of the force who have gathered intelligence materials. Furthermore, it undeniably facilitates the task of prosecution authorities because investigating magistrates do not hesitate to deliver rogatory commissions to change information collected by intelligence services into evidence acquired through a judicial investigation, which is admissible in court.

[50] Decision n° 86-213 DC, 3rd September 1986.

[51] Crim. 7th May 1987, *Bull. crim*. n° 186; confirmed by Crim. 24th November 2004, comm.. D.-N. Commaret, Revue de sciences criminelles, 2/2005, p. 332.

[52] See p. 2, footnote 7

[53] Articles 53 to 78-6 CPC.

Although in a White Paper released in 2006, the Government insists that the French counterterrorism system does not watertight compartmentalise between prevention and repression,[54] the counterterrorist framework relies on a twofold strategy, distinguishing strictly preventive measures (a) from investigation powers (b).

(a) Preventive measures. The main preventive procedures are the so-called "Pirate" plans.[55] These are protection governmental plans aimed to prevent terrorist attacks and implemented by the CILAT. They consist of police and military passive surveillance of public and sensitive areas (airports, train stations, public transports, ports, nuclear centrals…).[56]

The 2006 statute has considerably increased the area of passive surveillance by extending the legal authorisation, and sometimes obligation, to install video surveillance cameras in every place where acts of terrorism are likely to be carried out to prevent these acts from happening (streets, public places, and sensitive private places).[57] It further enables Police, Gendarmerie, and Customs and Excise Officers to use fixed or mobile automatic monitoring devices for the purpose of identifying vehicles by photographing the occupants.

The prevention of terrorism also draws from statutory provisions aimed to control aliens suspected of terrorism from entering or remaining on French territory. French legislation was amended in 2003[58] to reinforce border controls and extent the capacity of the Ministry of Interior's administration to expel or deport from French territory, under the control of the administrative judge, people suspected of being involved in terrorism or who might threaten law and order.[59]

---

[54] Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006, p. 47.

[55] The most famous is the "Vigipirate" plan which has been set up by a ministerial instruction of the SGDN of 7th February 1978; see: E.-P. Guittet, *Military activities within national boundaries: the French case*, Cultures et Conflits, Illiberal Practices of Liberal Regimes: the (in)security games, L'Harmattan, 2006, pp. 160–162.

[56] Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006, pp. 69–70.

[57] Although academic studies carried out in France on the issue conclude that video surveillance has a limited effect on delinquency (see, for example, F. Ocqueteau, *Cinq ans après la loi "vidéo-surveillance" en France, que dire de son application?*, Cahiers de la Sécurité intérieure, n° 43, 1/2001, p. 101), the fact that the terrorists who have perpetrated the bomb attacks in the London tube during the summer 2005 have been identified thanks to pictures taken by the security cameras probably played an important role on the enactment of this provision (C. Lienhard, *La loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et au contrôle frontalier*, JCP G, n° 12, 22 mars 2006, p. 527).

[58] Loi n° 2003-1119 of November 26th 2003: articles L511-1 and L521-1 to L523-1 of the Aliens Entry and Stay and Asylum Right Code.

[59] J.-F. Gayraud et D. Sénat, *Le terrorisme*, PUF, coll. Que sais-je?, 2ème éd., 2006, pp. 99–100; Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006, p. 57. The State Council has stated that such a deportation is not a sanction, which would require a judicial procedure, but "a police act exclusively aimed to protect law and order and public security" (CE, 20 janvier 1988, *Ministre de l'Intérieur c/ Elfenzi*, Rec. Lebon, p. 17).

(b) Investigation powers. As regards investigation powers, current French legislation is characterised by the integration of counterterrorism procedural rules within the definition of procedural rules applicable to a larger number of related offences, i.e. to investigation and prosecution of the wide category of "organised crimes".[60]

As a result of the successive legislative reforms passed between 1986 and 2006, when involved in either administrative or judicial counterterrorism investigations, police officers are, usually on public prosecutor or investigating judge authorisation, allowed to enforce the following powers[61]:

- Administrative identity controls and vehicles inspections and searches[62]
- Night coercive searches including, under specified circumstances, searches in inhabited dwellings[63]
- Entire national territory surveillance[64]
- Specific procedures relating to the protection of witnesses[65]
- Infiltration[66]

---

[60] The statute n° 2004-204 of 9th March 2004 marks the evolution of the commitment of the French legislator to keep the fight against terrorism within the ordinary criminal justice system and gives the feeling that the French legislator skilfully manoeuvred to, in the meantime, play a sleight of hand to keep counterterrorism within ordinary criminal procedure and exploit counterterrorism to increase the area of application of dispensatory police powers to a wide range of offences. The statute first provides for a sweeping up definition of organised crime, gathering almost 20 forms of criminal offences (Articles 706-73 and 706-74 CPC). The adaptation of the ordinary rules of criminal procedure is justified by the pretended intrinsic seriousness of the incriminated acts and by technical reasons such as the inherent complexity of the cases (M. Danti-Juan, *Les adaptations de la procédure*, Revue pénitentiaire et de droit pénal, n° 4/2003, p. 725). Regarding the subject matter of this study, article 706-73-11° CPC reads "the procedure applicable to the inquiry, prosecution, investigation and trial" of felonies and misdemeanours that constitute acts of terrorism is subject to the provisions of articles 706-80 to 706-106 of the Criminal procedure code. The powers thus given noticeably increase the coercive character of the proceedings, giving rise to proactive investigations (M. Schwendener, *Une police aux pouvoirs d'enquête renforcés*, Actualité juridique pénal, n° 6/2004, p. 228).

[61] S. Guinchard and J. Buisson, *Procédure pénale*, 4th ed, LexisNexis-Litec, 2008, pp. 523–542 and 559–576; F. Desportes and L. Lazerges-Cousquer, *Traité de procédure pénale*, Economica, 2009, pp. 1369–1579.

[62] Articles 78-2 to 78-2-4 CPC, J. Buisson, *Des contrôles d'identité aux fouilles requises*, Procédures, mars 2002, p. 6; P. Gagnoud, *Fouilles de véhicules automobiles; brèves remarques sur les principaux apports de la loi du 18 mars 2003*, Gazette du Palais, Recueil mai-juin 2003, p. 1623.

[63] Articles 706-89 to 706-94 CPC.

[64] Article 706-80 CPC.

[65] Articles 706-57 to 706-63 CPC; J. Danet, *De la procédure à la répression de la criminalité organisée, ou laquelle est l'instrument de l'autre?*, Actualité juridique pénal, n° 5/2004, p. 192.

[66] Articles 706-81 to 706-87 CPC. Although the provisions of article 706-85 call for concern, these provisions should be welcomed because they extend a procedure that was previously limited to the fight against drug trafficking to counterterrorism. Besides, taking into account the reservation of interpretation made by the Constitutional Council (Decision n° 2004-492 DC, §.6), they might lead to the reversal of the previous case-law of the Criminal chamber of the Court of Cassation, which admitted infiltration operations to be started and carried out sometimes before informing the magistrates supposed to control them (Court of Cassation, Criminal chamber, 1st April 1998, *Bull. crim*. n° 124).

- Police custody for up to 6 days[67]
- Administrative and judicial interceptions of communications[68]
- Taping of audio recording and visual images in specified vehicles and private places[69]
- Witnesses/suspects interviews in a territory belonging to another State[70]

Furthermore, taking argument of the need to improve police capacities in the fight against terrorism, the legislator has legalised existing police and gendarmerie databases and the subsequent processing of data collected.[71] Judicial police databases are further set up into centralised and national bases available for consultation by a very important number of police and gendarmerie officers but also by services not involved in judicial police missions, but which may be interested in getting access to police databases.[72] In addition, a new database, interoperated with the SIS and the wanted persons' database, with a view to collecting personal data (PNR) on non-EU citizen international travellers has been created. Finally, the government

[67] Article 706-88 CPC; See: A. Giudicelli, *La garde à vue après la loi n° 2004-204 du 9 mars 2004*, Actualité juridique pénal, juillet-août 2004, p. 265; H. Vlamynck, *Le policier et la garde à vue: remarques et interrogations*, Actualité juridique pénal, juillet-août 2004, p. 269.

[68] Articles 100 to 100-7 and 706-95 CPC; See: M. Garrigos, *Les aspects procéduraux de la lutte contre le terrorisme – Etude de droit interne et de droit international*, Thèse de doctorat, Université de Paris I – Panthéon Sorbonne, 2004, pp. 584–590. Commission Nationale de Contrôle des Interceptions de Sécurité, *17ème rapport d'activité* - 2008, La Documentation française, 2009.

[69] Articles 706-96 to 706-102 CPC. These provisions must be welcomed because they frame with legal boundaries a practice already admitted by the Court of Cassation (Crim. 23rd November 1999, Droit pénal, juin 2000, n° 82, p. 23). Furthermore, through recent decisions, the Criminal Chamber of the Court of Cassation has confirmed the unlawfulness of the implementation of these provisions without the prior authorisation of an investigating judge (Crim. 21st March 2007, Recueil Dalloz 2007, Actualité jurisprudentielle, p. 1204, comm. A. Darsonville), Rev. sc. crim. 3/2008, p. 655, com. J. Buisson) and defined their field of enforcement (Crim. 27th February 2008, Rev. sc. crim. 3/2008, p. 659, com. J. Buisson; Crim. 9th July 2008, A.J. Pénale 10/2008, com. J. Lasserre-Capdeville; Crim. 13th November 2008, Dr. pénal 3/2009, com. n°43, A. Maron and M. Haas).

[70] Article 18 subsection 5 CPC. The legal efficiency of this provision is nonetheless questionable (see: L. Desessard, *Contribution au débat sur l'article 18 alinéa 5 du code de procédure pénale*, Revue pénitentiaire et de droit pénal, n° 2/2006, p. 443; M. Massé, *Retour sur l'article 18, alinéa 5, du Code de procédure pénale*, Revue de sciences criminelles, 2/2007, pp. 387–392).

[71] The Loi n° 2003-239 of 18th March 2003 provides habilitated and specially designated agents with administrative police power access to personal data contained in the ministry of Interior services databases and in all national/administrative or private databases "for the needs of prevention and repression of terrorism". The law allows preventive administrative investigations to be carried out outside any possibility of control/claim from the person targeted. According to a recent report, 58 police databases are currently operated in France (Groupe de contrôle des fichiers de police et de gendarmerie, *Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés – Rapport remis au ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales,* 10th December 2008, La Documentation française, 2009). See, also: M. Delmas-Marty, *Libertés et sûreté dans un monde dangereux - Radicalisation des procédures de contrôle*, Cours au Collège de France, Chaire Etudes juridiques comparatives et internationalisation du droit, 3rd February 2009

[72] Such as the services in charge of the control of aliens.

has recently made official and legalised the former RG and DST databases and increased the power to file suspects in those databases.[73]

In addition, the 2006 statute allows pre-trial detention of 3 years for terrorist misdemeanours.[74] The rules governing the trial of terrorists do not show any specificity and the common rules are applied.

The cursor of legally authorised infringements with fundamental rights is thus globally pushed further, whatever the nature of the investigations carried out. Very intrusive coercive powers are provided to police officers when they investigate terrorism crimes. This has led a commentator to describe the current state of the law as a "counterterrorism administrative police regime".[75]

The Constitutional council has nonetheless ruled that these specific procedural means do not "excessively violate individual freedom, since the scope of these provisions extends to investigations into specific offences imposing special investigations on account of their seriousness and complexity and because the provisions challenged are drafted in sufficiently clear and precise terms to avert the risk of arbitrary action".[76]

The French model should be pondered. It is now a shared conviction among occidental democracies that terrorism constitutes a threat that, to be neutralised, requires an exceptional involvement of governments and security services. On the other hand, it is well documented that the action of security services is primarily governed by efficiency rather than by compliance with legislation.[77] It is even truer when the Executive requires immediate results. Therefore, the law must be adapted to provide security forces with the prerogatives necessary to fulfil their mission and prevent, as much as possible, that police forces argue that the lack of procedural means causes them to resort to illegal practices.

---

[73] Décret n° 2008-631 du 27 juin 2008 *portant modification du décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux et du décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978* et Décret n° 2008-632 du 27 juin 2008 *portant création d'un traitement automatisé de données à caractère personnel dénommé* "*EDVIGE*", JORF 1st July 2008, textes n° 2 et n° 3. Décret n°2008-1199 du 19 novembre 2008 portant retrait du décret n°2008-632 du 27 juin 2008 *portant création d'un traitement automatisé de données à caractère personnel denommé "EDVIGE", JORF*, 20th November 2008, p.17718; Projet de Décret *portant création de l'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique*, September 2008, currently under passing.

[74] Which seems consistent with the European Court case law; see: ECHR, *Chraidi v. Germany*, 26th October 2006. Nonetheless, The Human Rights Committee of the United Nations has recently expressed its concern regarding the length of pretrial detentions in terrorism cases (Comité des Droits de l'Homme des Nations Unies, *Examen des rapports soumis par les Etats parties conformément à l'article 40 du Pacte – Observations finales du Comité des droits de l'homme - France*, CCPR/C/FRA/CO/4, 22 juillet 2008, §.15).

[75] P. Chrestia, *La loi du 23 janvier 2006 relative à la lutte contre le terrorisme: premières observations*, Recueil Dalloz, n° 21, 2006, p. 1409.

[76] Decisions of 2004 and 2006, *infra*.

[77] See, for example: D. Montjardet, *Ce que fait la police – Sociologie de la force publique*, La Découverte, coll. textes à l'appui/série sociologie, 1996.

It seems the French legislator has managed to find an interesting balance. By adapting criminal law and procedure to the requirements of the fight against terrorism, it has provided its security services with legal tools that certainly contribute to the French antiterrorism system now being regarded as effective, while safeguarding its overall consistency with the provisions of the European Convention on Human Rights.[78] Furthermore, this approach has allowed curbing of the temptation to resort to exceptional or extra-judiciary management of terrorism.[79] To that extent, it is quite emblematic of the ambition of the European Union to keep the fight against terrorism outside a military apprehension and to avoid the two pitfalls that frame the social reaction to terrorism: pusillanimity and unlawfulness.[80]

Nonetheless, if the French system is certainly interesting, it can hardly be regarded as a model because, aside of the achievements above presented, it carries weaknesses that should not be neglected. Piercing the veil of appearances leads to notice that the French criminal justice system is also affected by the decline of the protection of fundamental rights and civil liberties consubstantial to the worldwide prevailing conception of the requirements of the fight against terrorism but also that, more than in some of the other democratic States, the checks and balances of counterterrorism policy are deeply impaired.

17.3 Weaknesses of the French Antiterrorism Framework: The Protection of Fundamental Rights and Civil Liberties

Primacy given to security since 1986 involves a consecutive strengthening of the role and prerogatives of the Executive apparatus and a concomitant restriction to individual rights and freedom. However, in a democratic State, the subsequent increase of internal security forces legally conceded capacity to infringe fundamental rights and civil liberties should be accompanied by a correlative strengthening of the control exercised on the enforcement of these intrusive powers. The analytical assessment of the current French counterterrorism system shows that, far from this ideal, the increase of the administrative threat on civil liberties is coupled with a substantial renouncement of the protection of fundamental rights. This situation can cause legitimately worry as the deficiencies of control institutions often responds to the arrogance of Executive bodies.

---

[78] The French counterterrorism system is thus consistent with the *Guidelines on human rights and the fight against terrorism* adopted by the Committee of Ministers of the Council of Europe on 11 July 2002 at the 804th meeting of the Ministers' Deputies (Directorate General of Human Rights, December 2002).

[79] Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006, pp. 117–118.

[80] J. Foyer, *Droit et politique dans la répression du terrorisme en France*, in Mélanges offerts à G. Levasseur, *Droit pénal et droit européen*, Gaz. Pal./Litec, 1992, p. 410.

17.3.1 Arrogance of the Executive Bodies

Despite the wording of article 34 of the French Constitution, the contribution of the Parliament in the working out of the legislation is mainly formal. The French Parliament is "weakened in its political function"[81] and, even if occasionally it manages to restrict the excesses of the Executive, it is not anymore, regarding the definition of criminal procedure rules, a sizeable obstacle to the satisfaction of governmental will,[82] particularly when dealing with such issues as national security and the fight against terrorism.[83] The government and the Administration thus occupy the crucial role in the definition of penal policy. Not surprisingly, the fight against terrorism is therefore subjected to their agenda, which, regarding this issue, is structured around seeking efficiency for the penal apparatus. Thus, the protection of civil liberties is an accessory concern, often perceived, or even presented, as a brake to providing security. The necessities of the fight against terrorism have been exploited by successive French governments to increase widely police powers when police forces argue the requirements of their efficiency to shield their activities from independent controls.

17.3.1.1 The Fight Against Terrorism as a Pretext to Increase Police Powers

In an outstanding article released in 2002, D. Bigo expressed his anxiety that France "which has managed to overcome difficulties which directly affected it in 1986 and 1995, by enforcing measures and a legislation appropriated to the situation" could enter, following 9/11, into a legislative and normative build-up that could result in using terrorism as a "catch-all category" justifying repressive policies in various areas thus giving rise to a "routinisation" of exceptional procedures through the bureaucratic tendency to always return to old law and order solutions.[84] Instead of anxiety, this was just a premonition.

In fact, from the mid 1990s, French governments, whatever their allegiance, have subscribed to law and order policies. This can be briefly explained. Until recently, France has been a Colbertist welfare State, which means that the involvement of the

---

[81] As stated by J. Mekhantar, *Droit politique et constitutionnel*, ESKA, coll. Droit public et sciences politiques, 1997, p. 489.

[82] See A. Delcamp, J.-L. Bergel et A. Dupas, *Contrôle parlementaire et évaluation*, La Documentation française, coll. Les études de la DF, série Institutions, 1995.

[83] As far as counterterrorism legislation is concerned, the recently passed reform of the Constitution (Loi constitutionnelle n° 2008-724 of 23rd July 2008 *de modernisation des institutions de la Ve République*, JORF 24th July 2008, p. 11890) will hardly have any influence as Members of Parliament will certainly not dare to use their new prerogatives to oppose the government's will on such a sensitive issue.

[84] D. Bigo, *L'impact des mesures anti-terroristes sur l'équilibre entre liberté et sécurité et sur la cohésion sociale en France*, in E. Bribosia et A. Weyembergh (ed.), *La lutte contre le terrorisme et les droits fondamentaux*, Nemesis, Bruylant, Coll. Droit et justice n° 34, 2002, pp. 221–227.

government on the overall economy has been important compared with most other occidental countries. Nonetheless, the combination of the influence of the European Union and of globalisation has drastically limited its influence on these issues and French Executives have proved unable for longer than 40 years to curb the economic crisis. The subsequent impoverishment of the country has influenced France's diplomatic and military importance on the international stage, driving governments to renounce the doctrine of independence to subscribe to the European Union primary competence in these fields. Therefore, internal security remains the last kingly prerogative on which French governments enjoy autonomous capacities. In the meantime, the security issue has been exploited for 20 years for electoral purposes, giving rise to great expectations within the population. Nonetheless, as in every liberal State, the influence of criminal law and procedure on delinquency is marginal. Therefore, to satisfy the expectations they have caused, Executives have no alternative but to carry on legislating in this field just to show a maintained political voluntarism.[85] The trouble they face is that the definition of criminal procedure is framed by superior norms that limit the capacities to provide indefinitely administrations in charge of policing with coercive and/or intrusive power. In early 2000, the French governments experienced a difficult situation, being, in the meantime, compelled for the abovementioned motive to carry on legislating and unable to increase further police powers without violating international and constitutional constraints. The fight against terrorism thus provided them with the opportunity to pass over this difficulty.[86] Being an exceptional form of criminality, both in the means used and in its purposes, terrorism justifies the enforcement of specific prerogatives to curb it.

However, the legitimation of the fight against terrorism does not extend to the fight against all forms of criminality. That is precisely where the French legislators' attitude calls for criticism. Our argument is that, although police powers enforced by the successive statutes passed since 2001 are legitimate to fight international terrorism, the French government has exploited this issue to increase globally police powers and implement a dispensatory criminal procedure that, instead of contributing to the protection of fundamental rights by providing the tools required to curb terrorism, is now a threat to the individual freedoms of the overall French population.

The current legislation is the result of a two-step evolution[87]. The move towards a reinforcement of the law and order orientation of French criminal procedure was initiated by the 15 November 2001 and the 18 March 2003 statutes, and established by the 9 March 2004 and the 23 January 2006 statutes.

Between 2001 and 2004, the fight against terrorism has been used to justify the implementation of some limited dispensatory procedures. The fight against terrorism drove control institutions to admit that the enforcement of some police prerogatives

---

[85] J. Danet, *Cinq ans de frénésie pénale*, in L. Mucchielli (dir.), *La frénésie sécuritaire – Retour à l'ordre et nouveau contrôle social*, La Découverte, coll. sur le vif, 2008, pp. 19–29.

[86] D. Hermant et D. Bigo, *Les politiques de lutte contre le terrorisme: enjeux français*, in F. Reinares (dir.), *European democracies against terrorism – Governmental policies and intergovernmental co-operation*, Ashgate Pub. Co., 2000, p. 75.

[87] *E. Rubi-Cavagna, L'extension des procédures dérogatoires,* Rev. sc. crim. 1/2008, p. 23

they had previously found illegal was justified by the particularities of the fight against terrorism.[88] It has thus implied a shifting of the cursor of legality. Then, in 2004, the legislator turned the definition of terrorism to a form of organised crime. Doing so, it has integrated it as a type of criminality amongst other forms of delinquency of identical seriousness. The legislator managed thereby (1) to extend the area of implementation of dispensatory criminal procedure rules, specially designed to fight terrorism, to various other forms of delinquency, and (2) having pushed the cursor of legality further in the name of the fight against terrorism, to further pass on a wide range of coercive tools, which could as a consequence be implemented to fight all of the types of organised crime enlisted.[89] To that extent, France is an outstanding example of the hegemonic tendency of counterterrorism dispensatory proceedings.

The new prerogatives allotted carry an undeniably threatening potential for civil liberties and individual rights.[90] Their implementation should have therefore been subjected to the requirements of the Rule of Law in a democratic society emphasised by the European Court of Human Rights, i.e. legality, necessity, proportionality, and submission to the due process of justice. The legality of the disputed provisions is unquestionable. Their necessity and proportionality are not arguable when considering the fight against terrorism. However, the issues of necessity, proportionality, and due process become more challengeable when considering enforcement conditions of these prerogatives for which the legislator has provided. The extension of the area of application of measures enacted to fight terrorism surpasses the reasons that legitimated the infringements to civil liberties and tend to constitute a set of parallel criminal procedure rules enforceable outside of the boundaries of the principles of equality of arms. In addition, the French government considers that the strengthening of the repressive apparatus should also be worked out through a restriction of the judicial control exercised on police activities. It has therefore considerably increased the area of application of proactive administrative police powers and brought in more situations in which either prosecutors or liberty and custody judges are substituted for the natural judge or the intervention of magistrates is delayed.[91] Furthermore, no provision within the law reserves the implementation of the prerogatives enacted in articles 706-80 to 706-106 to offences of some gravity. If it is legitimate that police forces may enforce extraordinary procedural

---

[88] See, *infra*.

[89] A. Mac Leod, *Insécurité et sécurité après les évènements du 11 septembre: France et Grande-Bretagne*, in S.-J. Kirschbaum (dir.), *Terrorisme et Sécurité internationale*, Bruylant, coll. Etudes stratégiques internationales, 2004, p. 215.

[90] Y. Bisiou, *Enquête proactive et lutte contre la criminalité organisée en France*, in M.-L. Cesoni (dir.), *Nouvelles méthodes de lutte contre la criminalité: la normalisation de l'exception – Etude de droit comparé (Belgique, Etats-Unis, Italie, Pays-Bas, Allemagne, France)*, Bryulant/LGDJ, 2007, pp. 348–349.

[91] C. Lazerges, *La dérive de la procédure pénale*, Revue de sciences criminelles, chronique de politique criminelle, n° 3/2003, p. 652; J.-L. Lennon, *Les aspects coercitifs et intrusifs de l'enquête préliminaire ou l'effritement de la distinction entre enquête de flagrance et enquête préliminaire*, Droit pénal, étude n° 21, octobre 2007, pp. 17–22; F. Rolin et S. Slama, *Les libertés dans l'entonnoir de la législation anti-terroriste*, Actualité juridique Droit administratif, 15th May 2006, pp. 975–982.

tools to fight criminal organisations or terrorist groups, their implementation to curb ordinary delinquency turns out to be more arguable[92]. Finally, the 2006 statute put the finishing touches on the confusion between prevention and repression, the legislator having taken arguments of the requirements of the fight against terrorism to set up an overall control of population outside of any judicial control.

Apart from the decline of the protection of civil liberties, the limitation of the judicial control on police activities also reveals the importance that police forces have in the elaboration of current French criminal law.

17.3.1.2 Police Forces' Resistance to External Independent Controls

In a democratic state, the activities of police forces are supposedly subordinated to the decisions of the Executive and controlled by the Judiciary. The establishment of security as the central issue of the political debate, and the subsequent governmental adhesion to the doctrine of "penal populism"[93] have modified this situation. It has given rise to a destabilisation of the political process regarding penal matters as legislation is no longer based on ideological grounds but on a *doxa* consisting of the reactive multiplication of bill-posting laws aimed to respond to the successive concerns of the public opinion. As a consequence, motives that used to prevail regarding the enforcement of penal rules have become accessory and the relation to constraints of legality and the influence of experts has been perverted. On the other hand, the dependency on police forces has become prevalent.[94] Thus, no French government can afford to displease the police.

Not surprisingly, police unions did not take much time to realise what perspective such a situation allows and the recurrent claim for a reduction of judicial control on police activities has thus eventually found a positive echo. They have thus managed to get (1) the repeal of most provisions of the 15 June 2000 statute, passed after the condemnation of France for torture in a police station,[95] which were intended to improve the judicial control of police activities; (2) through the reforms passed in 2003 and 2004, the substantial reduction of procedural, particularly judicial, constraints on police investigations; and (3) the suppression of the ad hoc independent commission in charge of the assessment of the respect of human rights by police forces, which will shortly be replaced by an ombudsman in charge of the "rights of the citizens".[96] It means that, apart from a

---

[92] B. de Lamy, *La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (Crime organisé – Efficacité et diversification de la réponse pénale)*, Recueil Dalloz 2004, n° 27, p. 1912–1913.

[93] D. Salas, *La volonté de punir – Essai sur le populisme pénal*, Hachette, coll. Littératures, 2005. See also J.-R. Spencer et N. Padfield, *L'intégration des droits européens en droit britannique*, Rev. sc. crim. 3/2006, p. 539.

[94] G. Sainati et U. Schalchli, *La décadence sécuritaire*, La fabrique, 2007, p. 69.

[95] ECHR, Grand Chamber, *Selmouni v. France*, 26th July 1999, Application no. 25803/94.

[96] Presentation of the draft Constitutional Reform Bill, http://www.elysee.fr/edito/?lang=fr&id=59; Titre XI bis of the French Constitution (article 41, Loi constitutionnelle n° 2008-724 du 23 juillet 2008 *de modernisation des institutions de la Ve République*, JORF July 24th 2008, p. 11890).

limited judicial control, French police forces have succeeded in bringing the level of control exercised on the activities they carry out on French territory to a minimum.

On the other hand, the fight against terrorism implies international co-operation, which is governed by rules that are not defined by French authorities. Nonetheless, police forces have managed, with the implicit agreement of the French government, to escape external controls on their activity. The involvement of the French police within the European co-operation illustrates this assertion.

Although France has ratified the Schengen Agreement 1985, the Application Convention of the Schengen Agreement 1990, and, more recently, the Prüm Convention, French authorities have limited their enforceability on French territory through the adaptation to internal law.[97] On the other hand, they tend to privilege direct bilateral co-operation through intergovernmental agreements signed with all frontier countries.[98] Regarding the fight against terrorism, some procedures adopted within these bilateral agreements have proved most efficient.[99] However, they all allow and promote direct informal co-operation between the forces involved. In practice, the official networks (Schengen or Interpol) are used only to provide the results of the co-operation with apparent legality to allow the prosecution to use them in courts. The situation is not really different regarding the relationship with Europol. In a discussion paper released on 23 November 2007, the UE Counter-terrorism Coordinator points out that, with regard to Europol, "the situation remains largely unsatisfactory for certain Member States".[100] France is one of these States and although Europol puts it forward diplomatically,[101] the reluctance of the French police to transmit information and the lack of involvement of the French police authorities

---

[97] S. Garcia-Jourdan, *L'émergence d'un espace européen de liberté, de sécurité et de justice*, Bruylant, 2005, p. 407 et pp. 486–500.

[98] Accord entre le Gouvernement de la République française et le Gouvernement de la République italienne *relatif à la coopération transfrontalière en matière policière et douanière*, fait à Chambéry le 3 octobre 1997; Accord entre le Gouvernement de la République française et le Gouvernement de la République fédérale d'Allemagne *relatif à la coopération dans les zones frontalières entre les autorités de police et les autorités douanières*, fait à Montdorf-les-Bains le 9 octobre 1997; Traité entre la République française et le Royaume d'Espagne *relatif à la coopération transfrontalière en matière policière et douanière*, fait à Blois le 7 juillet 1998; Accord entre le Gouvernement de la République française et le Gouvernement du Royaume de Belgique *relatif à la coopération transfrontalière en matière policière et douanière*, fait à Tournai le 5 mars 2001; Accord entre la République fédérale d'Allemagne, le Royaume de Belgique, la République française et le Grand Duché du Luxembourg relatif au renforcement de la coopération transfrontalière entre les autorités policières et douanières respectives, fait à Luxembourg le 24 octobre 2008; Regarding police co-operation with the United Kingdom, see O. Cahn, *La coopération policière franco-britannique dans la zone frontalière transmanche*, Thèse de doctorat en droit pénal et sciences criminelles, Université de Poitiers, 2006, vol. 1.

[99] For example: the Franco-Spanish working group – which gathers magistrates and representatives of the police forces and of the intelligence services of both countries – is playing an important role in the operational coordination of the fight against Basque separatist terrorism. The EU Council General Secretariat has suggested the model should be adopted as European best practice.

[100] Council of the European Union, Counter-terrorism Coordinator, *Implementation of the EU Counter-terrorism strategy – Discussion paper*, 23rd November 2007, 15448/07, p. 4.

[101] Europol, *Annual Report 2006*, May 2007, p. 40: "Despite many successes, the French desk remained aware that there was still room for improvement on both sides".

can hardly be denied.[102] On the other hand, in 1971, representatives of national antiterrorist intelligence and enforcement services have, on a US initiative, installed the "Club of Berne".[103] Being entirely informal, this club works outside of any judicial or political control. Not surprisingly, both the DST and the RG have expressed their preference for co-operation through this club rather than through European institutions, and French political authorities have implicitly admitted this.[104]

Now, strong arguments are made by the agencies to justify their hesitation to take part in the European multilateral counterterrorism framework.[105] Nonetheless, apart from these official motives, there is another important reason for the French counterterrorism services' reluctance to comply with Decision 2005/671/JHA and to assign international co-operation within the European framework. Indeed, such compliance would imply services renounce the informal direct co-operation, entirely shielded from judicial control, that they have built for years and that characterise their collaboration.[106]

The subjection of the Executive to counterterrorism police forces' *desiderata* in the definition of criminal procedure rules and the concomitant tolerance for police services' eluding from independent controls allow to conclude that the protection of human rights and civil liberties in counterterrorism investigations is entirely handed down to the a priori control exerted on legislation by the Constitutional Council and to the concomitant and a posteriori control exercised by the judiciary on police activities. Now, regarding antiterrorism, these controls prove extremely benevolent to enforcement forces and therefore unsatisfactory regarding the protection of human rights.

---

[102] For example, the DST shows much reluctance to provide Europol and the Situation Centre (SITCENT) with intelligence they collect, despite the obligations resulting from the Decision 2005/671/JHA of September 2005.

[103] Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006, p. 53; D. Bigo, *L'Europe des polices et de la sécurité intérieure*, 1992, Ed. Complexe, pp. 51–52.

[104] For example: M. Le Fur, *Rapport n° 3363 sur le projet de loi de finances pour 2007, annexe 30* "*sécurité*", Assemblée nationale, octobre 2006.

[105] They claim that preventing the mutualisation of intelligence is the only way to preserve the cornerstone principles basing the relationships between intelligence services (rules of speciality and of third party service), which are the condition for the confidence required in such activities. Furthermore, bilateral co-operation is regarded as the only way to prevent intoxication effects (in which information is passed constantly between all services involved and thus acquires an undue importance) that might pollute the quality of the treatment of intelligence and subsequently impair its efficiency. Finally, as regards enforcement activities, they claim that direct long-term collaboration is the *sine qua non* condition of successful operational co-operation.

[106] Their position is certainly made easier by the rules governing criminal evidence in France, since the Criminal chamber of the Court of Cassation has admitted that an anonymous information is sufficient to start an investigation with a view to confirm it (for example: Crim. 9th January 2002, *Bull. crim.* n° 2). Thus, French police officers may deal with intelligence directly received from a foreign police force as "anonymous" information allowing them to start an inquiry. Furthermore, the DST officers' double competence allows them to turn intelligence into evidence by simply reporting the information through a statement.

17.3.2 Deficiencies of Control Institutions

French antiterrorist legislation cannot in itself be regarded as threatening individual freedoms. What is indeed problematic when it comes to the issue of civil liberties and human rights is that, antiterrorism criminal procedure being particularly intrusive and coercive, it should be restricted in its enforcement to its designated targets and, furthermore, it should be submitted to a reinforced control regarding both its a priori legality and its enforcement. Practice happens to fall far from this ambition. It has previously been demonstrated that the government has used the pretext of the fight against terrorism to enact a criminal procedure encompassing an impressive number of offences. On the other hand, the adhesion of control authorities to the specific needs of the fight against terrorism has led to a lowering of their requirements regarding legality. It has resulted in the admission of practices which carry an intrinsic risk for human rights, when they are not simply inconsistent with international human rights standards. We shall distinguish the practise of the Constitutional Council (a) from that of the judicial judges (b).

17.3.2.1 The Lowering of the Constitutionality Control

Previous to any development, it must be pointed out that, although the Constitutional Council has sometimes tempered the attempts of legislators, it never contested the mere enforcement of a specific counterterrorism law justifying the enactment of specific criminal procedure provisions.[107] The control exerted by the French Constitutional Council is in no way a control of the appropriateness of the statutes passed by Parliament but only a control of their legality. Related to human rights and civil liberties, it implies that the control is limited to the consistence of the statutory provisions – in terms of proportionality of the infringements on human rights – with the principles established by the Declaration on Human and Civil Rights of 1789 and by he Fundamental Principles established by the Laws of the Republic (mainly derived from the Preamble of the 1946 Constitution and by international norms).[108] There are nonetheless differences in the construction of proportionality, which varies according to the periods of time, to the mere nature of the purposes of the referred legislation, and to the composition of the Council. Regarding criminal procedure legislation, the council moved through the years from control to legitimation of the legislator's ambitions. Whereas the protection of individual freedoms has long prevailed, recent

[107] Already the first time it was called to control the conformity to Constitution of counterterrorism legislation, it stated the principle that investigations in terrorism matters "call, because of their connection with individual or collective undertaking the purpose of which is seriously to disturb law and order through intimidation or terror, for specific proceedings" (Conseil Constitutionnel, décision n° 86-213 DC, 3rd September 1986, §.17).

[108] P. Mazeaud, *La lutte contre le terrorisme dans la jurisprudence du Conseil constitutionnel*, conférence lors de la visite à la Cour suprême du Canada, 25 avril 2006, www.conseil-constitutionnel.fr/divers/documents/20060426.pdf.

years are characterised by the Council's adhesion to law and order policies. Decisions on the 2003, 2004, and 2006 statutes give reason for fear of a lowering of the control exerted by the Council on counterterrorism legislation and of the establishment of an increased margin of assessment left to the legislator.

Between 1974 and the end of the 1990s, the French Constitutional Council's case law can be regarded as principally orientated towards the protection of civil liberties, the Council having then contributed to extend the area of freedoms within French criminal law.[109] The reversal can symbolically be traced to the decision n° 99-411 DC of 16 June 1999, when the Council first adopted a restrictive construction of article 66 of the Constitution.[110] The consequence of this decision is that, except when the enforcement of a police power involves a risk of arbitrary deprivation of liberty, there is no constitutional requirement that the implementation should be controlled by a magistrate. Subsequently, although implying important restrictions to rights and liberties, the Constitutional Council was generally able to validate the recent modifications of the counterterrorism procedural regime.[111]

Thus, the French Constitutional Council recently approved criminal procedure provisions that it had overruled few years before.[112] Furthermore, the content of the recent decisions demonstrates the modesty of the Council requirements when the protection of human rights comes into conflict with criminal procedure provisions of the referred legislation.

The decision n° 2004-492 DC of 2 March 2004 illustrates this analysis. At first sight, it seems a priori balanced[113] because the Council establishes the limits within which the legislator is allowed to enact proactive investigation prerogatives.[114] But

---

[109] See, for example: Conseil constitutionnel, Décision n° 90-281 DC, 27th December 1990, Recueil p. 91, §§.7–8; Décision n° 93-334 DC of 20th January 1994 or Décision n° 96-377 DC, JORF 23rd July 1996, p. 11108.

[110] JORF, 19th June 1999, p. 9018. The issue was to decide whether the notion of "freedom of the individual" stated in article 66 of the Constitution only referred to the right not to be arbitrarily detained or whether it should be constructed broadly. The Council has decided that the narrower construction should prevail.

[111] M. Garrigos, *Les aspects procéduraux de la lutte contre le terrorisme – Etude de droit interne et de droit international*, Thèse de doctorat, Université de Paris I – Panthéon Sorbonne, 2004, p. 80.

[112] Compare: Conseil Constitutionnel, Décision n° 93-323 DC, Rec. p. 213 and Décision n° 2005-532 DC, Rec. p. 31 on border controls; or Conseil constitutionnel, décision n° 96-377 DC, 16th July 1996, Recueil p. 87 and Décision n° 2004-492 DC of 2nd March 2004, Rec. p. 66 on night searches in preliminary investigations.

[113] V. Bück, *Chronique de droit constitutionnel pénal*, Revue de sciences criminelles 1/2005, pp. 122–134; J.-E. Schoettl, *La loi "Perben II" devant le Conseil constitutionnel – Décision n° 2004-492 DC du 24 mars (loi portant adaptation de la justice aux évolutions de la criminalité)*, Gazette du Palais, Recueil mars-avril 2004, p. 893.

[114] The judicial judge must be allowed to control the implementation of dispensatory inquiry techniques, restrictions to fundamental rights must be necessary to the "appearance of truth", and infringements with individual rights must be proportionate to the gravity and complexity of the offences committed and should not involve unjustified discriminations (see: Y. Bisiou, *Enquête proactive et lutte contre la criminalité organisée en France*, in M.-L. Cesoni (dir.), *Nouvelles méthodes de lutte contre la criminalité: la normalisation de l'exception – Etude de droit comparé (Belgique, Etats-Unis, Italie, Pays-Bas, Allemagne, France)*, Bryulant/LGDJ, 2007, p. 353).

a closer look leaves some dissatisfaction. The statement made on the constitutionality of the postponement of the consultation with a lawyer in police custody,[115] although coherent with the case law of the Council,[116] is hardly consistent with international standards.[117] As regards the rules governing searches and seizures or interceptions of communications, the Council validated the provisions of the statute mainly because their enforcement is subjected to the authorisation by the liberty and custody judge. The issue is now to decide whether this authorisation provides sufficient guarantee. Certainly the liberty and custody judge has access to the police file but the judge is not in charge of the overall control of the investigations in which authorisation is demanded and must commonly decide in a situation of emergency. It means that, in practice, the obtaining of the authorisation mostly depends of the ability of the prosecutor to convince the judge – and not merely on the needs of the investigation.[118] In fact, it suggests that the institution of liberty and custody judge has been exploited by the legislator to put in front of the public prosecutor a judicial judge – which apparently satisfies the requirements of the ECHR – with apparent powers but no proper means to enforce them in practice.[119] In other words, the decision confirms that appearance of legality is sufficient to satisfy the Constitutional Council's requirements, which obviously is not satisfactory as regards the protection of fundamental rights. The 2004 decision thus suggests that, regarding the fight against terrorism, the Constitutional Council concedes the lowering of the standards of necessity, proportionality, and due process that it previously established to frame police powers and that it somehow sacrifices the protection of individual rights to increase thereby the room for manoeuvring of security forces.

Such an assessment is confirmed by the Constitutional Council's decision n° 2005-532 DC of 19 January 2006. Despite the management and exploitation of the numerous French police databases cause much difficulties[120], the administrative judge has renounced control of administrative police use of databases[121]. Furthermore,

---

[115] §§.21–34.

[116] Conseil Constitutionnel, décision n° 93-334 DC, 20th January 1994, §§.16–19; see: J.-E. Schoettl, *note sous Conseil Constitutionnel, décision n° 2005-532 DC*, Gazette du Palais, Recueil janvier-février 2006, p. 449.

[117] Comp. ECHR, *Huber v. Switzerland*, 23rd October 1990 and article 30 CPC. Furthermore, the conditions of implementation of this provision are regarded as a matter of concern by the Human Rights Committee of the United Nations (Comité des Droits de l'Homme des Nations Unies, *Examen des rapports soumis par les Etats parties conformément à l'article 40 du Pacte – Observations finales du Comité des droits de l'homme - France*, CCPR/C/FRA/CO/4, 22 juillet 2008, §.14).

[118] J.-F. Ricard et M.-A. Houyvet, *Lutte contre le terrorisme: spécificités de la loi française*, Actualité juridique pénal, n° 5/2004, p.191.

[119] H. Leclerc, *La dérive des libertés en France*, Petites Affiches, 7 avril 2005, n° 69, p. 22.

[120] CNIL, *Rapports annuels*, 2004–2006; Groupe de travail sur les fichiers de police et de gendarmerie, *Comment améliorer le contrôle et l'organisation des fichiers de police et de gendarmerie utilisés dans le cadre des enquêtes administratives?*, Rapport remis au ministre de l'Intérieur, novembre 2006; Comité des Droits de l'Homme des Nations Unies, *Examen des rapports soumis par les Etats parties conformément à l'article 40 du Pacte - Observations finales du Comité des droits de l'homme - France*, CCPR/C/FRA/CO/4, 22 juillet 2008, §.22.

[121] CE, 28 juillet 1995, *CGT*, Recueil Lebon, p. 312.

in spite of the inconsistencies between, on the one hand, the provisions of the statute and, on the other hand, the recommandations made by the experts mandated by the European Union[122] and the case law of the ECHR[123], the Council has reckoned that the powers granted to agents of services involved in counterterrorism carrying administrative inquiries to access, request, process and exploit outside any judicial control data from both public and private data files do not contravene the Constitution.[124] Its conclusion that the guidelines provided by the legislator are sufficient to satisfy the requirement of the protection of the right to private life constitutes, to say the least, a misapprehension of the reality of practices. In addition, the Council does not hesitate to thus admit that the fight against terrorism justifies that forces involved can have access to any databases out of any judicial control whereas, in 2003, it had justified the ratification of the extension of filling in judicial police databases by the control exercised by the judiciary on their exploitation.[125] This confirms that the Council has pushed further the cursor of legality and opted for a very extensive definition of proportionality when called to assess counterterrorism statutory provisions.[126] Finally, although this provision was not referred by the parties, the Council has *obiter dictum* considered the constitutionality of the extension of the length of police custody to 6 days in terrorism cases. Again, it is blatant that appearances of legality and proportionality have been regarded as sufficient by the Council[127]. In fact, this *obiter dictum* seems mainly aimed at sealing the possibility of later challenging the legality of this statutory provision before the Courts or the Council itself.[128]

The assessment of its recent decisions on counterterrorism legislation leads to the conclusion that the French Constitutional Council has renounced the mission of guarantor of civil liberties it attributed to itself in the mid 1990s to gradually develop a restrictive construction of the fundamental rights established by the Declaration on Human and Civil Rights of 1789 and the individual guarantees provided by, or inferred from, the Constitution. Regarding this issue, the Council

---

[122] Council of the European Union, Presidency in co-operation with the Counter Terrorism Coordinator, *Final report on the Evaluation of National Anti-Terrorist Arrangements: Improving national machinery and capability for the fight against terrorism*, 12168/3/05 REV 3, 18 November 2005, recommendation 7.

[123] ECHR, Gde Chamber, 4th December 2008, *S. and Marper v. United Kingdom*, AJ pénal, 2/2009, p. 81, com. G. Roussel.

[124] §§.8–12.

[125] J. Boyer, *Fichiers de police judiciaire et normes constitutionnels: quel ordre juridictionnel ? (Commentaire de la décision du Conseil constitutionnel du 13 mars 2003 relative à la loi sur la sécurité intérieure, ou* "*Splendeurs et misères…*"*)*, Petites affiches, 22 mai 2003, n° 102, p. 14.

[126] A. Paris, *L'objet du contrôle de constitutionnalité*, Revue administrative n° 355, chronique de jurisprudence constitutionnelle, p. 32.

[127] Current overall French police custody law is, indeed, hardly consistent with ECHR, Gde Chamber, 27th November 2008, *Salduz v. Turkey*, req. n°36391/02.

[128] Article 61-1 of the French Constitution (article 29 of the Loi constitutionnelle n° 2008-724 du 23 juillet 2008 *de modernisation des institutions de la Ve République*, JORF 24th July 2008, p. 11890).

has thus turned its role from the watchdog against the abuses perpetrated by the Legislator to legitimation of the Executive law-and-order aspirations. The field of human rights finds itself reduced in proportion.

On the other hand, the insistence of the Council to present the judicial control of police activities as, in itself, the guarantee of the respect of civil liberties and human rights requires assessing now whether, in practice, the judiciary satisfactorily discharges this burden when it deals with terrorism cases.

17.3.2.2 Lowering of Judicial Control

Although recent decisions of the European Court of Human Rights leave to think that this jurisdiction takes into account the necessities of the protection of Members States' national security,[129] its assessment of national practices remains governed by the requirements of the pre-eminence of the law and of the Rule of Law in a democratic society. The decision in *Öcalan v. Turkey* proves the fact that the accused charged with terrorist offences has very little influence on the construction of the guarantees granted to him/her.[130] Despite pressure to give rise to a kind of counter-terrorism exception to fundamental rights,[131] the Court has emphasised, in *Jalloh v. Germany*, that "even in the most difficult circumstances, such as the fight against terrorism and organised crime", the protection of fundamental rights remains non-negotiable beyond the exceptions and derogations provided by the Convention itself.[132]

Most regrettably, it seems that French courts have sometimes opted for a different construction of the implications of the requirements of the fight against terrorism.

M. Garrigos points out that "the strengthening of the police network favours the hypertrophy of the preliminary stage of the procedure".[133] The role of the judicial judge has thereby been limited by the legislator and so has been the control he/she exerts on police activities. To that extent, the French system does not depart from an evolution experienced by most other occidental democracies. However, whereas it seems that foreign magistrates[134] try to resist this movement, the French

---

[129] For example: ECHR, Grand Chamber, *Ramirez Sanchez v. France*, 4th July 2006.

[130] ECHR, Grand Chamber, *Öcalan v. Turkey*, 12th May 2005.

[131] See, for example: H. Mock, "*Guerre*" *contre le terrorisme et droits de l'Homme, Réflexions à propos du rapport de la FIDH intitulé* "*l'antiterrorisme à l'épreuve des droits de l'homme: les clés de la compatibilité*", Revue trimestrielle des droits de l'Homme, 65/2006, p. 23.

[132] ECHR, Grand Chamber, *Jalloh v. Germany*, 11th July 2006, §.99; see, also, ECHR, Gde Chamber, 28th February 2008, *Saadi v. Italy*, Rev. sc. crim. 3/2008, p. 692, com. J.-P. Marguénaud; H. Tigroudja, *L'équité du procès pénal et la lutte internationale contre le terrorisme. Réflexions autour de décisions internes et internationales récentes*, Revue Trimestrielle des Droits de l'Homme n° 69, 2007, p. 22.

[133] M. Garrigos, *Les aspects procéduraux de la lutte contre le terrorisme – Etude de droit interne et de droit international*, Thèse de doctorat, Université de Paris I – Panthéon Sorbonne, 2004, pp. 155–156.

[134] For example, in the United Kingdom or in the United States of America.

jurisdictions are more conciliatory. Instead of considering that, as dispensatory powers imply an important infringement to fundamental rights, their enforcement should be drastically overseen and the legal provisions restrictively constructed, the French judiciary adopts an understanding position. This deficiency affects the entire judicial process.

The lack of control exercised by public prosecutors over counterterrorism police activities can be briefly dealt with. It has previously been mentioned that the provisions of the CPC organises the interdependence between police forces and prosecution services. The combination of the provisions of articles 12 and 13 are particularly problematic because prosecutors are, in the meantime, supposed to direct judicial police operations and to supervise, indeed to control, them. The rationalisation of the judicial administration activity is translated into an obligation for prosecution services to justify, through statistics sent to the Ministry of Justice, the efficiency of their action. These authorities are thus made entirely dependant on the benevolence of the police forces.[135] As a consequence, the control exerted by prosecutors on police activities is in practice reduced to its simplest terms.[136] Finally, the functional subordination of French public prosecutors towards the minister of Justice, in a context of hegemony of the ministry of Interior on the security agenda, also reduces the ability of public prosecurtors to fulfill their duty to supervise police activities.[137] The role of French prosecution services should therefore be considered of little interest as far as the protection of the rights of terrorism suspects is concerned.

The issue of the control exercised over investigating judges is rather controversial too from a human rights perspective. Juvenal's interpellation "*Quis custodiet ipsos custodet*?" proves its pertinence when considering the issue of counterterrorism in France. In spite of the provisions of article 81 of the Criminal Procedure Code, the relationships of mutual trust developed and kept by intelligence and enforcement police forces with counterterrorism judges legitimate doubts being formed regarding the reality of the control exercised.[138] In fact, it is probably more accurate to consider that these magistrates are now mainly involved in the prosecution process, which seriously impairs their capacity as individual freedom guarantors.

---

[135] D. Salas, *La volonté de punir – Essai sur le populisme pénal*, Hachette, 2005, p. 159.

[136] The lack of satisfactory control is constantly denounced by the Committee for the Prevention of Torture of the Council of Europe (CPT/Inf (2001) 10, 19 July 2001, §.16), by the Commissioner for Human Rights of the Council of Europe (CommDH(2006)2, 15 February 2006, §§.174–180), by Amnesty International (Amnesty International, *France, Pour une véritable justice – Mettre fin à l'impunité de fait des agents de la force publique dans les cas de coups de feu, de morts en garde à vue, de torture et autres mauvais traitements*, EUR 21/001/2005), and even by the French National Commission for a Security Code of Conduct, an independent administrative authority (*Rapport annuel 2007*, April 2008, pp. 9–17).

[137] ECHR, 5th Section, 10th July 2008, *Medvedyev v. France* (§.61), Rev. sc. crim. 1/2009, p. 176, com. J.-P. Marguénaud. This case is currently pending before the ECHR Grande Chamber; hearings took place on 6th May 2009 (see: A. Salles, *Les liens entre procureurs et pouvoir devant la CEDH*, Le Monde, 8th May 2009, p. 9)

[138] J. Shapiro and B. Suzan, *The French Experience of Counter-terrorism*, Survival, vol. 45, n° 1, Spring 2003, p. 91.

The difficulty then is that, as article 81 also reads that the investigation judge "seeks out evidence of innocence as well as guilt", it is somehow difficult for the tribunal to dismiss evidence resulting from a judicial investigation because it implicitly implies criticising the work done by the investigation judge, who is a peer. This is where the status of counterterrorism investigating magistrate happens to be problematic. When one considers the way investigation files are sustained, the role of the investigating magistrate is substantially often limited to providing rogatory letters to turn intelligence collected by police services into judicial evidence. Thus, the status of the investigating judges confers to police information an illegitimate conviction potential that might impair the quality of the administration of justice and should therefore be regarded as implying serious risks for the protection of the fundamental rights of suspected terrorists. Although it is undeniable that the connivance between specialised investigating magistrates and counterterrorism police forces makes the fight against terrorism more efficient, the price paid regarding civil liberties issues is neither deniable.

The control exercised by the courts in counterterrorism cases neither escapes criticism. The assessment of the case law of French jurisdictions leaves the feeling that sometimes the efficiency of repression prevails over the constitutional mission of guarantor of individual freedom.[139]

The issue of the admission of evidence obtained by illegal means illustrates this assertion. Certainly, according to the ECHR case law, public authorities enjoy a margin of assessment taking into account the interests involved regarding the admissibility of evidence[140] and the admission of evidence obtained by unlawful means does not necessarily impair the fairness of the trial.[141] Nonetheless, although in *Sölemez v. Turkey*, the European Court of Human Rights pointed out that "a declaration made under a violation of article 3 intrinsically lacks reliability" and subsequently that "the taking into account of such evidence is inconsistent with the guarantees of article 6 of the Convention",[142] French judicial authorities appear accommodating when they try terrorism cases. According to the construction stated by the Criminal chamber of the Court of Cassation, article 427 CPC implies that "no legal provision allows criminal jurisdictions to dismiss evidence presented by one of the parties for the sole reason that they have been obtained unlawfully or disloyally; courts should only assess the probative value of these evidence after having subjected them to a contradictory debate".[143] As a

[139] For example, despite the Constitutional Council-expressed reservation of interpretation and the wording of article 706-95, subsection 1 *in fine*, the Court has decided that the control exercised by the liberty and custody judge on interceptions of communication in administrative investigations on a suspicion of organised crime does not have to be concomitant to the course of the operation (Crim. 23rd May 2006, Recueil Dalloz 2006, n° 41, jurisprudence, p. 2836).

[140] ECHR, Grand Chamber, *Edwards and Lewis v. United Kingdom*, 27th October 2004.

[141] ECHR, *Schenk v. Switzerland*, 12th July 1988.

[142] ECHR, Grand Chamber, *Söylemez v. Turkey*, 21st September 2006, §.122.

[143] For example: Crim, 11th June 2002, Petites affiches, 6th January 2003, n° 4, p.15, comm. F. Ringel.

consequence, evidence collected by illegal means, including torture, is not automatically dismissed.[144] This situation is not the pride of the French criminal justice system, particularly when compared with foreign jurisdictions.[145] Besides, it is paradoxical: the French legal system is monist and according to article 55 of the Constitution, international norms prevail over national law; furthermore, article 66 of the Constitution provides that magistrates of the judiciary are the guarantor of individual liberty; nonetheless, despite the international prohibition,[146] the French specialised jurisdiction, when it tries terrorism cases, shows much deference to the prosecution pretensions and seems to have admitted that civil liberties can be sacrificed to what the prosecution services regard as the requirements of national security.

The expulsion of foreigners from French territory for breach of law and order also illustrates this assertion. Although they enjoy the necessary powers to oppose the purposes of the Ministry of Interior when expulsion of suspected terrorists to countries where they risk being tortured or ill-treated on return is planned, French jurisdictions generally refuse to cancel such orders whatever the reality of the risk faced and, furthermore, they carry on passing sentences of banishment of the French territory against nationals of undemocratic countries.[147]

Nonetheless, despite the reservations inspired by the above elements, the current situation in France is that antiterrorism forces act almost outside any kind of control at the pre-trial stage, and it is only at the trial stage that counter-powers find relevance. There is evidence that in a majority of cases the specialised Court in a majority of cases of Assizes and correctional tribunal carry on assuming their duty to assess the investigation magistrates' work.[148] Besides, through a few recent decisions, the Criminal Chamber of the Court of Cassation has restated an exacting construction

---

[144] O. Cahn, *L'arrêt HL. R. v. Secretary of State for the Home Department, ex parte Ramda du 27 juin 2002: incident isolé ou précédent dommageable?*, Cultures et Conflits n° 66 "Construire le voisin. Pratiques européennes", juin 2007, pp. 121–156; E. Molina, *Réflexion critique sur l'évolution paradoxale de la liberté de la preuve des infractions en droit français contemporain*, Revue de sciences criminelles, 2/2002, p. 263.

[145] See, for example, British House of Lords, *A (FC) and others (FC) v. Secretary of State for the Home Department (2004) – A and others (FC) and others v. Secretary of State for the Home Department (conjoined appeals)* [2005] UKHL 71, 8th December 2005.

[146] M. Delmas-Marty, *Le paradigme de la guerre contre le crime: légitimer l'inhumain?*, Revue de sciences criminelles, 3/2007, pp. 470–471.

[147] Human Rights Watch, *Au nom de la prevention. Des garanties insuffisantes concernant les éloignements pour des raisons de sécurité nationale*, vol. 19, n° 3(D), June 2007, p. 28; Human Rights Watch, *World Report*, 2008, p. 386; Comité des Droits de l'Homme des Nations Unies, *Examen des rapports soumis par les Etats parties conformément à l'article 40 du Pacte – Observations finales du Comité des droits de l'homme – France*, CCPR/C/FRA/CO/4, 22 juillet 2008, §.20. or Paris Court of Appeal, 24th February 2009 (see. Le Monde, *Cinq anciens détenus français de Guantanamo relaxés en appel*, 25th February 2009).

[148] For example: *Chalabi* case 1999; *Castella/Peruzzi* case 2006

of the principle of loyalty in the gathering of evidence admissible in Courts.[149] This case law is hardly compatible with the current admission of evidence obtained in violation of article 3 and might therefore lead to a reversal in the construction of article 427 CPC by the jurisdictions. It suggests that magistrates are not ready yet to abdicate their ultimate decision power to the demands of both the Executive agencies and the specialised prosecutors and investigating judges.

The conclusion might be that the protection of human rights has been concentrated on the trial stage. This is not entirely satisfactory because it leaves to the personal convictions of seated judges a duty that should be a concern of the overall counterterrorism apparatus. Even if egregious violations of civil liberties remain isolated in the recent history of French counterterrorism, the whole system carries a threat for human rights that cannot be neglected. It leaves "an open door to arbitrariness"[150] both by too often leaving the protection of fundamental rights to police officers and investigating magistrates' consciousness and by the failure to provide appropriate controls.

The question now is to decide whether the neutralisation of this threat will compromise the efficiency of the repressive apparatus. The restriction of the enforcement of specific procedural rules to the fight against terrorism and international organised crimes will have no effect. Surely, extending judicial controls to preventive or proactive police activities, excluding in courts evidence obtained by illegal means, and integrating the group of investigating judges within the prosecution services might make the burden of security services officers heavier. Is such a burden put on police officers an unbearable price to pay for strengthening the fundamental rights of suspects facing heavy charges carrying a minimum of 10 years' imprisonment incurred?

In a conspicuous article published in 2000, J.-P. Marguénaud states that criminal procedure is an area where the gap between views expressed by the French authorities on the international scene and their domestic practice is particularly blatant and he puts further that as French authorities pretend to give lessons on human rights to the entire world, an elementary coherence should lead them to apply exemplarily lessons dispensed to them by the European Court of Human Rights.[151]

The above developments should be reconsidered in the light of Professor Marguénaud's assertions. Before expressing pride for having managed to maintain the fight against terrorism within the sphere of ordinary criminal law, the French authorities might be well inspired to consider that what they regard as an achievement

---

[149] Crim. 11 mai 2006, *Bull. crim.* n° 132; Crim. 9 août 2006, *Bull. crim.* n° 202; Crim, 7 février 2007, Bull. crim. n° 37, Rev. sc. crim. 3/2008, p.663, com. J. Buisson; Cass. Crim., 4 juin 2008, n° de pourvoi: 08-81045, Communication - Commerce électronique, 9/2008, com. n°106, A. Lepage; see also: P. Conte, *La loyauté de la preuve dans la jurisprudence de la chambre criminelle de la Cour de cassation: vers la solution de la quadrature du cercle?* Dr. pénal, 4/2009, *Etudes*, n°8.

[150] Fédération Internationale des Ligues des Droits de l'Homme, *France: la porte ouverte à l'arbitraire*, Rapport d'une mission internationale d'enquête en France sur l'application de la législation antiterroriste, January 1999, n° 271.

[151] Jean-Pierre Marguénaud, *La dérive de la procédure pénale française au regard des exigences européennes*, Recueil Dalloz 2000, chronique, p. 249.

is probably more the result of the weaknesses and deficiencies of the protection of human rights over the whole French criminal justice process rather than a success of French democracy. Criminal justice legislation, which currently allows police forces to implement the same prerogatives to fight an ordinary small town gang of drug dealers and an international terrorist organisation can hardly be regarded as satisfactory. Similarly, a legislator which so openly used the pretext of the fight against terrorism to push further the frame of legality and to reduce so significantly civil liberties can hardly be regarded as a model. Neither can a judiciary that often makes repressive effectiveness prevail over due process and internationally established fundamental rights. It would then be audacious to assert that it is only in countries where exceptional legislations have been enforced that the fight against terrorism has jeopardised human rights.

References

Alix, J. *Terrorisme et droit pénal - Etude critique des incriminations terroristes*, Thèse pour le doctorat en droit, Dir. G. Giudicelli-Delage, Université de Paris 1 Panthéon-Sorbonne, 2008

Bianchi, V. *La loi du 23 janvier 2006 ou l'extension à l'application des peines de la compétence nationale en matière de terrorisme*, Gazette du Palais, Recueil mai-juin 2006, 1570–1571

Bigo, D. *L'Europe des polices et de la sécurité intérieure*, 1992, Ed. Complexe

Bigo, D. *L'impact des mesures anti-terroristes sur l'équilibre entre liberté et sécurité et sur la cohésion sociale en France*, in E. Bribosia et A. Weyembergh (ed.), *La lutte contre le terrorisme et les droits fondamentaux*, Nemesis, Bruylant, Coll. Droit et justice n° 34, 2002, 221–247

Bisiou, Y. *Enquête proactive et lutte contre la criminalité organisée en France*, in M.-L. Cesoni (dir.), *Nouvelles méthodes de lutte contre la criminalité: la normalisation de l'exception – Etude de droit comparé (Belgique, Etats-Unis, Italie, Pays-Bas, Allemagne, France)*, Bryulant/ LGDJ, 2007, 344–379

Bonelli, L. *Les caractéristiques de l'antiterrorisme français: "Parer les coups plutôt que penser les plaies"*, in D. Bigo, L. Bonelli et T. Deltombe (dir.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, pp.168–187

Boyer, J. *Fichiers de police judiciaire et normes constitutionnels: quel ordre juridictionnel? (Commentaire de la décision du Conseil constitutionnel du 13 mars 2003 relative à la loi sur la sécurité intérieure, ou "Splendeurs et misères…")*, Petites affiches, 22 mai 2003, n° 102, 4–19

Bück, V. *Chronique de droit constitutionnel pénal*, Revue de sciences criminelles 1/2005, pp.122–134

Buisson, J. *Des contrôles d'identité aux fouilles requises*, Procédures, mars 2002, 6–8

Buisson, J *Chronique de procédure pénale*, Rev. sc. crim. 3/2008, pp. 655–665

Cahn, O. *La coopération policière franco-britannique dans la zone frontalière transmanche*, Thèse de doctorat en droit pénal et sciences criminelles, Université de Poitiers, 2006, 2 vol

Cahn, O. *L'arrêt HL. R. v. Secretary of State for the Home Department, ex parte Ramda du 27 juin 2002: incident isolé ou précédent dommageable?*, Cultures et Conflits n° 66 "Construire le voisin. Pratiques européennes", juin 2007, 121–156

Caprioli, L. & Pochon, J.-P. *La France et le terrorisme international – Les racines historiques et organisationnelles du savoir policier*, Cahiers de la Sécurité intérieure, n° 55, 1/2004, 147–179

Chrestia, P. *La loi du 23 janvier 2006 relative à la lutte contre le terrorisme: premières observations*, Recueil Dalloz, n° 21, 2006, 1409–1413

Chrestia and Commission: Comité de réflexion sur la justice pénale, *Rapport d'étape sur la phase préparatoire du procès pénal*, 6th March 2009

Comité de réflexion sur la justice pénale, *Rapport d'étape sur la phase préparatoire du procès pénal*, 6th March 2009
Commission chargée de l'élaboration du Livre Blanc sur la Défense et la Sécurité Nationale, *Défense et Sécurité Nationale – Le Livre Blanc*, Odile Jacob - La Documentation française, 2008
Commission Nationale de Contrôle des Interceptions de Sécurité, *17ème rapport d'activité - 2008*, La Documentation française, 2009
Conte, P. *La loyauté de la preuve dans la jurisprudence de la chambre criminelle de la Cour de cassation: vers la solution de la quadrature du cercle?* Dr. pénal, 4/2009, *Etudes*, n°8
Conte, P. *Les propositions du pré-rapport du comité de réflexion sur la justice pénale*, Droit pénal, 6/2009, *Etudes*, n°11
Danet, J. *De la procédure à la répression de la criminalité organisée, ou laquelle est l'instrument de l'autre ?*, Actualité juridique pénal, n° 5/2004, 192–195
Danet, J. *Cinq ans de frénésie pénale*, in L. Mucchielli (dir.), *La frénésie sécuritaire – Retour à l'ordre et nouveau contrôle social*, La Découverte, coll. sur le vif, 2008, pp.19–29
Danti-Juan, M. *Les adaptations de la procédure*, Revue pénitentiaire et de droit pénal, n° 4/2003, 725–734
De Lamy, B. *La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (Crime organisé - Efficacité et diversification de la réponse pénale)*, Recueil Dalloz 2004, n° 27, 1910–1918
Delcamp, A., Bergel J.-L. & Dupas, A. *Contrôle parlementaire et évaluation*, La Documentation française, coll. Les études de la DF, série Institutions, 1995
Delmas-Marty, M. *Le paradigme de la guerre contre le crime: légitimer l'inhumain?*, Revue de sciences criminelles, 3/2007, 461–472
Delmas-Marty, M. *Libertés et sûreté dans un monde dangereux - Radicalisation des procédures de contrôle*, Cours au Collège de France, Chaire Etudes juridiques comparatives et internationalisation du droit, 3rd February 2009
Desessard, L. *Contribution au débat sur l'article 18 alinéa 5 du code de procédure pénale*, Revue pénitentiaire et de droit pénal, n° 2/2006, 443–453
Desportes, F. and Lazerges-Cousquer, L., *Traité de procédure pénale*, Economica, 2009
Dutheillet de Lamothe, O. *French legislation against terrorism: constitutional issues*, November 11th 2006, www.conseil-constitutionnel.fr/divers/documents/constitutionalterrorism.pdf
Europol, *Annual Report 2006*, May 2007
Europol, *TE-SAT 2008, EU Terrorism situation and trend report*, 2008, www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/TESAT2008.pdf
Fédération Internationale des Ligues des Droits de l'Homme, *France: la porte ouverte à l'arbitraire*, Rapport d'une mission internationale d'enquête en France sur l'application de la législation antiterroriste, Hors série de la *Lettre bimensuelle de la FIDH*, n° 271, January 1999
Foyer, J. *Droit et politique dans la répression du terrorisme en France*, in Mélanges offerts à G. Levasseur, *Droit pénal et droit européen*, Gaz. Pal./Litec, 1992, 408–421
Gagnoud, P. *Fouilles de véhicules automobiles; brèves remarques sur les principaux apports de la loi du 18 mars 2003*, Gazette du Palais, Recueil mai-juin 2003, 1623–1624
Garcia-Jourdan, S. *L'émergence d'un espace européen de liberté, de sécurité et de justice*, Bruylant, 2005
Garrigos, M. *Les aspects procéduraux de la lutte contre le terrorisme – Etude de droit interne et de droit international*, Thèse de doctorat, Université de Paris I – Panthéon Sorbonne, 2004
Gayraud, J.-F. & Sénat, D. *Le terrorisme*, PUF, coll. Que sais-je?, 2ème éd., 2006
Giudicelli, A. *La garde à vue après la loi n° 2004–204 du 9 mars 2004*, Actualité juridique pénal, juillet-août 2004, 261–268
Gleizal, J.-J. *Sécurité et globalisation*, Revue de Sciences criminelles 4/2004, 949–954
Gonnard, J.-M. *Terrorisme - Art. 421–1 à 422–5*, Jurisclasseur Droit pénal, 1994
Gouvernement de la République Française, *La France face au terrorisme – Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La Documentation française, 2006
Groupe de contrôle des fichiers de police et de gendarmerie, *Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés – Rapport remis au ministre de l'Intérieur,*

de l'Outre-mer et des Collectivités territoriales, 10th December 2008, La Documentation française, 2009

Guinchard, S. and Buisson, J., *Procédure pénale*, 4th ed, LexisNexis-Litec, 2008

Guittet, E.-P. *Military activities within national boundaries: the French case*, Cultures et Conflits, *Illiberal Practices of Liberal Regimes: the (in)security games*, L'Harmattan, 2006, 139–166

Guittet, E.-P., *L'implication de l'armée dans la lutte antiterroriste: le cas français*, in D. Bigo, L. Bonelli & T. Deltombe (dir.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, pp.188–193

Hermant, D. & Bigo, D. *Les politiques de lutte contre le terrorisme: enjeux français*, in F. Reinares (dir.), *European democracies against terrorism – Governmental policies and intergovernmental co-operation*, Ashgate Pub. Co., 2000, 72–98

Huet, A. and Koering-Joulin, R. *Droit pénal international*, PUF, coll. Thémis droit, 3è ed., 2005

Human Rights Watch, *Au nom de la prevention. Des garanties insuffisantes concernant les éloignements pour des raisons de sécurité nationale*, vol. 19, n° 3(D), June 2007

Human Rights Watch, *World Report*, 2008

Human Rights Watch, *La justice court-circuitée - Les lois et procédures antiterroristes en France,* Report 1-56432-350-1, July 2008

Labayle, H. *Terrorisme et droit communautaire*, Cour de cassation, cycle droit européen 2007, 8ème conférence, 12 novembre 2007, *n.p*.

Lasserre-Capdeville, J. *Note sous Crim. 9th July 2008*, AJ Pénal 10/2008

Lazerges, C. *La dérive de la procédure pénale*, Revue de sciences criminelles, chronique de politique criminelle, n° 3/2003, 644–654

Leclerc, H. *La dérive des libertés en France*, Petites Affiches, 7 avril 2005, n° 69, 19–23

Le Fur, M. *Rapport n° 3363 sur le projet de loi de finances pour 2007, annexe 30 "sécurité"*, Assemblée nationale, octobre 2006

Lennon, J.-L. *Les aspects coercitifs et intrusifs de l'enquête préliminaire ou l'effritement de la distinction entre enquête de flagrance et enquête préliminaire*, Droit pénal, étude n° 21, octobre 2007, 17–22

Lepage, A., *Note sous Crim. 4th June 2008*, Communication - Commerce électronique, 9/2008, com. n°106

Lienhard, C. *La loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et au contrôle frontalier*, JCP G, n° 12, 22 mars 2006, 527–528

Mac Leod, A. *Insécurité et sécurité après les évènements du 11 septembre: France et Grande-Bretagne*, in S.-J. Kirschbaum (dir.), *Terrorisme et Sécurité internationale*, Bruylant, coll. Etudes stratégiques internationales, 2004, 199–216

Marguénaud, J.-P. *La dérive de la procédure pénale française au regard des exigences européennes*, Recueil Dalloz 2000, chronique, 249–260

Marguénaud, J.-P. *Note sous ECHR, Gde Chamber, 28th February 2008*, *Saadi v. Italy*, Rev. sc. crim. 3/2008, p.692

Marguénaud, J.-P. *Note sous ECHR, 5th Section, 10th July 2008, Medvedyev v. France, Rev. sc*. crim. 1/2009, p.176

Maron, A. and Haas, M., *Note sous Crim. 13th November 2008*, Dr. pénal 3/2009, com. n°43

Massé, M. *Retour sur l'article 18, alinéa 5, du Code de procédure pénale*, Revue de sciences criminelles, 2/2007, 387–392

Mayaud, Y. *Terrorisme*, Rep. pén. Dalloz, 1997

Mazeaud, P. *La lutte contre le terrorisme dans la jurisprudence du Conseil constitutionnel*, conférence lors de la visite à la Cour suprême du Canada, 25 avril 2006, www.conseil-constitutionnel.fr/divers/documents/20060426.pdf

Mekhantar, J. *Droit politique et constitutionnel*, ESKA, coll. Droit public et sciences politiques, 1997

Mock, H. *"Guerre" contre le terrorisme et droits de l'Homme, Réflexions à propos du rapport de la FIDH intitulé "l'antiterrorisme à l'épreuve des droits de l'homme: les clés de la compatibilité"*, Revue trimestrielle des droits de l'Homme, 65/2006, 23–34

Molina, E. *Réflexion critique sur l'évolution paradoxale de la liberté de la preuve des infractions en droit français contemporain*, Revue de sciences criminelles, 2/2002, 263–282

Montjardet, D. *Ce que fait la police – Sociologie de la force publique*, La Découverte, coll. textes à l'appui/série sociologie, 1996

Ocqueteau, F. *Cinq ans après la loi "vidéosurveillance" en France, que dire de son application ?*, Cahiers de la Sécurité intérieure, n° 43, 1/2001, 101–110

Paris, A. *L'objet du contrôle de constitutionnalité*, Revue administrative n° 355, 2006, chronique de jurisprudence constitutionnelle, 31–34

Ricard J.-F. & Houyvet, M.-A. *Lutte contre le terrorisme: spécificités de la loi française*, Actualité juridique pénal, n° 5/2004, 191–192

Rolin, F. et Slama, S. *Les libertés dans l'entonnoir de la législation anti-terroriste*, Actualité juridique Droit administratif, May 15th 2006, pp.975–982

Roussel, G. *Note sous ECHR, Gde Chamber, 4th December 2008, S. and Marper v. United Kingdom*, AJ pénal, 2/2009, p.81

Rubi-Cavagna, E. *L'extension des procédures dérogatoires*, Rev. sc. crim. 1/2008, p.23

Sainati, G. & Schalchli, U. *La décadence sécuritaire*, La fabrique, 2007

Salas, D. *La volonté de punir – Essai sur le populisme pénal*, Hachette, coll. Littératures, 2005

Salles, A. *Les liens entre procureurs et pouvoir devant la CEDH*, Le Monde, 8th May 2009, p.9

Schoettl, J.-E. *La loi "Perben II" devant le Conseil constitutionnel – Décision n° 2004–492 DC du 24 mars (loi portant adaptation de la justice aux évolutions de la criminalité)*, Gazette du Palais, Recueil mars-avril 2004, 893–907

Schoettl, J.-E. *note sous Conseil Constitutionnel, décision n° 2005–532 DC*, Gazette du Palais, Recueil janvier-février 2006, 449–463

Schwendener, M. *Une police aux pouvoirs d'enquête renforcés*, Actualité juridique pénal, n° 6/2004, 228–232

Shapiro, J. & Suzan, B. *The French Experience of Counter-terrorism*, Survival, vol. 45, n° 1, Spring 2003, 67–98

Spencer, J.-R. & Padfield, N. *L'intégration des droits européens en droit britannique*, Revue de sciences criminelles 3/2006, 537–550

Tigroudja, H. *Quel(s) droit(s) applicable(s) à la "guerre antiterrorisme"?*, AFDI, XLVIII, 2002, p.81–102

Tigroudja, H. *L'équité du procès pénal et la lutte internationale contre le terrorisme. Réflexions autour de décisions internes et internationales récentes*, Revue Trimestrielle des Droits de l'Homme n° 69, 2007, 3–38

Touchot, O. *Etude comparée des législations antiterroristes en France, au Royaume-Uni et aux Etats-Unis*, Thèse de doctorat, Université de Paris II – Panthéon Assas, 2004

Vlamynck, H. *Le policier et la garde à vue: remarques et interrogations*, Actualité juridique pénal, juillet-août 2004, 269–275

Chapter 18
The Secret Service's Influence on Criminal Proceedings

Marc Engelhart

18.1 Introduction

The German secret services[1] are traditionally the institutions that collect information within and outside of Germany about threats to the security of the state or the public order. Their tasks have been seen as distinct to the tasks of the police (preventing crimes) and the prosecution (prosecuting crimes). Therefore the secret services and the police/prosecution traditionally did not cooperate closely. This does not mean that there had been no overlap of their tasks and in their everyday work. Especially in the field of crimes against the state, cooperation between the secret services, the police, and the prosecution has a long tradition (Martin 1966).

In the 1980s the legislator began more and more to regard criminal law and police law as parts of the more comprehensive area of homeland security (*Innere Sicherheit*) and no longer as separate sectors of legislation alone (Hassemer 1993; Wolter 1999). Homeland security is understood to include all the tasks of the state in regard to preventing harm for individuals and the state as well as fighting crimes (Götz 2006; Pieroth et al. 2005; Roggan and Kutscha 2006: 24). Although the term has been used a lot in the last decade, one has to concede that in the absence of any legal definition it is a rather vague description of different tasks. The term as a conglomeration of various aspects raises more questions than it answers and should only be used carefully unless accompanied by an exact definition.

In spite of these uncertainties (maybe also because of them), in the context of homeland security the traditional borders of criminal law, police law, and the law of the security services have begun to vanish and the different fields of law have begun to merge (Sieber 2007; see also Hetzer 1999; Staff 1999). This was visible in a first wave when the law of the secret services as well as police and criminal law

M. Engelhart (✉)
Max-Planck-Institute for Foreign and International Criminal Law, Freiburg, Germany
e-mail: marcengelhart@googlemail.com

[1] In the following, the terms secret services and (intelligence) agencies will be used interchangeably because there does not exist any clear definition for these terms.

M. Wade and A. Maljević (eds.), *A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications,*
DOI 10.1007/978-0-387-89291-7_18,

where adjusted in order to fight organised crime (see for example Soiné 2007). The second wave is still rolling and is aimed at fighting international terrorism (Hassemer 2006; Hoffmann-Riem 2002). Terrorism is not new to the German system, as during the 1970s and 1980s Germany had to deal with left-wing terrorism by the *Rote Armee Fraktion* (RAF). These events of national terrorism did leave their mark on the German legal system (especially in the field of criminal procedure) but in comparison to developments today, they where only minor adjustments.

In the following, only the secret services and their relationship to traditional criminal justice institutions will be depicted although the changes of police and criminal procedure law are also remarkable. However, the new developments can be seen best within the law of the secret services. New developments also mean new problems. Many of these problems exist in regard to constitutional law and the protection of individual rights. This chapter will show where the law of the secret services stands now, what important developments have taken place, and what problems exist.

In the first part, the secret services and their legal environment will be described. This includes the organizational structure of the services, their tasks, and powers. In the second part, the cooperation between the secret services and the criminal justice institutions will be examined, with the main emphasis on the exchange of information. In the third part, some major problems in criminal proceedings will be discussed that arise out of the criminal functions of the secret services or out of their collection of information for other tasks.

18.2 Secret Services in Germany

As in many other countries, Germany does not have one omnipotent secret service but has established several agencies, to each of which a different task has been assigned (Bäumler 1991; Gröpl 1993; Würtenberger and Heckmann 2005). On the federal level, three different agencies exist: the *Bundesamt für Verfassungsschutz* (BfV),[2] the *Bundesnachrichtendienst* (BND),[3] and the *Militärischer Abschirmdienst* (MAD).[4] In addition to these federal agencies, each state (*Bundesland*) has established a *Landesamt für Verfassungsschutz*.[5] These State Offices vary in size, structure, and partly in the powers with which they have been provided. However, in substance and concerning their tasks, they very much resemble the Federal Office, therefore the Federal Office will mainly be dealt with in the following.

[2] Federal Office for the Protection of the Constitution. For further information, see the website under <http://www.verfassungsschutz.de>.

[3] Federal Intelligence Agency. For further information, see the website under <http://www.bundesnachrichtendienst.de>.

[4] Military Counter-Intelligence Service. For further information, see the website under <http://www.mad.bundeswehr.de>.

[5] State Office for the Protection of the Constitution.

18.2.1 General (Constitutional) Requirements

18.2.1.1 Constitutional Power

According to art. 73 No. 1, 10 b), c) GG the legislative power to set up and regulate the federal agencies rests exclusively with the federal state (Gröpl 1993; Singer 2002). Apart from their powers in the Federal Council of Germany (*Bundesrat*), the states do not have influence on the regulation of these agencies. However, the states have the right to set up their own "State Offices for the Protection of the Constitution."[6] This Power is limited to the area of the respective state. The distribution of power between the federal and state level is due to the federal structure of the Republic of Germany.

The Federal Constitutional Court interprets the constitutional provisions to set up and regulate the secret services (art. 73 No. 1, 10 b), c) GG) to also include the possibility to use information collected by the secret services for police matters and criminal proceedings (see BVerfGE 100, 313). The court argues that such a use is only a consequence of the basic task of the services in regard to state security and foreign policy. As long as this primary task remains the cornerstone of the work of the secret services, no explicit constitutional provision is required in regard to some (minor) police and criminal law tasks (see Staff 1999). This approach of the constitutional court has opened the door for the influence of the secret services on criminal proceedings.

18.2.1.2 Requirement of a Statutory Provision

German constitutional law requires fundamental decisions to be taken by the legislative power (*Vorbehalt des Gesetzes*). One basis for this requirement is the rule of law (*Rechtsstaatsprinzip*, art. 20 para. 3 GG) that allows state action only when it can be traced back to a rule set up by parliament. Another basis is the democratic principle (art. 20 para. 2 GG) that wants to ensure that only the body elected by the people makes fundamental decisions in public proceedings and not the executive in a non-transparent way. The most important decisions must be taken by Parliament itself and cannot be delegated to the executive or subsidiary bodies (*Parlamentsvorbehalt*). According to the German Federal Constitutional Court, this requirement of a parliamentary provision applies especially when a regulation for state action can infringe fundamental rights (BVerfGE 47, 46).

In the context of the secret services, the requirement of a parliamentary provision means on the one hand that the framework of the services has to be decided by parliament and cannot for example be delegated to the Head of the Federal

[6]Therefore a constitution does not only exist on the federal level but also in the states: each of the 16 states has its own constitution.

Chancellery (*Chef des Bundeskanzleramts*, who is responsible for the coordination of the federal secret services). On the other hand, there has to be a parliamentary provision for all measures of the secret services that can infringe individual fundamental rights. Measures that are not allowed by law are forbidden and the secret services would act illegally if they nonetheless took action. An example of such an action is the secret search of computers via the internet in order to investigate if users store information about bomb building. German courts have decided in 2007 that such an investigative measure is illegal unless parliament has explicitly allowed it (BGHSt 51, 211). Although the cases were in regard to actions planned by public prosecutors, the standards apply to secret services alike.

Theory and practice have not gone hand in hand for a long time. Until 1990 only the BfV had been based on a parliamentary act, the BND and the MAD had worked without such a basis. In addition tasks and powers had only been rudimentarily regulated. However, since 1990, each federal secret service has its own legal grounding that describes its tasks and powers.[7]

18.2.1.3 The Distinction Between Tasks and Powers

Closely connected to the aforementioned requirement of a statutory (parliamentary) provision is the distinction between tasks and powers within German law. The task ascribed to a public authority does not give the authority the power to take certain measures. There must be a specific provision that clearly states in which cases the authority can act and what exactly the authority can do. The task alone just sets the framework within which the authority is allowed to act. The description of the task alone is not regarded specific enough to fulfil the constitutional requirements of certainty (*Bestimmtheitsgebot*), which is part of the general rule of law (*Rechtsstaatsprinzip*, art. 20 para. 3 GG).

An exception is made for such actions that are not of relevance for individual fundamental rights (Gusy 2006; Schenke 2005). As long as the authority takes measures that do not infringe individual rights, no specific authorization is needed. In this case the description of the task alone is sufficient for the authority to act.

[7] The BfV is regulated by the Act on the cooperation of the Federal Government and the State Governments concerning the Protection of the Constitution and the Federal Office for the Protection of the Constitution ("*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz*" [BVerfSchG]), the BND is regulated by the act on the federal intelligence agency ("*Gesetz über den Bundesnachrichtendienst*" [BNDG]), and the MAD is regulated by the Act on the Military Counter-Intelligence Service ("*Gesetz über den militärischen Abschirmdienst*" [MADG]). In addition to these acts, the Act on Limitations on the Privacy of correspondence, posts, and telecommunications ("*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*" [G-10]) provides powers to supervise postal and electronic communication.The aforementioned acts are available for free on the website of the collection of German federal statutes hosted by the Federal Ministry of Justice: <http://www.gesetze-im-internet.de>.

This means that the secret services can base their internal work, general administrative measures, etc. on the provisions that describe their general tasks. For measures to gather information about citizens in particular by special technical methods, a specific authorization by statute is needed.

18.2.1.4 The Separation of Secret Services and the Police

In German law the principle of separation between secret services and the police (*Trennungsgebot*) is imperative. This separation is the outcome of negative historic experiences during the Third Reich. During this period the combination of secret services and police in one office (the Reich Security Main Office – *Reichssicherheitshauptamt*) was an important element in the terror structure of the Third Reich. After the war the allied occupying powers therefore put emphasize on the separation of secret services and the police (Dorn 2004: 121; Droste 2007: 290; König 2005: 49; Schafranek 2000: 29). The police primarily received coercive powers whereas the secret services primarily received investigative (non-coercive) powers. The separation between the institutions is mentioned explicitly in the acts regulating the secret services. For example section 1 para. 1 BNDG states that no police agency may be affiliated to the BND. The constitution itself is silent on the topic. Whether the separation requirement can be seen as part of the rule of law is highly disputed among scholars (Lisken 1994; Middel 2007: 72; Nehm 2004).[8] The German Federal Constitutional Court has left the question open so far (BVerfGE 97, 217; 100, 369).

The separation between secret services and the police means that there have to be separate authorities, thus an institutional separation is demanded. In addition the secret services are not allowed to possess police powers, such as the power to arrest persons or search houses (BVerfGE 97, 217). Equally, the secret services are not allowed to circumvent the separation by demanding the police take measures the secret services cannot take themselves. Thus, in addition to institutional separation, there has to be a certain separation of executive powers. However, it is not forbidden that police and secret services cooperate (just as other public authorities are allowed to cooperate), which is especially relevant for the exchange of data (see below Sect. 18.3.2.1). Furthermore, the principle of separation has not received much attention in practice, as the following examination of the current legal situation will show. The developments of the last decades have rather reduced the principle to an often cited but substantially neglected legal institution.

[8] Some scholars regard the acts of the allied occupying powers as constitutional documents. However, these acts became void when Germany regained sovereignty. Whether the constitutional rule of law demands the separation between police and secret services is rather doubtful. Certainly this principle wants to avoid the existence of one omnipotent authority, however, such a requirement can be fulfilled even when police and secret services merge partly.

18.2.2 Organizational Structure and Tasks

18.2.2.1 Federal Office for the Protection of the Constitution

The Federal Office for the Protection of the Constitution is, according to section 2, 3 BVerfSchG, a central office (*Bundesoberbehörde*) under the control of the Federal Ministry of the Interior. The Office is mainly situated in Cologne, and had an annual budget of approximately 145 million Euros and employed 2,503 people in the year 2007.[9] During the 1990s the staff number and the budget decreased, but after the year 2000, both numbers have risen again (see Droste 2007: 734).

The BfV has been primarily tasked with the collection and analysis of "information, intelligence and other documents" concerning efforts directed against the free democratic basic order or against the existence and the security of the Federation or one of its States (section 3 BVerfSchG). The task includes the surveillance of the work of foreign secret services in Germany (counterintelligence). These activities are of strong preventive character because they are aimed at the prevention of any endangerment of legal interests (*Rechtsgüter*) in Germany.

By means of the Act on the fight against international terrorism[10] from 2002, these "classic" secret service tasks have been amended in 2002 in order to strengthen the fight against terrorism (Middel : 223; Paeffgen 2002, 2003). Section 3 BVerfSchG now lists the additional task of collecting information of efforts "directed against the idea of international understanding […] especially against the peaceful coexistence of peoples". The wording does not clearly refer to terrorism, but terrorism is commonly understood as the (current) main threat against international relations (Baldus 2002; Denninger 2002; Middel 2007: 225). The new task allows for the surveillance of terrorist activities directed against other countries within Germany even when there is not yet current danger as defined by police law.[11] Because of the low threshold, it is doubtful whether the surveillance of such terrorist activities is in accordance with the German constitution (Baldus 2002; Denninger 2002; Paeffgen 2002). Nonetheless the legislative has extended the application of the amendment until 2012; initially it was foreseen for just a period of 5 years.

---

[9] See the yearly report on the secret services by the Federal Ministry of the Interior: Bundesministerium des Innern, Verfassungsschutzbericht 2007, p. 8.

[10] Gesetz zur Bekämpfung des internationalen Terrorismus, Terrorismusbekämpfungsgesetz – TerrBekG, 9. January 2002, BGBl. I S. 361. The statute was amended in 2007 by the Act amending the fight against terrorism act (*Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes, Terrorismusbekämpfungsergänzungsgesetz* [TerrBekErgG]), 5. January 2007, BGBl. I S. 2.

[11] The requirement of current danger (*konkrete Gefahr*) is important in German (police) law. Only if current danger is given, may the police take investigative and coercive measures. If a situation does not reach the level of current danger, the authorities are not allowed to take such measures.

18.2.2.2 Federal Intelligence Agency

The Federal Intelligence Agency is, according to section 1 BNDG, also a central office with two main locations in Berlin and Pullach (Bavaria). The agency is under control of the (administrative) Head of the Federal Chancellery. Based on estimations, approximately 6,000 people work for the agency and it has an annual budget of approximately 430 million Euro.[12]

The BND has the task to collect and analyze information about foreign countries, which is of relevance for German foreign and security policy (section 1 para. 2 BNDG). This includes information about transnational terrorism and organised crime. The agency is *the* German foreign secret service. The collection of information does not necessarily have to take place outside Germany, but can also be carried out within Germany as long as information about foreign states is collected (Bäumler 1991).

18.2.2.3 Military Counter-Intelligence Service

According to section 1 MADG, the Military Counter-Intelligence Service is a central unit of the Federal Armed Forces and responsible to the Federal Ministry of Defense. The unit has its main office in Cologne; throughout Germany, 14 subordinate offices exist. In 2006 the service employed 1,290 persons and had a budget of approximately 72 million Euro.[13] Similar to the BfV, the service had a cutback in personnel and budget in the 1990s, which increased after 2000 again and has now reached a steady level since 2005 (see Droste 2007: 734).

The MAD has the task to collect and analyze information about activities directed against the constitution (section 1 para. 1 MADG). Like the task of the BfV, this includes the surveillance of (military) counterintelligence. In contrast to the BfV, the MAD is only responsible as far as the activities are of concern for the branch of the Ministry of Defense, thus of military relevance. This is the case when activities are directed against personnel or institutions of the Ministry of Defense or if a person belonging to the branch of the Ministry of Defense participates in such an activity. Similar to the BfV, the task of the MAD has been amended in 2002 and now includes the collection and analysis of information about efforts "directed against the idea of international understanding […] especially against the peaceful coexistence of peoples". Again this is generally understood to refer to the surveillance of terrorist activities. The task of the MAD is primarily limited to activities within Germany. As the German armed forces increasingly participate in missions abroad, the MAD has been allowed to extend its work to countries where German troops are based (section 14 MADG). However, this extension is quite limited, so that the BND remains the main German foreign secret service.

[12] See http://de.wikipedia.org/wiki/Bundesnachrichtendienst.

[13] Bundesministerium des Innern, Verfassungsschutzbericht 2007, p. 8.

18.2.3 Powers

18.2.3.1 Federal Office for the Protection of the Constitution

The BfV has far-reaching powers in order to collect information. The office can gather, process, and use information that is of relevance to fulfil its tasks (section 8 para. 1 BVerfSchG). This information can include personal data about individual persons. The office can use several technical surveillance measures, in order to collect information. For instance, it can track active mobile phones (section 9 para. 4 BVerfSchG). The statute only names some of the measures the BfV can use. Instead it allows in general the use of "methods, objects and instruments for the secret collection of information" (so-called *nachrichtendienstliche Mittel* [secret service measures]) and gives the examples of undercover agents, observations, taking of pictures, sound recordings, forged papers, and license plates (see section 8 para. 2 BVerfSchG).[14]

What kind of secret service measures in addition to the aforementioned are allowed is not completely clear (Droste 2007: 262; Gröpl 1993: 310, 332; Roewer 1987: 112; Rose-Stahl 2006: 70; Singer 2002: 284).[15] At least the open regulation allows the secret services to adjust to new developments without publicly having to describe their new (technical) possibilities (Droste 2007: 265; Rieger 1986: 37; Roewer 1987: 132). However, the use of new techniques is only possible as long as it does not lead to new or intensive encroachments on fundamental rights (see Hirsch 1996: 39; Singer 2002: 298). In such a case parliamentary regulation is needed. For instance the BfV cannot conduct online searches of computers until the BVerfSchG is amended.

Since 2002 the BfV is allowed to require in particular financial, postal, and telecommunications companies to provide information (section 8a BVerfSchG; see Huber 2007) when there are indicators for the commission of a serious crime. In such a case the office can also monitor telecommunication and postal correspondence (section 3 G-10). The list that describes what constitutes a serious crime includes crimes against the state (e.g. high treason), crimes against public order (e.g. founding a terrorist organization), as well as individual crimes such as murder (Paeffgen 2002). Since 2007 the office can also issue a search warrant for persons (in the Schengen information system) without asking the police to do this, as was previously the case (section 17 para. 3 BVerfSchG).

Especially the possibilities to ask companies for information and to issue a search warrant show that the BfV has been assigned powers that have traditionally

[14] It is disputed if section 8 para. 2 BVerfGSchG is merely a description of different measures (Droste 2007: 265) or if it describes the powers of the BfV (Gusy 1991). The correct answer is between these positions: section 8 para. 2 BVerfGSchG gives the BfV the power to use certain measures as long as there is no intensive encroachment on fundamental rights. In case of an intensive encroachment on fundamental rights, a special parliamentary regulation is needed.

[15] Section 8 para. 2 BVerfSchG provides that an internal guideline shall enumerate the measures. The guideline has been issued (Rose-Stahl 2006: 70) but it is not publicly available.

been regarded as police powers. These powers are special because they aim at the investigation of individual cases and are not restricted to the examination of a general threatening situation (Roggan and Bergemann 2007). The possibility of issuing a search warrant is the first measure that grants the BfV direct access to police databases. This is quite remarkable because the division between police and secret services has been regarded as a cornerstone of the German system.

Information that has been gathered by the BfV is collected in the *Nachrichtendienstliches Informationssystem* (NADIS).[16] This system is operated in cooperation with the State Offices for the Protection of the Constitution. It contains more than one million individual-related entries. The information can be transmitted to other authorities. Since 2007 the BfV participates in the so-called *Antiterrordatei* (Anti-Terrorism File) and there is the possibility to set up special files at the BfV, which can be accessed by all German secret services and the police as well. The question of data transmission and cooperation with the police will be further elaborated on below.

18.2.3.2 Federal Intelligence Agency

The powers of the BND are similar to the powers the BfV possesses. The office can gather, process, and use information that is of relevance to fulfil its tasks (section 2 para. 1 BNDG). In 2002 and to 2007, the office received the same new powers as the BfV did (see above).

A special power only the BND possesses is the so-called strategic surveillance of telecommunication (*strategische Fernmeldeüberwachung*; Köhler 1994; Roggan and Kutscha 2006: 427; Zöller 2002: 350). This power allows monitoring of all international communication to and from Germany. The aim of this regulation is primarily to discover terrorist threats as early as possible. However, the power is not limited to the discovery of terrorist scenarios, although its application is limited to the number of crimes listed within the provision (section 5 G-10). In addition to terrorist activities, the provision enumerates the import of narcotics and drugs, counterfeiting of money, and internationally organized money laundering. In particular, counterfeiting and money laundering often have a close connection to German territory, so that it is rather obscure why such an investigative power has been given to the German foreign secret service (Huber 2000; Paeffgen 2002). Besides this question of whether the power is still within the tasks of the BND, the most remarkable aspect concerning strategic surveillance is that it allows an investigation without any further precondition; there does not have to be any threat in terms of police law or a suspicion in terms of criminal procedure law. In short, it allows a criminal investigation without the suspicion of the commission of a criminal offence. Because the BND is quite substantially involved in the investigation of

[16] Secret services' information system.

crimes, it can be seen as a "secret criminal police agency" (Köhler 1994; Pieroth et al. 2005; Roggan and Kutscha 2006: 431).

The BND (like the BfV) is allowed to exchange information with other authorities. Special rules exist for the transmission of information that stems from the strategic surveillance of telecommunication (see the section below "The "Traditional" Way of Exchanging Information"]. The office also participates in the Anti-Terrorism File since 2007. Likewise there is the possibility to set up special files at the BND that could be accessed by the other German secret services and the police as well.

18.2.3.3 Military Counter-Intelligence Service

The powers of the MAD are almost identical with the powers of the BfV. The office can gather, process, and use information that is of relevance to fulfil its tasks. Since 2002 the MAD is also allowed to ask financial, postal, telecommunications and other companies to provide information, when there exists a serious danger to legal interests (*Rechtsgüter*) the MAD has to protect (Huber 2007). When there are indicators for the commission of a serious offence, the office can monitor telecommunication and postal correspondence. Since 2007 the office can issue a search warrant for persons. The MAD is in general allowed to exchange information with other authorities and participates in the Anti-Terrorism File since 2007. The possibility to set up special files has not been provided for the MAD yet.

18.2.4 Conclusion

The secret services are responsible for the collection and analysis of information that is relevant for national security. Their traditional field of work has been to collect information about dangers before there is a concrete threat or suspicion that would allow the police or the public prosecutor to take up their investigations (Nehm 2004). However, especially in the context of fighting terrorism, tasks and powers of the secret services have been amended to prevent and to investigate single serious crimes. These serious crimes are quite broadly defined and include offences of the German criminal code that are closely connected to terrorism (such as the formation of terrorist organizations) as well as "classic" offences (e.g. manslaughter). The broad definition is much due to the fact that the secret services shall fight terrorism whereas there does not exist a crime of terrorism in German criminal law at all.

The powers the secret services have gained during the last decade are substantially traditional police powers. These investigative powers are of a coercive nature because they offer possibilities going far beyond the mere collection of publicly

available information. Because of the principle of separation between police and secret services, the secret services have not been regarded as police agencies (Gusy 2006: para. 37; Kugelmann 2006: 50; Schoch 2005: para. 41). However, equipped with the present powers, the secret services have developed into special police authorities (see Schenke 2005: para. 443; Würtenberger and Heckman 2005: para. 93). This development has not only taken place on the secret services' side. The police also have gained new powers for the investigation of crimes that traditionally have been tailored for the secret services, such as the secret surveillance of persons (section 100a–100i StPO), the automated comparison and transmission of personal data (section 98a StPO), or the use of undercover investigators (section 110a StPO).

Concerning tasks and powers, the separation of police and secret services is by far not as clear as it had been in the decades after the war (Gröpl 1993: 303; Nehm 2004: 3292). The principle of separation has been no bar for the development at all. It rather seems that the principle is regarded to be observed as long as the organizational separation between police and secret services remains untouched (Baumann 2005; König 2005: 255). One has therefore to ask how far both institutions can approach each other. The German constitutional court has made clear so far that the police generally cannot have powers to investigate without the existence of a concrete threat to public security (BVerfGE 113, 348).[17] Thus the police cannot use their investigative powers just to find out if there is any grounds for suspicion. The secret services, on the other hand, cannot receive investigative powers that deeply restrict individual rights in order to resolve minor crimes (BVerfGE 100, 313). The power to collect information in secret and without the existence of a concrete threat or suspicions must go hand in hand with a limitation of the power to prevent or investigate only the most serious crimes. Thus the secret services cannot be turned into a general criminal police (unless they will be equipped with less far-reaching powers).

18.3 Cooperation of the Secret Services' and Criminal Justice Institutions

As the foregoing analysis has shown, the secret services have become a relevant player in regard to criminal matters. It is therefore important to take a look at the modes of cooperation between the secret services and the traditional criminal justice institutions. Traditional criminal justice institutions are the police, the prosecution, the court, and the defence. To provide better understanding, their functions will be sketched in brief.

[17] The court did not base its decision on the separation of police and secret services but mainly on the grave infringement of individual rights.

The police have investigative powers and are the authority to execute coercive measures.[18] The prosecution is the responsible authority for the investigation and supervises the police. In practice a case is often handled by the police alone before a final report is submitted to the prosecution. In cases of serious crimes, the prosecution is involved in the investigation right from the beginning. Police and prosecution collect evidence against and in favour of the accused. During the investigative proceedings (*Ermittlungsverfahren*), the court is only involved when a decision on coercive measures is needed. The power to order coercive measures rests almost exclusively with a special investigating judge, apart from cases of urgency, when the prosecution and the police can take preliminary measures. When sufficient evidence is collected, the prosecution takes the decision to indict or not. If an indictment is issued, the court (different from the investigating judge) takes over the proceedings and is responsible for the case until a judgment is reached. The defence, although formally an impartial organ, acts in practice primarily on behalf of the accused in all stages of the proceedings.

18.3.1 Constitutional Framework for the Exchange of Information

Cooperation often means the exchange of information gathered and processed by public authorities. It has already been mentioned that the constitution requires a statutory provision if the action of an authority encroaches on fundamental rights. Insofar as the collection of information touches the right of privacy of correspondence, posts, and telecommunications (art. 10 GG) or the right of inviolability of the home (art. 13 GG), the statutory requirement is quite obvious. However, in many cases the collection of information does not encroach on these rights (e.g. when publicly available information is collected). Equally the processing, committing, or transmission of data does not affect these rights. The constitution

[18]To speak of the police is a simplification because there are numerous police authorities in Germany. The police have two main functions: the preventive function to fight threats to public security and the repressive function to investigate crimes. For each function there exists a different legal framework. Preventive measures are primarily regulated in special state and federal police laws (*Polizeigesetze*), whereas repressive measures are regulated in the code of criminal procedure (StPO). There are different two categories of police officers: officers that are so-called investigators working for the prosecution (*Ermittlungsbeamte der Staatsanwaltschaft*) who are endowed special investigative powers, and there are all the other officers who only have a limited set of investigative powers. The main police power rests with the states. But there are also several federal police authorities. The most important federal police authorities are the Federal Criminal Police Office (*Bundeskriminalamt* [BKA]) and the Federal Police (*Bundespolizei*, formerly the Federal Border Police, *Bundesgrenzschutz*). According to the two functions, the state police are often organized in two different ways: the protective police (*Schutzpolizei*) and the criminal police (*Kriminalpolizei*). In general only the criminal police deals with crimes. As far as the following text speaks of the police, primarily the police in its repressive function is referred to.

does not provide explicitly for a general right to the protection of ones personal data. Nonetheless in 1983 the German Federal Constitutional Court recognized a right of informational self-determination (*Recht auf informationelle Selbstbestimmung*, BVerfGE 65, 1). This right is part of the general right of privacy (*Allgemeines Persönlichkeitsrecht*).[19]

The right of informational self-determination is encroached by the collection, the storing, the use, and the transmission of data. Such measures can only be justified by a statutory provision that pursues a constitutionally recognized aim.[20] The constitutional court has accepted that the aim to investigate and solve serious crimes can justify an encroachment on the right of informational self-determination (BVerfGE 103, 21; BVerfGE 118, 168). The court emphasizes that the aim to solve crimes provides no automatic ground for justification. In every single case the measure's proportionality has to be evaluated; thus the public interest in a criminal prosecution has to be weighed against the individual right to informational self-determination.

Since the judgment in 1983, the legislator has created numerous regulations for the collection and the exchange of information between public authorities (Zöller 2002: 53).[21] The legislator has been so active that by now there is almost no area without regulations that allow for an exhaustive exchange of information between public authorities. In addition, the number of regulations that permit the collection of information has substantially increased. In recent years the constitutional court has therefore ruled several times on the question of how far the exchange of information can go and what constitutional conditions a legal regulation must fulfil.

The court has declared several statutes unconstitutional because they contained regulations violating the right of informational self-determination or the right of privacy of telecommunications, such as the secret collection and transmission of information by the secret services (BVerfGE 100, 313), the secret collection and transmission of information by the customs criminal office (*Zollkriminalamt*, BVerfGE 110, 33), or the automatic recording of license plate numbers by the police in order to track criminal suspects (BVerfG, NJW 2008, 1505). Many of these regulations were too

[19]This right itself is not explicitly mentioned in the constitution but derived from art. 1 para. 1 GG (human dignity – *Menschenwürde*) in conjunction with art. 2 para. 1 (general freedom to act – *Allgemeine Handlungsfreiheit*).

[20]The German Federal Supreme Court regularly follows a three-step examination when it considers the legality of measures by public authorities: First, does the measure affect the scope (*Schutzbereich*) of the fundamental right in question? Second, is the measure an infringement (*Eingriff*) of the right? Third, is there a justification (*Rechtfertigung*) because the measure aims at the protection of other fundamental rights or constitutional values?

[21]The Federal Act concerning the Protection of Personal Data (*Bundesdatenschutzgesetz* [BDSG]) is the central piece of legislation concerning data protection. It regulates the collection and storing of data in general and provides for special mechanism of protection (e.g. the control by data protection commissioners). The act is supplemented by specific regulations: e.g. regulations within the statutes governing the secret services, within the police statutes, or within the code of criminal procedure.

general and their scope of application unclear; the regulations lacked certainty (*Normenbestimmtheit*) and proportionality (*Verhältnismäßigkeit*).

In 2008 the constitutional court recognized a new constitutional right, the guarantee of confidentiality and integrity of information technology systems as a specification of the general right of privacy. The court considered the secret search and surveillance of computers via the internet by a state police to be unconstitutional (BVerfG, NJW 2008, 822; Kutscha 2008: 1042). Information stored in a personal computer can reveal many aspects about the personality of its user, including private details. The secret access to such information by the state must be limited to interests of upmost public importance under clearly defined circumstances.

The rulings of the constitutional court mean that a legal provision justifying an encroachment on the right to informational self-determination or the guarantee of confidentiality and integrity of information technology by the secret services must clearly state who knows what and when about whom. The provision must precisely define the situation when it is applicable and give the purpose for which the collected information will be used. Any use of the information is limited to the given purpose. It is not allowed to collect and store personal information for an unspecified purpose in the future.

For the exchange of data between different public authorities, the ruling means that it is only allowed when a special legal regulation allowing the exchange of data exists. Exchanged data may also only be used for the stated purpose. If data shall be transmitted for another purpose than the one it has been collected for, there has to be a specific provision allowing for the change of purpose (*Zweckänderung*, see Golembiewski 2000: 51; Roggan and Kutscha 2006: 448 ff.). For instance information that has been collected in order to prevent threats to public security may not be transmitted to other authorities in order to prosecute crimes, unless a parliamentary regulation allows it. In addition, such a regulation has to be specifically balanced. For instance the threshold to transmit information for criminal proceedings is higher than the one to transmit information in order to prevent a crime, because the interest in preventing harm is higher than the one to investigate incidents in the past (BVerfGE 100, 313, 394; see also Würtenberger and Heckmann 2005).

To give an example, the constitutional court considered regulations that allowed the federal intelligence agency to transmit information to the prosecution as unconstitutional (BVerfGE 100, 313). The regulations were not restricted to the transmission in cases of serious crimes and it allowed information to be transmitted whose factual basis was below the threshold the code of criminal procedure sets in order to start an investigation. The far-reaching powers to conduct secret investigations by the secret services allowed measures that the prosecution could not conduct by itself. The court concluded therefore that the prosecution should only be allowed to receive information by the secret services where there exists a special public interest (such as in the cases of serious crimes, but not in the cases of street crimes) and where the factual basis of the information is not below the one in the code of criminal procedure. Following the decision the legislator has limited the exchange of information (see above Sect. 18.2.3.2).

18.3.2 Cooperation in Detail

18.3.2.1 Cooperation with the Police

The tasks of the secret services and the police are similar insofar as they both aim at preventing threats to public security and investigating crimes. Therefore the cooperation between the secret services and the police is closer than the cooperation between the secret services and other criminal justice institutions. As mentioned above the principle of separation is the main barrier to merging both institutions, although the principle has not barred the police from receiving powers of the secret services and vice versa. As we will see, the principle has also been no bar to a close de facto cooperation of both institutions.

The "Traditional" Way of Exchanging Information

The most important kind of cooperation between the secret services and the police is the exchange of information. The principle of separation does not aim at the exclusion of the possibility of an exchange of information as this would make the work in the field of public security quite inefficient (Albert 2000; Nehm 2004; Wolff and Scheffczyk 2008; Zöller 2002: 323). The principle merely shall secure that there is neither an all-embracing informational network among both institutions nor an unlimited right to access the databases of the other institution (Hirsch 1996: 97; König 2005: 256; Roggan and Bergemann 2007).

The "traditional way" of cooperation in ongoing proceedings between the secret services and the police is governed by the legal institution of administrative assistance. This institution shall enable the efficient handling of cases where tasks and powers have been distributed among different authorities (Pünder 2006). However, only the basic aspects of administrative assistance are regulated by law.[22] Especially the transmission of information (so-called information aid – *Informationshilfe*) is not regulated in detail.[23] Because these regulations do not fulfil the requirements of a specific parliamentary regulation (see above Sect. 18.3.1),

[22] See art. 35 para. 1 GG (administrative assistance between federal and state authorities) as well as section 4 of the federal administrative procedure act (*Bundesverwaltungsverfahrensgesetz*) and the similar regulations in the state administrative procedure acts (*Landesverwaltungsverfahrensgesetze*).

[23] Administrative assistance is only possible when the following preconditions are fulfilled: A request for assistance must be limited to a special part of an ongoing proceeding. It is not allowed to ask another authority to take over whole proceedings. The requesting authority is also not allowed to extend its tasks and powers just by asking another authority to do it (Lisken and Denninger 2007: 388; Schlink 1982: 108); it is limited to file a request that is within its own tasks and powers. Equally the requested authority can only act within its own tasks and powers, it cannot borrow powers from the requesting authority. The requested authority is bound by the request and is not allowed to make decisions on its own, it is just the "extended arm" of the requesting authority.

the transmission of information is limited to an exchange of non-personal information in single cases on the request of another authority (see Droste 2007: 473). Any further exchange (e.g. the constant transmission of personal information) requires an extra parliamentary regulation. Therefore all the statutes governing the secret services now contain detailed regulations on the exchange of information (see sections 18–20 BVerfSchG, sections 8–9 BNDG, and sections 10–11 MADG).

The police are allowed to transmit information to the secret services when the information is of relevance for the tasks of the secret services (see Soiné 2007). Equally the secret services can transmit information that is of relevance for the tasks of the police (Droste 2007: 518). Because the institutions are not obliged to transmit information, they can evaluate whether the transmission of information is within their interest or not. A very broad exception is made when the police receive information about foreign secret service activities or violent acts against the state, which includes terrorist activities. In these cases the police are obliged to inform the secret services (section 18 para. 1 BVerfSchG). Another exception is made when the secret services receive information about the commission of serious crimes against the state (e.g. high treason). Then the services are obliged to inform the police.[24] The secret services can also request the police to provide any information they need for their work. However, vice versa, the police have only the right to request information if it concerns the already mentioned serious crimes against the state.

Special rules exist for the transmission of data by the BND gained by the strategic surveillance of telecommunication (see 18.2.3.2). The power of the BND to collect information by strategic surveillance includes also the power to transmit the information to the police and the prosecutorial authorities, when the BND gains knowledge about a threat to public security or about a suspected criminal offence (Paeffgen 2003: 653). However, the transmission of information is only allowed in cases in which a concrete threat or a concrete suspicion is given. This means that the police and prosecution can only receive information at a stage where they are allowed (and the prosecution obliged) by law to take action. Information that is not substantial enough in order to constitute a concrete threat in terms of police law or a suspicion in terms of criminal procedure law will never leave the BND. The important question in such cases is who decides if the information is concrete enough to be transmitted? The answer is quite simple: the BND alone does, although not every person in the agency is allowed to make the decision, only a lawyer is. The BND is not bound by the principle of mandatory prosecution (see below Sect. 18.3.2.2) and can therefore refrain from submitting information to the prosecution when there are prevailing interests of the agency (e.g. in order to keep the names of informants secret).

[24] Schünemann (2008) denies a right of the secret services to transmit information to the police if it does not concern serious crimes against the state because of the principle of separation between secret services and the police. Yet this understanding would be against the clear wording of section 19 para. 1 BVerfSchG, section 9 para. 1 BNDG (see also Droste 2007: 519).

The Anti-Terrorism File (ATDG)[25]

In addition to the aforementioned "traditional" possibilities to exchange information, a complete novelty in the field of informational cooperation was introduced in 2006. The legislator created the already mentioned Anti-Terrorism File (Roggan and Bergemann 2007; Ruhmannseder 2007; Wolff and Scheffczyck 2008; Zöller 2007).[26] This so-called file is a joint database hosted by the *Bundeskriminalamt* (BKA)[27] to which police and secret services have automatic access (and do not need to contact the other institution any more). Federal and state police participate in the project as well as the federal secret services and the state offices for the protection of the constitution (section 1 ATDG). The database contains information about natural persons, legal persons, and about objects that are connected to terrorist activities. The information covers future as well as past activities. The database aims at the collection of information for the prevention as well as the investigation of terrorist activities.

In order to guarantee data protection, only a limited set of information is available through the automatic access, the so-called basic data set (*Grunddatensatz*, section 3 ATDG). However, already this data set includes a substantive amount of personal information (e.g. name, date of birth, address, spoken languages, and special physical features). An enlarged basic data set (*erweiterter Grunddatensatz*) exists, which contains the complete information of the databank about a person or an object. This enlarged data set is only available when a request is filed at the authority that had entered the information into the databank. The procedure resembles the traditional path of administrative assistance, but is much faster because one can find the authority possessing information by simply checking the database. In an emergency case, the enlarged data set can be accessed without such a request. The enlarged data set can include almost any possible information (about bank accounts, cars, special abilities for example in using weapons, and so on). It is also possible to save comments, notes, and assessments within the file. Thus, the databank provides an investigator with great detail (Zöller 2007).

Information is not only collected about suspects, but also about persons having contact with a suspect (contact person). Information about a contact person shall only be stored if the authority expects this person to contribute to the investigation of terrorist activities. This vague and subjective restriction will not be very efficient in limiting the storage of data of innocent persons (Ruhmannseder 2007). The use of the stored data is not restricted to the aim of the Anti-Terrorism File because information can be used for example for criminal proceedings (section 6 ATDG).

---

[25] See also Stock and Herz, this volume.

[26] See the Act on the establishment of a standardised central anti-terrorism-file for federal and state police and secret services (*Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern, Antiterrordateigesetz* [ATDG]), 22 December 2006, BGBl. I S. 3409.

[27] Federal Criminal Police Office.

The only restrictions are that a serious crime (that is not specified in more detail by the act) must be concerned and that the authority that has entered the information into the databank agrees with the use of the information.

The Anti-Terrorism File is remarkable in several ways. The principle of separation between police and secret services seems to be no barrier to joint institutions and to a very intensive informational cooperation so that the principle has become even less important than it has already been (Wolff and Scheffczyk 2008 are, therefore, critical). In addition, the constitutional right of informational self-determination or the guarantee of confidentiality and integrity of information technology seemed not to have played any vital part in the drafting of the act. The pure amount of information that can be stored, the potential to store (biased?) commentaries, and at last the very broad competence to use information not only in terrorist proceedings but also in other non-specified cases of serious crimes let one doubt whether the act is in accordance with constitutional law (see Ruhmannseder 2007; Wolff and Scheffczyk 2008; Zöller 2007). Because the act also aims at the investigation of committed terrorist acts, it is very questionable not to include the prosecution.[28] In the German system the prosecution is responsible for supervising the police during the investigation of crimes. It has been regarded a problem for many years that the prosecution does not have access to existing police databases (see Ringwald 1988; Wolter 1999; Zöller 2002: 172). With the installation of such a substantive database for a special set of crimes, the ability of the prosecution to actually conduct and guide investigations is highly diminished.

The Possibility to Establish Additional Databases

The same legislation that installed the Anti-Terrorism File provided for the possibility to establish other joint databases of the police and the secret services (see section 9a BKAG,[29] section 9a BNDG, section 22a BVerfSchG). The establishment has to be temporary and is limited to certain crimes or certain threats to public security that are covered by the tasks of the secret services. The databases can be introduced by the police or the secret services without any further parliamentary legislation or consent by parliament. Only the federal ministries concerned have to approve the introduction of the database. The legal framework contains very general guidelines so that the authorities introducing the databases are left with

[28]The only exception is the possibility of the federal attorney general (Generalbundesanwalt) to use information of the Anti-Terrorism File via the participating police institutions (section 6 para. 4 ATDG). However, this is only a mediated kind of participation and does not include the state prosecution that is in principle responsible for the prosecution of the crimes mentioned in the ATDG.

[29]BKAG – *Gesetz über das Bundeskriminalamts und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten* (Act on the Federal Criminal Police Office and the cooperation of the federation and the states in criminal matters).

vast discretion. This discretion is very problematic in regard to the constitutional requirement of a precise parliamentary provision (important points are not decided by parliament but left almost completely to the establishing authority), the right to informational self-determination, and of course the principle of separation between police and secret services. It is quite doubtful whether these regulations are constitutional in their present form (see Roggan and Bergemann 2007 and the *Bundesbeauftragte für Datenschutz und Informationsfreiheit*[30] 2007: 60).

Organizational Cooperation

Beyond the exchange of information, police and secret services partly work together. This is no new development. Traditionally the police can ask the members of the secret services to join the investigation of certain serious crimes against the state. Administrative assistance allows for such cooperation and the guidelines for the prosecution explicitly mention it (see no. 205 para. 5 RiStBV; Nehm 2004). Apart from this case-related cooperation, police and secret services coordinate their work in fields in which their tasks overlap. Such coordination for example takes place in special workshops. In recent years the coordination has begun to become more institutionalized by establishing regular group meetings, coordinating for instance the work in the fields of terrorism or extremism (Albert 2002; Droste 2007: 577; Schreiber 1996). In the days immediately following the events of September 11, 2001, a special organizational structure was established for several months; within this structure members of the secret services and the police worked together.[31]

In order to institutionalize the coordination against terrorism on a long-term basis, the *Gemeinsames Terrorismusabwehrzentrum*[32] (GTAZ) was established in Berlin in 2004 (Baumann 2005; Kerner et al. 2006; Schily 2006). Almost 200 members of the federal and state police, the federal secret services, and the state offices for the protection of the constitution work there together. Unlike in relation to the anti-terrorism file, the federal attorney general (*Generalbundesanwalt*) also participates. In order not to merge police and secret services too much, the centre is divided into two different sections: into a police division and into a secret services division.[33] Both divisions meet in regular panels where cases are discussed, potentially threatening situations are evaluated, and information is exchanged. Insofar as police and secret services are divided into two sections, there is a certain guarantee that no police officer has direct access to secret services databases and vice versa.

---

[30]For information on and by the Federal data protection commissioner, see the website under <http://www.bfdi.bund.de>.

[31]In addition to German officers, officials of Europol and the FBI participated; see the description of the German government in response to a parliamentary inquiry BT-Drs. 16/892.

[32]Joint anti-terrorism centre.

[33]The police division is called the *Polizeiliche Informations- und Analysestelle* (PIAS) and accordingly the secret service division is called *Nachrichtendienstliche Informations- und Analysestelle* (NIAS).

In 2007 another institution was opened in Berlin, the *Gemeinsame Internet-Zentrum*[34] (GIZ). In this centre the Federal Criminal Police Office (BKA), the federal secret services, and the federal attorney general work together. The task of the centre is a general analysis of the internet in regard to terrorist activities by monitoring websites of extremists and by collecting and analysing publicly available information.

Conclusion

Taking the development in regard to informational and organizational cooperation into account, one has to concede that by now a very close and intensive connection between police and secret services exists. The principle of separation is formally obeyed as both institutions just work side by side (and are not merged into one joint office) and exchange information (and do not have automatic and complete access to each other's databanks). Apart from this formal separation, not many barriers exist, especially in regard to the exchange of information when members of both institutions sit together in one centre on a permanent basis (for critique, see Bundesbeauftragte für Datenschutz und Informationsfreiheit 2007: 65 f.; Roggan and Bergemann 2007; Sieber 2007; Zöller 2007). In substance the principle of separation has been reduced to a purely formalistic approach and does not guarantee an effective control of the powers of police and secret services.

18.3.2.2 Cooperation with the Prosecution

Whereas cooperation between secret services and police is quite extensive, contacts between the prosecution and the secret services are rather scarce in comparison. If cooperation takes place it is, in most cases, restricted to the exchange of information.

Like the police the prosecution is allowed to transmit information to the secret services, when the information is of relevance for the tasks of the secret services. The secret services can also request the prosecution to provide any information they need for their work. On the other side the secret services can transmit information that the prosecution may need for the task of investigating crimes. Again exceptions are made for the transmission of information concerning foreign secret services activities and especially terrorist activities. In this case the prosecution has to inform the secret services. The other exception is made for information about the commission of serious crimes against the state. In this case the agencies are obliged to inform the prosecution. Apart from these provisions regulated in the acts on the secret services, the prosecution has the right to request information from the secret services as from any other public authority. This power is based on the code of criminal procedure (section 161 para. 1 StPO; see Martin 1966; Roggan and Kutscha 2006: 501 f.).

[34] Joint Internet Center.

As mentioned above the BND is not obliged to transmit information about crimes that the BND has gained during the strategic surveillance of telecommunication. This rule applies equally to all powers and all secret services. The secret services are not part of the prosecution or under the supervision of the prosecution and therefore not bound by the requirement of mandatory prosecution. This principle of criminal procedure law (art. 152 StPO) requires the prosecution (and the police as well) to investigate all cases as soon as a suspicion is given. Because the law on the secret services does not explicitly extend the principle to the secret services (see section 20 BVerfSchG), the agencies are not required to inform the prosecution about a crime they discover during their work.[35] Instead they are allowed to make use of their administrative discretion in order to decide whether it is in the interest of the agency to inform the prosecution or not (Roggan and Kutscha 2006: 500; see also Gröpl 1993: 318).

Cooperation beyond the exchange of information does not commonly take place, but is not impossible. The internal guidelines for the prosecution advise the prosecution (similar to the police) to request the secret services to take part in an ongoing investigation on crimes committed against the state (see no. 205, 206 RiStBV).[36] Secret service agents can be of great use because of their expert knowledge on criminal organizations (Droste 2007: 299; Martin 1966). The guidelines propose to contact the secret services at an early stage in order to exchange information and to coordinate further proceedings. Likewise the secret services can ask the prosecution to take part in the interrogation of informants or other persons (Soiné 2007). Such coordination is covered (in absence of a special parliamentary regulation) by the general rules of administrative assistance.

The limits of cooperation are often not very clear, and it might be this uncertainty that causes the secret services to tend to interpret the scope of possible assistance in a rather broad way (for critique, see Lisken and Denninger 2007: 115). A prominent recent example can show the difficulties. A former employee of a Liechtenstein bank had illegally copied information at his workplace about Germans who had illegally transferred money to Liechtenstein in order to escape German taxes (see Schünemann 2008; Sieber 2008; Trüg and Habetha 2008).[37] The employee asked the BND if the agency wanted to buy the information. The BND informed the tax authorities (that are also partly responsible for criminal prosecutions). The tax authorities were interested in the information, asked the BND to buy the data, and promised to pay the costs. The BND met the employee, paid him, received the data,

[35] An exception is made in cases of serious crimes where the "Failure to Report Planned Crimes" constitutes a crime itself (see section 138 StGB). In this case the discretion is reduced to zero (Borgs-Maciejewski and Ebert 1986: § 3 BVerfSchG para. 38; Singer 2002: 63).

[36] The guidelines for proceedings in criminal matters and matters of administrative offences (*Richtlinien für das Strafverfahren und das Bußgeldverfahren* [RiStBV]) are no statutes but internal administrative regulations issued by the federal and state ministries of justice. Nonetheless the guidelines are binding for the prosecution.

[37] The case is still under investigation therefore not all facts are clarified. The facts in the text are based on the information given by Sieber 2008 and Trüg and Habetha 2008.

and gave it to the tax authorities. The information enabled the tax authorities to take up criminal proceedings against a number of Germans because of alleged tax crimes.

The case raises several difficult legal questions (see Schünemann 2008; Sieber 2008; Trüg and Habetha 2008). Was the cooperation between BND and tax authorities legal? Whereas the BND was allowed to inform the tax authorities about the informant, it is questionable if the additional help was legal. The BND has the power to pay informants, but the investigation of tax crimes is clearly beyond its mandate unless the BND expected information about the financing of terrorism (which was very unlikely). On the other side the tax authorities respectively are not allowed to pay informants (because there is no legal provision allowing it), whereas it is clearly within their task to investigate tax crimes. Administrative assistance does not allow the tax authorities to ask the BND to use powers the tax authorities do not have themselves. Likewise the BND cannot borrow the task to prosecute tax crimes from the tax authorities. Thus the combination of tasks and powers from both authorities seems to be illegal.[38]

A new development is the participation of the prosecution in the joint anti-terrorism centre and the joint internet centre as it is allows for a constant cooperation not restricted to a case-by-case basis. Because the centre aims at the prevention of future and the investigation of past terrorist acts, it is a positive development that the prosecution (the institution legally in charge of the investigation of crimes) is included. Unfortunately only the federal attorney general (*Generalbundesanwalt*) takes part in these centres. This is quite problematic because the federal attorney general is responsible for the investigation of a very limited number of crimes (see sections 142a, 120 GVG). The state prosecution is the body that is in general responsible for criminal investigations. In German law there exists no special crime of terrorism, its different aspects are covered by various criminal offences and not all of them can be prosecuted by the federal attorney general. The state prosecution has quite a disadvantage in comparison to the federal attorney general when the state prosecution has to investigate a case and has not been involved in the investigation right from the beginning. The state prosecution must wait until it is informed by one of the participants in the centre. It is hard to imagine how the state prosecution can actually guide an investigation in such a case.

18.3.2.3 Cooperation with the Courts

Cooperation between the courts and the secret services rarely takes place (see Droste 2007: 588). This is mainly due to the late involvement of courts in criminal proceedings. If information of the secret services is relevant for a criminal prosecution, this information

[38]The question following this conclusion is whether the information received can be used in criminal proceedings. Assuming that the acquisition of the information was illegal, the information as such would probably not be allowed as evidence in court. However, any information gathered just as a consequence of the original information would probably not be banned as evidence, because the German system does not now a general fruit-of-the-poisonous-tree doctrine (see below under Sect. 16.4.3).

regularly is sent to the police or the prosecution and can then be found in the case file. The case file the prosecution compiles is completely sent to the court, so that the court has the same information as the prosecution. Because the courts do not conduct investigations themselves, it rarely happens that courts have information that is relevant for the secret services and that has not already be sent to them by the police or prosecution.

An exchange of information is not completely excluded by law. The secret services are allowed to transmit information to the courts, if the courts need it in a criminal proceeding (see sections 19 BVerfSchG, 9 BNDG; 11 para 1 MADG). The secret services can also request the courts to transmit information they need for their work (section 18 para. 3 BVerfSchG). Apart from these regulations no legal provisions exist, in particular there exists no explicit possibility for the courts to transmit information to the secret services on their own initiative (critical Droste 2007: 599). This can be explained by the impartiality of the courts, which could be impaired if the courts provide information to secret services. The most common kind of cooperation probably is the request of the secret services to be granted the inspection of the case file because the services did not get to know the case in an earlier stage of the proceeding. This kind of cooperation is covered by the aforementioned regulations and the principles of administrative assistance.

In many cases the court will first get to know about the involvement of the secret services in a criminal proceeding when reading the case file. The court has then the power to request evidence from the secret services (Martin 1966). The main question in such a case is whether the results of the investigations of the secret services can be used as evidence. In view of the comprehensive powers of the secret services for conducting criminal investigations themselves as well as the possibility to introduce information not collected for criminal purposes into criminal proceedings (by informing the police/prosecution), this situation is not unlikely to happen. Because the powers of the secret service have been extended substantially in recent years, the probability is much higher than a decade ago. However, the use of secret service information as evidence is not without problems: the criminal proceedings in court are public, the work of the secret services is to remain secret. It is obvious that there is a tension between these two aspects. The main problems that arise will be depicted in the following section (see Sect. 18.4).

18.3.3 The Defense and the Secret Services

There exists no formal cooperation or contact between the defence and the secret services. Hence there is no notification of the defence that certain investigative measures are to take place or have taken place. The existing possibility to question secret service measures in a proceeding before an administrative court is therefore mostly theoretically (Huber 2007; Sieber 2008). Partly it is not even possible to reach a judicial decision. Instead of judicial review, German law provides for a parliamentary control (Hirsch 1996: 191). However, this kind of control is rather weak, especially

because of the small number of members of the control committee. The problem has become worse in recent years because the increasing tasks and powers of the secret services have not been equally balanced by an increase in parliamentary control or other measures (Gusy 2008).

There is no right of the defence to get access to the files that the secret services keep about a client. The only possibility for the defence is to assert the rights of its client such as the right to information. However, without being informed, it is unlikely to get to know about an ongoing proceeding (Lisken and Denninger 2007). Even when the defence gets to know, there are many grounds to deny a claim (e.g. because it would endanger the work of the services or there are prevailing interest of secrecy, see section 15 BVerfSchG).

In many cases the defence will not find out about the involvement of the secret services until the prosecution grants access to the case file (of the criminal proceeding). The defence has then the right to see the original and complete case file (section 147 StPO). However, if the file contains restricted, confidential, or secret information of the secret services, the right might be limited. Such a limitation can be that the defence is not allowed to take the file to their lawyer's office, that they are not allowed to make copies of documents, or that they are not allowed to take notes (see no. 213 RiStBV). If the content of documents can endanger public security, the documents can even be removed from the file before the defence receives it (Meyer-Goßner 2007: § 147 para. 14). Although in this case the documents might not be used as evidence in court (see in detail below, in Sect. 18.4.1), the defence cannot find out if there is evidence in favour of the accused. Altogether the position of the defence is rather weak if the defence wants to get to know or to question information collected by the secret services.

18.4 Problems Arising from the Use of Secret Services' Information in Criminal Proceedings

As seen above the secret services have far-reaching powers to collect information relevant for criminal proceedings and they also have the possibility to transmit this information to criminal justice institutions. The use of such information often substantially changes the way the criminal proceeding is conducted. The traditional public proceeding experiences a number of restrictions on the law of evidence, which can lead to a partially secret proceeding.[39] The following section analyses the current approach of the courts to strike a balance between the traditional criminal proceeding and the interests of the secret services to keep information secret. The greatest problems arise in regard to the use of documents produced by the secret services, the hearing of witnesses, and questions on the admissibility of evidence.

[39] Because the police have received powers in recent decades to conduct investigations in secret, some of the problems depicted in the text also apply to the use of evidence collected by the police.

18.4.1 Documents

Information in a file or other written information that is in possession of the secret services and that can be used as evidence in criminal proceedings (and thus in a public hearing) must be handed out to the prosecution or the court. Section 96 StPO provides an exception to this general rule. Authorities can deny a request for the submission or delivery of documents when they declare that the publication of these files or documents would be detrimental to state's welfare (see Paeffgen 2003). Thus, the secret services can withhold documents (including names or statements of witnesses, records of conversations, or pictures of observations) claiming that their publication would endanger their work and public security.

German courts have clarified that it is not enough that the secret services just claim that their work would be endangered by the publication of documents. The authority has to state concrete facts that enable the court to understand the decision of the authority (see BVerwGE 75, 1 and BVerfGE 57, 250). The fact that documents are of relevance for the general work of the secret services does not suffice in order to deny their production (BVerwGE 75, 1). The declaration also cannot be given by any department but must be given by the superior authority. The court has to ascertain if there is no other possibility than to withhold the document, for example by blackening names. However, the alternatives are limited because for example "in camera" proceedings are not allowed in criminal trials (BGH NStZ 2000, 265).

If the authority does not want to withdraw its decision, the court cannot use the documents in the criminal proceeding. The court does not have the possibility to take legal measures against the refusal of the authority (BGHSt 32, 115). The only exception is made in case of an obvious illegal refusal to produce documents. In this case a court can order the seizure of the documents (BGHSt 38, 237). Unlike the court the accused has the right to question the refusal in another procedure, mainly in front of an administrative court (BGHSt 44, 107). However, neither the court asking the authority to rethink its decision nor the accused questioning the decision in an administrative proceeding are very likely to be successful; the secret services have discretion in deciding whether the interest to keep information secret or the public prosecution shall prevail (see BVerfGE 57, 250; BGHSt 44, 107). As long as the secret services provide some plausible arguments for their decision, the documents will not be handed to the courts. Thus, the secret services (and not the court or the defence) have great influence on a criminal trial because they can decide what kind of evidence cannot be used.

18.4.2 Witnesses

As shown, the secret services have the power to observe persons in secret. Observation (besides the use of technical measures) can take different forms: the secret services

can use their own personnel or they can ask individuals to work for the agencies (see Ellbogen 2004).[40] When these persons have observed the commission of a crime, the question of whether they can give evidence in court arises. Very often the secret services do not want to let their personnel give evidence, because this could reveal the identity of the employee or the involvement of the secret services in a certain case. Likewise individuals frequently do not want to reveal their identity (and make public their work for the secret services). In many cases the promise to keep their identity secret is a precondition for their work for the secret services (Soiné 2007).

The problem legally arising for the taking of evidence is that the German criminal procedure system is based on the principle of examination in person. This means, according to section 250 StPO, if "the proof of a fact is based on the observation of a person, such person shall be examined at the main hearing. The examination shall not be replaced by reading out the record of a previous examination or reading out a written statement". Thus, the law of evidence and the interests of secrecy are conflicting.

18.4.2.1 Withholding Witnesses

In order to keep the identity of persons secret, the secret services can declare that these persons are withheld as witnesses. This can lead to the situation that decisive witnesses cannot testify in court and the court might not be able to reconstruct the crime. The declaration to withhold a witness is regarded possible by applying the aforementioned section 96 not only to documents but also to persons (Eisenberg 2006: 298; Ellbogen 2004: 140; Kühne 2007: 528). A special regulation for undercover investigators exists in section 110b para. 3 StPO. The superior authority must declare that the publication of the identity of the person would be detrimental to the welfare of the state.[41]

The German Federal Constitutional Court has accepted that an endangerment of health, life, and liberty of the potential witness is a ground for justification that the identity of the witness is not revealed (BVerfGE 57, 250). It is equally accepted that the promise to keep one person's identity secret or the need to use

[40] The personnel of the secret services can work as undercover agents who observe certain persons on a long-term basis. They can also just work on a single case and are then called undercover investigators (*Verdeckte Ermittler*, see section 110a StPO). There is also the possibility that employees have no special cover and just observe a person secretly. Individuals who work for the agencies are called informants if they just provide information (*Informant*, see no. 2.1 RiStBV annex D). Individuals who work for the agencies on a long-term basis in order to investigate crimes are called confidants (*Vertrauensperson, V-Person*, see no. 2.2 RiStBV annex D).

[41] The statement of any other authority, for example the prosecution that wants to keep the names of informants confidential, is of no relevance for the court (BGH NStZ 2001, 333).

the person for further secret observations are grounds for withholding the person as a witness (Eisenberg 2006: 299; Ellbogen 2004: 146). However, the constitutional court has also made clear that it is not enough that the authority claims the existence of threat to the welfare of the state (BVerfGE 57, 250). The criminal court must investigate the grounds for withholding the witness and must evaluate whether there are other means of protection for the witness (BGH StV 1989, 284; BGH NStZ 2005, 43). However, as long as the secret services provide plausible arguments, the court has no possibility of challenging their decision. In the end it is the secret services (and not the criminal court) who decide whether a witness is allowed to testify.

18.4.2.2 Denial of Authorization to Testify

Another possibility on side of the secret services is not to withhold the witness completely but not to give the person the authorization to testify (*Aussagegenehmigung*, section 54 StPO). This is only possible when the person is employed by the agency or formally committed to keep his work for the agency secret. Before accepting the denial the criminal court has to investigate whether there is another way to protect the witness. However, again the possibilities of the court are limited when the secret services provide a plausible explanation. In this case, such as in the cases of withholding documents and witnesses, the executive can take influence on the selection of evidence by the courts.

18.4.2.3 Measures by the Court to Ensure Witness Protection in Order to Enable the Witness to Testify

A court can take various measures in order to protect a witness and therefore to enable the witness to testify in court (Ellbogen 2004: 190; Kühne 2007: 529; Soiné 2007). Several levels of protection are possible. On the first level, the court has to examine whether the witness can be protected in the courtroom during the public main hearing (*Hauptverhandlung*). If this is not possible, the court has to try to question the witness by a judge outside the main proceedings. As a last possibility, the court has to examine whether a written statement of the witness can be accepted as evidence or if the officer questioning the witness can be heard as a hearsay witness.

Protection During the Main Hearing

During the main hearing, some protection can be reached by not revealing the name and residence of the witness, by excluding the accused or the public or even by interviewing the witness in a different room by means of a video

conference.[42] But all these possibilities do not guarantee that the identity of a person is kept secret enough not to be recognized outside the courtroom again (Soiné 2007). It is not very likely that the secret services will accept such a low level of protection.

A higher level of protection is reached if the identity of the witness is kept secret and the outer appearance is changed for example by wearing a wig. The modern version of this camouflage is the visual and acoustical shielding of the witness. The Federal Court of Justice (BGH) allowed this possibility in 2003 (BGH NJW 2003, 74 see also BGH NStZ 2005, 43). In the case the witnesses were placed in a separate room and the testimony transmitted to the courtroom. A special lens made it impossible to recognize the face, a sound equalizer made it impossible to recognize the voice. These precautions enabled the court to hear the witnesses because otherwise the ministry would have withheld them. The advantage of this method is that the person can be seen and heard in action and can be directly questioned by the prosecution, the court, and the defence (Safferling 2006). This kind of protection seems to be suitable for all cases except those in which the mere statement of the witness would reveal their identity.

Questioning of the Witness Outside the Main Hearing

If the protection of the witness during the main hearing is not possible, the court has to try to question the witness outside the public proceedings and then introduce the written record of the questioning in the main hearing (*Kommissarische Vernehmung*, section 223 StPO). The court can only proceed in this way when it has a statement of the superior authority that in any other case the witness will be withheld (BGH NJW 1984, 65). The witness can be examined by a commissioned judge (a judge of the court conducting the main proceedings) or a requested judge (a judge of another court asked to do the questioning by judicial assistance). The examination is not public. If the witness will only give evidence in case neither the accused nor the defence is present, the court can refrain from notifying the defence and the accused (section 224 StPO). The Federal Court of Justice (BGH NJW 1980, 2088) as well as the Federal Constitutional Court (BVerfGE 57, 250) have also accepted

[42]The least protection during the main hearing offers the possibility not to reveal the place of residence (section 68 para. 2 StPO). More protection is given by not revealing the identity or just by giving an old or fake identity (section 68 para. 3 StPO). However, the person is still visible in the courtroom and could be identified later by the accused or an auditor. If there is a concrete threat to the health of a witness, the accused can be removed from the courtroom (section 247 StPO, see BGHSt 32, 32). However, in this case the accused gets to know the identity of the witness, so that it only makes sense when the witness is intimidated by the accused. A step further is the exclusion of the public, which requires a threat for life, liberty, or freedom of the witness (section 172 GVG). But in this case the accused also gets to know the identity of the witness. Similar problems arise when the witness is interviewed outside the courtroom by means of a video conference (sections 247a StPO) or that the video of an earlier questioning is shown (section 58a StPO).

that the defence can even be excluded from the questioning if otherwise the witness would be withheld by the authority.[43] On the one hand this enables the court to question the witness but on the other hand it restricts the influence of the defence, because they neither know who the witness is nor have the chance to ask questions. However, with the now-allowed possibility of a visual and acoustical shielding of a witness, a questioning outside the main hearing will happen less frequently (Safferling 2006).

Written Statements and Hearsay Witnesses

If the aforementioned measures do not guarantee enough secrecy for a person, the secret services will either withhold the witness by a declaration according to section 96 StPO or by a denial of the authorization to testify according to section 54 StPO. In such a case the court cannot get hold of the witness. However, the court has the possibility to introduce a statement of the witness indirectly (Ellbogen 2004: 216; Kühne 2007: 530). Section 251 StPO allows for an exception to the principle of examination in person of section 250 StPO. If a witness is prevented from appearing at the main hearing for an indefinite period, a written statement can replace the testimony. Withholding the witness for reasons of secrecy have been accepted as a constellation covered by section 251 StPO (BGHSt 29, 109; see also BVerfGE 57, 250). In such a case written statements of the witness can be read out in the main hearing. It is obvious that any further questioning of the witness is not possible that way. If a written statement of the witness is not available, the courts have also allowed introducing summaries of statements of the witness compiled by the secret services (see BGH NJW 2007, 384; OLG Hamburg, NJW 2005, 2326).

Another possibility is to question the person who has interrogated the witness. The interrogator is a witness, so that there is no direct conflict with section 250 StPO. However, the interrogator can only present hearsay about the crime. A hearsay witness is allowed as long as the original witness (the better piece of evidence) is not available (BVerfGE 57, 250; BGH NStZ 2000, 265; BGHSt 32, 115; see also Droste 2007: 597). Although the interrogator can be questioned personally, it is not possible to get to know many details of the original witness.

The possibility of introducing indirect evidence of a witness is only allowed by the courts if the refusal to let a person testify was not obviously illegal (BGHSt 29, 109). This can be the case when the publicity would not be detrimental to the welfare of the state or when the superior authority does not give any reasons, the reasons are not substantive enough, or the authority just gives an arbitrary reasoning. The Federal Court of Justice has not yet seen the preconditions fulfilled in a case. Only some lower courts have refused indirect evidence on these grounds

[43] In a later decision the BGH has ruled that if the defence nonetheless gets to know the date and place of the examination and shows up, they have the right to participate in the questioning (BGHSt 32, 115). However, not all details are clarified yet.

(see Eisenberg 2006: 301; Ellbogen 2004: 237). Although there are some examples, one has to say that the threshold is so high that the non-admission of indirect evidence will rarely happen as long as the secret services give some reasonable grounds for withholding a witness.

When indirect evidence is allowed, this does not mean that the evidence is of the same value as the oral statement of the witness would be (Ellbogen 2004: 256). The court has to be more critical than usual and analyze in detail the consistency of the indirect evidence. In addition, the indirect evidence can never be the basis for a conviction alone, especially if the court receives only summaries of statements of the witness compiled by the secret services. The indirect evidence has always to be backed by other direct evidence (BGH NStZ 2000, 265; see also BGHSt 49, 112). The evaluation of evidence by the court according to section 261 has to be described in detail in the judgment. It has to be pointed out that the court was aware and did pay special attention to the uncertainties of the indirect evidence. If there arise doubts about facts against or in favour of the accused, the court has strictly to apply the principle in favour of the accused (*in dubio pro reo*). This is in particular the case if withheld evidence could speak in favour of the accused. The Federal Court of Justice has explicitly made clear that the interest of the state to keep information secret may not lead to disadvantages for the rights of the accused (BGHSt 49, 112; see also BGH NStZ 2000, 265; BVerfGE 57, 250).

The German courts try to compensate for the reduced value of indirect evidence by an especially careful consideration of it. The reason behind this approach is that some evidence is better than no evidence at all (see BVerfGE 57, 250). However, in many cases the court will not really be able to evaluate the value of the evidence, because it lacks all the necessary information under which circumstances the evidence was collected, what the motivation of the witness has been and especially what omissions there are in the statements. This is equally true for the defence, which makes it almost impossible to question or counterbalance such evidence. Thus, the indirect evidence can only to support the reasoning the court has based on other evidence.

18.4.2.4 Dropping of Cases Because Evidence is Withheld

If important evidence is withheld by the secret services, the question arises of whether the court can drop a case because a fair trial is not possible. The Federal Court of Justice has decided that such a possibility exists (BGHSt 49, 112). In one case the accused (Mounir el Motassadeq) was indicted because of aiding one of the hijackers of September 9/11 (Mohamed Atta). One witness (Ramzi Binalshib) who might have clarified the involvement of the accused in the crime was imprisoned in the USA and not allowed to be questioned by the court. A FBI officer being interrogated in court was not allowed by the FBI to give evidence on statements made by Binalshib. Information the German secret services possessed on statements of Binalshib was withheld. The Federal Court of Justice ruled that withholding such important evidence violates the right of a fair trial of the accused. It declared that when the retention of the evidence has the consequence that the

judge has only a minimum basis of facts for deciding the case, the case must be dropped. However, in the case of el Motassadeq, the court saw other means that could compensate for the violation of the fair trial right. It ordered a rehearing of the case at first instance. Concerning the evidence, the first instance court was ordered to be especially careful in considering the evidence and strictly decide *in dubio pro reo*. In the rehearing, new evidence was provided by US authorities that allowed (together with other evidence) to prove an involvement of el Motassadeq in the attacks of September 9/11 (see BGH NJW 2007, 384).

18.4.3 Inadmissible Evidence

If evidence collected by the secret services is introduced into a criminal proceeding, this does not mean that the evidence is admissible for proving the guilt of the accused. For the question of whether a piece of evidence can be used as a basis for a criminal conviction, the German criminal procedure system differs between obstacles to obtaining evidence (*Beweiserhebungsverbote*) and obstacles to the admission of evidence (*Beweisverwertungsverbote*). As a general rule violations while collecting evidence can lead to a prohibition of the admission of evidence in court. However, the courts have allowed many exceptions to this rule and unfortunately have not succeeded in developing a coherent system for when evidence is admissible and when it is not (for the developments of recent years, see Fezer 2007; Jahn 2008: C39). In the context of the use of secret service information in criminal proceedings, two constellations are of special interest; first, the collection of evidence without the necessary legal basis; and second, the use of information collected abroad.

18.4.3.1 Illegally Collected Evidence

The collection of evidence by the secret services can be illegal for a number of reasons (Martin 1966). The secret services can lack the power to investigate certain crimes, such as the investigation of tax crimes in the aforementioned Liechtenstein case (see Schünemann 2008; Sieber 2008; Trüg and Habetha 2008). The services can also lack the power for certain coercive measures such as searching computers via the internet. In addition, the services can have disregarded the principle of proportionality and not refer to less far-reaching measures.

Violations do not necessarily ban the evidence from being admissible in court (see BVerfG NStZ 2006, 46; Jahn 2008: C32). The Federal Court of Justice tries to balance the public interest in prosecuting crimes and the interest of the individual not to be infringed in their rights. Main factors in judging the admissibility are the seriousness of the crime and the seriousness of the violation of rights by the secret services (see BGHSt 47, 172; BGH NJW 1997, 1018; Jahn 2008: C45). The more serious the violation by the services is, because they do not just

violate a formal regulation of the StPO but infringe important fundamental rights of the constitution, the more likely it is that the courts will disallow the evidence in the main hearing.

A special problem arises if the secret services gain evidence that was illegally collected by an individual. This can happen when the secret services ask individuals to work for them such as informants or confidants. In general courts allow evidence that was illegally collected by individuals (BGHSt 36, 172; Eisenberg 2006: 116; Gleß 2007: para. 10; Jahn 2008: C100). An exception can be made when the conduct of the individual is attributable to the secret services (Eisenberg 2006: 118; Jahn 2008: C101). Therefore the admissibility very much depends on the question of whether the individual acted on their own initiative or was instructed by the secret services. However, even when the conduct of the individual is attributed to the secret services, the courts tend to strike a balance between the interest in the prosecution and individual rights (BGHSt 40, 211); thus, allowing the rules of evidence and procedure to be "circumvented".

Very often the measures of the secret services do not produce the evidence later used in court, but only give hints for further investigations by the police or the prosecution. If the collection of evidence by the secret services was illegal, the question arises what happens with the later legally produced evidence by the police or prosecution. The German system does not have a "fruit of the poisonous tree doctrine" (Eisenberg 2006: 118; Jäger 2003: 111; Jahn 2008: C 91). Therefore the courts again balance the interest in the prosecution against individual rights. There are not many cases where evidence was not allowed in court. The most prominent example is that the court did not allow evidence that was collected by the prosecution on basis of an illegal collection of information by the secret services (BGHSt 29, 244). Because the secret services violated the important right of privacy of correspondence, posts, and telecommunications (art. 10 GG), the court regarded the violation as grave enough to ban later collected evidence. However, even in this case the ban was not total because the court allowed the use in cases of serious crimes.

Thus, illegally collected evidence by the secret services will not automatically be banned from the use in a criminal proceeding. This will only be the case when the secret services collect evidence in regard to minor crimes for which they are not responsible. If they collect information about serious crimes that are enumerated within their tasks, the evidence will probably be allowed in the proceeding. In short one can say that German jurisprudence puts much emphasis on allowing a public prosecution and less on the protection of individual rights.

18.4.3.2 Evidence Collected Abroad

In recent years the secret services receive more and more information from abroad. The secret services, the police, and the prosecution see no problem in using such information as a basis for further investigations in Germany. German authorities take this approach even when information might have been collected by illegal

means such as torture (see Hetzer 2006). This constellation rarely becomes public because in many cases just the outcomes of the additional investigations are used as evidence in court.

In more and more cases, the collection of evidence abroad itself is of importance when the commission of the crime takes place in a transnational setting. Examples are terrorist attacks where the planning and training of at least some members of a group take place outside the countries where the attack is committed. In these cases the question arises of whether evidence collected abroad can be used in court as well.[44] The main problem is in regard to the standards that should be applied in such a case in order to introduce the evidence into a German criminal proceeding. The courts have clarified that, for the collection of the evidence, the standards of the country in which the interrogation or the coercive measures take place are relevant (BGH NStZ 1994, 595; BGH NStZ 1992, 394; see also Böse 2002; Schuster 2006: 84). Hence German courts will examine in a case if the foreign standards have been observed while the evidence was collected (BGH NStZ 1992, 394; BGH NStZ 1983, 181).

However, the examination if the collection of evidence according to foreign standards was legal is only a precondition to the question of whether the evidence is admissible. The final question of admissibility is answered according to German law (BGH NStZ 1996, 609; Böse 2002). Therefore the illegal collection of evidence does not necessarily mean that the evidence is not allowed in court. This is only the case if the breach of foreign law is also relevant according to German standards. Vice versa, the legal collection abroad does not mean that the evidence is allowed, when German standards would not allow such a collection. This can be the case when German authorities initiated an interrogation abroad and the interrogation methods used are not allowed in Germany (Schuster 2006: 84).[45] Without the involvement of German authorities, evidence can be disallowed when the German standards of the rule of law (*rechtsstaatliche Anforderungen*) were not observed (BGH NStZ 1983, 181).

The question of whether the standards of the rule of law have been observed has been discussed in the already mentioned terrorist proceedings against Mounir el Motassadeq (see OLG Hamburg, NJW 2005, 2326). In this case the USA provided summaries of statements of several witnesses who where imprisoned by the USA. It was doubted whether the statements where obtained without the use of torture,

[44]The classic mechanisms to obtain the evidence are international judicial assistance or mutual cooperation (*internationale Rechtshilfe*). These aspects will not be examined any further in this context. The assistance can vary greatly, especially when EU countries are asked for help, because there already exists an extensive legal network for the exchange of information within the EU or parts of the EU.

[45]The involvement of German authorities abroad is obviously hard to prove. Information is often kept secret. If information becomes public it is mainly too general in order to be brought forward in a criminal proceeding. For example, it has become public that German secret service agents took part in interrogations in Guantanamo (see Hetzer 2006). However, as long as this participation cannot be connected to the interrogation of a specific person, the complaint that a statement was reached in circumvention of German law is unsuccessful.

because there had been press coverage concerning these witnesses. From the legal point, methods such as "waterboarding" may be legal according to US law but doubtless constitute torture according to German law. Section 136a StPO is quite clear in regard to such ill-treatment and completely bans any evidence based on the ill-treatment.[46] It is generally accepted that section 136a StPO contains standards that must be obeyed in any proceeding abroad (Gleß 2007: para. 11, 72; Schuster 2006: 219).

The problem in the case was that the court, the higher regional court of Hamburg (OLG Hamburg), did not have more than a vague suspicion that the witnesses had been tortured. Neither US authorities nor the German secret services provided any information about the circumstances under which the witnesses had been questioned. The court solved the problem by applying a high burden of proof. As long as it has not been proven that the witnesses had been tortured, it assumed that they were not and their statements were admissible in court (OLG Hamburg, NJW 2005, 2326). Hence it is not assumed *in dubio pro reo* that a witness has been tortured. This ruling is in accordance with a long-standing point of view of the Federal Court of Justice and was not overruled in the appellate proceeding (see BGH NJW 2007, 384). In fact this means that the defence has to prove that the witnesses had been tortured if their statements should not be used in court. This is a task almost impossible if the state authorities do not even state where the witnesses are held in custody. Thus, German jurisprudence again puts public prosecution first and the protection of individual rights second.

18.5 Conclusion

As has been shown, the secret services have the tasks and the power to collect evidence that can be introduced into criminal proceedings. The substantive powers of the secret services double the possibility of how a criminal proceeding can start. On the one hand, there is the normal criminal proceeding initiated by the police or the prosecution when a suspicion is given. On the other hand, a second form of proceedings exists (not even called a criminal one) that is conducted by the secret services when there are indicators for a serious crime or in the case of the strategic surveillance by the BND without any indicator at all. The main difference between the two is not only the level of suspicion that can trigger proceedings, but the almost complete secrecy of the investigative proceeding by the secret services (see Lisken and Denninger 2007: 118). This is quite astonishing in a system where the publicity of the criminal proceeding has been regarded a main achievement of the enlightenment. Although one has to admit that the publicity has never been realized in the

[46] Besides section 136a StPO, the court discussed the UN anti-torture treaty, to which Germany is a signatory and which is directly applicable in Germany (OLG Hamburg, NJW 2005, 2326). Any evidence based on torture is not allowed in a criminal proceeding (art. 15).

investigative stage because the police and prosecution also conduct their investigation out of the public eye, such complete secrecy is a novelty; especially because almost no possibilities exist to control or supervise these investigations.

The double possibility to start a proceeding causes many constitutional problems that can only be mentioned briefly. The rule of law requires that the legal system is clear in regard to the question of which authority is responsible for a certain case (BVerfGE 67, 299; BVerfGE 104, 249; Mehde 2005). It is not allowed to have two authorities dealing with the same questions. Doubling responsibilities diminishes legal certainty because it is never clear which authority actually has to act and citizens do not know which actions they can expect by whom. Thus, it is problematic that police and secret services are partly responsible for the same tasks, have overlapping powers, and in consequence double databases (for the data aspect see Ronellenfitsch 2007).

In normal criminal proceedings, the prosecution has the task to supervise the police when the police conduct the investigation. Because of the manpower of the police and their greater data resources in comparison with the prosecution, it has been regarded a problem for years that the prosecution is not able to supervise the police efficiently (Satzger 2004). In the case of investigations carried out by the secret services, the prosecution has no influence at all. This adds to the already diminished influence of the prosecution and leaves the prosecution in many cases with the only possibility being to accept the outcomes of investigations conducted by the police or the secret services. The vanishing influence of the prosecution can also be seen in everyday cooperation of police and secret services. Police and secret services extensively work together side by side, exchange information, and even share data banks. The prosecution does not participate in these different kinds of cooperation. It is not unlikely that the prosecution is informed at a very late stage of the investigation and therefore scarcely has the chance to conduct investigations of its own. In the end the prosecution has to take the evidence already collected.

Concerning the exchange of information, it has been clarified by the Federal Constitutional Court that no limitless exchange of information between the secret services and other authorities is allowed by the Constitution (BVerfGE 100, 313). This is an important restriction because the vast powers of the secret services to collect information substantially encroach upon fundamental rights. In consequence the services are allowed to collect personal details but are not allowed to share them in whole with other German authorities. The exception that is made by the Constitutional Court when a special public interest is given seems to be sensible at first glance. However, the vagueness of the term special public interest leaves much discretion to the legislator. In regard to crimes, probably only minor crimes committed in the private sphere are clearly excluded. It seems to be common sense that in the case of terrorism a far-reaching exchange of information is allowed (as it is in the case of organized crime). In absence of a definition of terrorism or organized crime, this is hard to contradict. However, one might for example question whether all bomb builders are terrorists because there are a great differences between a youngster who builds a bomb in order to take revenge for loosing his girlfriend and a religious fanatic who wants to attack the Western way of life by blowing up

a train. The vagueness of the term seems to be an invitation for regulations that are rather too broad than too narrow.

The law on the anti-terrorism file (ATDG) is an illustrative example. Carrying the term terrorism in its name, one would expect to find a precise definition of terrorism in the law. With the reference to section 129a StGB (formation of terrorist organizations), there is indeed a connection to terrorism. But the ATDG is applicable to many more cases, namely it applies to all persons who want to use violence as a mean for achieving goals of "international political or religious concerns"; yet such information may only be stored if it is of relevance for fighting "international terrorism concerning Germany". Defining the content of the anti-terrorism file with a reference to terrorism makes the ATDG not only applicable to a vast number of constellations but also opens the door for arbitrary decisions on a case-to-case basis whether certain conduct is a terrorist act or not. The secret services are left with much discretion in order to decide what information is stored in the anti-terrorism database and via the database available to the police.

When the secret services decide about giving information to the prosecution, they are not bound by the principle of mandatory prosecution and therefore they have much discretion on the question if at all, when and how much information shall be transmitted. At first hand this seems problematic because the executive has power to decide whether a criminal case reaches the prosecution and can therefore go its normal way to the courts. However, this power should not be overestimated because the secret services are legally required to transmit information about serious crimes. And if one really wants to take the principle of separation between secret services and police (and in consequence the prosecution) seriously, one has to accept that the secret services get to know crimes because they collect lots of information but must not necessarily inform the police/prosecution. This is a result of the distribution of powers among different institutions in order to guarantee a maximum of fundamental freedoms. There is not *the* one state, for which it is irrelevant which branch of the state knows something, because the knowledge of the person is automatically that of the state and can be shared among all other authorities. The real problem with the secret services deciding whether to transmit information about the commission of a crime or not is the lack of control and thus the wide discretion about who is punished and who is not. It is quite unusual that criminal proceedings can be brought to an end without any possibility of another institution to control this decision.

When it comes to criminal proceedings conducted by the prosecution and later continued in court, we have the situation that evidence collected by the secret services can be used that neither the police nor the prosecution would have been allowed to collect (see Lisken and Denninger 2007: 119). This is simply the case because only the secret services have these far-reaching powers to collect information and to transmit it to the prosecution. Formally the influence of the secret services ends with the transmission of the evidence. However, in practice it does not. It is true that the secret services (apart from their power not to transmit information) do not decide how a case is handled; they do not have any position of their own in criminal proceedings. The StPO does not even mention the secret services. However, we have

seen that the influence on the evidence is substantial because the secret services have the power to withhold evidence. This is not of great relevance when there is enough evidence deriving from other sources. However, in difficult cases, such as the terrorist proceedings against Mounir el Motassadeq, the prosecution and the court often must rely on the evidence collected and provided by the secret services.

The Federal Court of Justice tries to counterbalance the influence of the secret services by carefully evaluating the evidence. This is an understandable move in order to receive at least some evidence that is of course better than no evidence at all. The court even has opened the possibility of dropping a case. However, the threshold is set very high so that it is doubtful whether a case will be dropped at all in the near future. The option to drop cases should be elaborated more extensively by the courts because at this point the influence of the secret services touches a cornerstone of criminal proceedings: the freedom of the court to determine which evidence is needed to reach a decision (Safferling 2006). At this point it has to be made clear that if the secrecy of certain information is the prevailing interest of the state, it is not possible to conduct criminal proceedings according to criminal procedure standards at the same time. The solution cannot be lowering criminal procedure standards to a point where vague evidence constitutes the basis for a conviction. We have not completely reached this point, but the road seems to lead there.

The introduction of evidence collected by the secret services into criminal proceedings is a special burden for the defence. The defence has almost no possibility of questioning secret service measures when they take place. The situation for the defence remains difficult in court, when evidence is (partly) withheld. Obvious problems are to find out whether there is evidence withheld in favour of the accused or what the circumstances of the collection of evidence have been. The last point is especially problematic in view of the decision of the higher regional court of Hamburg (OLG Hamburg, NJW 2005, 2326), which left it to the defence to bring forward evidence in order to show that statements provided by the secret services were collected by means of torture. This impossible task may be an exception, but it shows clearly that the burden for questioning evidence provided by the secret services is so high that it can hardly be done successfully.

To sum up the foregoing considerations, one has to say that the secret services have a remarkable influence on criminal proceedings. This development creates many problems that have not been solved yet. If one does not want to retreat from the present situation and restrict the tasks and powers of the secret services, the solution can only be found in a strict adherence to criminal procedure and constitutional safeguards. It is up to the courts to guarantee these safeguards more vigorously by examining evidence of the secret services more intensively and especially by setting clear limits. The field of secret services and criminal proceedings clearly shows what happens if the legislator follows a broad and undefined concept such as the one of homeland security. It leads to a mixture of different approaches, causes confusion, and neglects the value of individual rights in order to guarantee a vague state of security.

References

Albert, Helmut (2000). Gedanken zum Verhältnis von Polizei und Verfassungsschutz. In Bundesamt für Verfassungsschutz (ed.), *Bundesamt für Verfassungsschutz. 50 Jahre im Dienst der inneren Sicherheit* (pp. 85–100). Köln: Carl Heymanns Verlag.

Baldus, Manfred (2002). Nachrichtendienste – Beobachtung völkerverständigungswidriger Bestrebungen. *Zeitschrift für Rechtspolitik*, 400–404.

Baumann, Karsten (2005). Vernetzte Terrorismusbekämpfung oder Trennungsgebot? – Möglichkeiten und Grenzen der Zusammenarbeit von Polizei und Nachrichtendiensten. *Deutsches Verwaltungsblatt*, 798–805.

Bäumler, Helmut (1991), Das neue Geheimdienstrecht des Bundes. *Neue Zeitschrift für Verwaltungsrecht*, 643–645.

Borgs-Maciejewski, Hermann & Ebert, Frank (1986). *Das Recht der Geheimdienste: Kommentar zum Bundesverfassungsschutzgesetz (Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes) sowie zum G 10 (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses – Gesetz zu Art. 10 Grundgesetz)*. Stuttgart: Boorberg.

Böse, Martin (2002). Die Verwertung im Ausland gewonnener Beweismittel im deutschen Strafrerfahren. *Zeitschrift für die gesamte Strafrechtswissenschaft*, 114, 148–182.

Bundesbeauftragte für Datenschutz und Informationsfreiheit (2007). *21. Tätigkeitsbericht 2005–2006*. Berlin (May 1, 2008); http://www.bfdi.bund.de.

Denninger, Erhard (2002). Freiheit durch Sicherheit? Anmerkungen zum Terrorismusbekämpfungsgesetz. *Strafverteidiger*, 96–102.

Dorn, Alexander (2004). *Das Trennungsgebot in verfassungshistorischer Perspektive – Zur Aufnahme der inlandsnachrichtendienstlicher Bundeskompetenzen in das Grundgesetz vom 23. Mai 1949*. Berlin: Duncker & Humblot.

Droste, Bernadette (2007). *Handbuch des Verfassungsschutzrechts*. 5th edition. Stuttgart: Richard Boorberg Verlag.

Eisenberg, Ulrich (2006). *Beweisrecht der StPO. Spezialkommentar*. München: Verlag C. H. Beck.

Ellbogen, Klaus (2004). *Die verdeckte Ermittlungstätigkeit der Strafverfolgungsbehörden durch die Zusammenarbeit mit V-Personen und Informanten*. Berlin: Duncker & Humblodt.

Fezer, Gerhard (2007). Die Rechtsprechung des BGH zum Strafverfahrensrecht seit 1995. *Juristenzeitung*, 665–676, 723–729.

Gleß, Sabine (2007). § 136a. In Löwe-Rosenberg (ed.), *Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar* (pp. 580–631). 26th edition, Volume 4. Berlin: De Gruyter Recht.

Golembiewski, Claudia (2000). *Mitteilungen durch die Justiz. Verfassungsrechtliche Grundlagen und rechtsdogmatische Strukturen des Justizmitteilungsgesetzes*. Baden-Baden: Nomos-Verlagsgesellschaft.

Götz, Volkmar (2006). Innere Sicherheit. In Josef, Isensee & Paul, Kirchof (eds.), *Handbuch des Staatsrechts der Bundesrepublik Deutschland*, *Band IV Aufgaben des Staates* (pp. 671–699). 3rd edition, Heidelberg: C.F. Müller Verlag.

Gröpl, Christoph (1993). *Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung. Legitimation, Organisation und Abgrenzungsfragen*. Berlin: Duncker und Humblot.

Gusy, Christoph (1991). Befugnisse des Verfassungsschutzes zur Informationserhebung. *Deutsches Verwaltungsblatt*, 1288–1295.

Gusy, Christoph (2006). *Polizeirecht*. 6th edition, Tübingen: Mohr Siebeck.

Gusy, Christoph (2008). Parlamentarische Kontrolle der Nachrichtendienste im demokratischen Rechtsstaat. *Zeitschrift für Rechtspolitik*, 36–40.

Hassemer, Winfried (1993). Innere Sicherheit im Rechtsstaat. *Strafverteidiger*, 664–670.

Hassemer, Winfried (2006). Sicherheit durch Strafrecht. Eröffnungsvortrag Strafverteidigertag 24.3.2006, Frankfurt/M., Paulskirche. *Strafverteidiger*, 321–332.

Hetzer, Wolfgang (1999). Polizei und Geheimdienste zwischen Strafverfolgung und Staatsschutz. *Zeitschrift für Rechtspolitik*, 19–24.

Hetzer, Wolfgang (2006). Verschleppung und Folter – Staatsraison oder Regierungskriminalität? *Kriminalistik*, 148–159.

Hirsch, Alexander (1996). *Die Kontrolle der Nachrichtendienste. Vergleichende Bestandsaufnahme, Praxis und Reform*. Berlin: Duncker und Humblot.

Hoffmann-Riem, Wolfgang (2002). Freiheit und Sicherheit im Angesicht terroristischer Anschläge. *Zeitschrift für Rechtspolititk*, 497–501.

Huber, Bertold (2000). Post aus Pullach – Das G 10-Urteil des BVerfG vom 14.7.1999. *Neue Zeitschirft für Verwaltungsrecht*, 393–396.

Huber, Bertold (2007). Das Bankgeheimnis der Nachrichtendienste – Zur Neuregelung des Auskunftsersuchen der Nachrichtendienste durch das Terrorismusbekämpfungsergänzungsgesetz vom 9.1.2007. *Neue Juristische Wochenschrift*, 881–883.

Jäger, Christian (2003). *Beweisverwertung und Beweisverwertungsverbote im Strafprozess*. München: Verlag C. H. Beck.

Jahn, Matthias (2008). Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, Gutachten C für den 67. Juristentag. In Ständige Deputation des Deutschen Juristentags (ed.), *Verhandlungen des Siebenundsechzigsten Deutschen Juristentages* (pp. C1–C128). München: Verlag C. H. Beck.

Juy-Birmann, Rodolphe, revised by Biermann, Jörg (2006). The German system. In Mireille, Delmas-Marty & John, Spencer (eds.), *European Criminal Procedure* (pp. 292–347). Cambridge: Cambridge University Press.

Kerner, Hans-Jürgen, Stierle, Claudia & Tiedtke, Ingo (2006). Kriminalitätsbekämpfung durch Behörden des Bundes. Ein Überblick über nationale, europäische und internationale Elemente. *Kriminalistik*, 292–304.

Köhler, Michael (1994). Unbegrenzte Ermittlung und justizfreie Bundesgeheimpolizei: Der neue Strafprozess. *Strafverteidiger*, 386–389.

König, Marco (2005). *Trennung und Zusammenarbeit von Polizei und Nachrichtendiensten*. Stuttgart: Boorberg.

Kugelmannn, Dieter (2006). *Polizei- und Ordnungsrecht*. Berlin Heidelberg New York: Springer.

Kühne, Hans-Heiner (2007). *Strafprozessrecht*. 7th edition, Heidelberg: C. F. Müller Verlag.

Kutscha, Martin (2008). Mehr Schutz von Computerdaten durch ein neues Grundrecht? *Neue Juristische Wochenschrift*, 1042–1044.

Lisken, Hans (1994). Vorfeldeingriffe im Bereich der "Organisierten Kriminaliltät" – Gemeinsame Aufgabe von Verfassungsschutz und Polizei? *Zeitschrift für Rechtspolitik*, 264–270.

Lisken, Hans & Denninger, Erhard (eds) (2007). *Handbuch des Polizeirechts*. 4th edition, München: Verlag C.H. Beck.

Martin, Ludwig (1966). Die Rolle der Ämter für Verfassungsschutz bei der Strafverfolgung. In Bundesministerium des Innern (ed.), *Verfassungsschutz – Beiträge aus Wissenschaft und Praxis* (pp. 81–92). Köln: Carl Heymanns Verlag KG.

Mehde, Veith (2005). Terrorismusbekämpfung durch Organisationsrecht. *Juristenzeitung*, 815–822.

Meyer-Goßner, Lutz (2007). *Strafprozessordnung. Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen*. 50th edition, München: Verlag C.H. Beck.

Middel, Stefan (2007). *Innere Sicherheit und präventive Terrorismusbekämpfung*. Baden-Baden: Nomos Verlagsgesellschaft.

Nehm, Kay (2004). Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur. *Neue Juristische Wochenschrift*, 3289–3295.

Paeffgen, Hans-Ullrich (2002)."Vernachrichtendienstlichung" von Strafprozess- (und Polizei-) recht im Jahr 2001. Weitere grundsätzliche Anmerkungen zur deutschen "Sicherheitsrechts"-Entwicklung bis zum Terrorismusbekämpfungs-Gesetz. *Strafverteidiger*, 336–341.

Paeffgen, Hans-Ullrich (2003). Vernachrichtendienstlichung des Strafprozesses, *Goltdammer's Archiv*, 647–671.

Pieroth, Bodo, Schlink, Bernhard & Kniesel, Michael (2005). *Polizei- und Ordnungsrecht mit Versammlungsrecht*. 3th edition, München: Verlag C.H. Beck.

Pünder, Hermann (2006). Verwaltungsverfahren. In Erichsen, Hans-Uwe & Ehlers, Dirk, *Allgemeines Verwaltungsrecht* (pp. 365–518). 13th edition, Berlin: de Gruyter.

Rieger, Thomas (1986). *Der Bundesnachrichtendienst im demokratischen Rechtsstaat*. Ellwangen/Jagst: Roswitha Wimmer Verlag.

Ringwald, Gerhard (1988), Gegenpol zu INPOL? Computer bei der Justiz, *Zeitschrift für Rechtspolitik*, 178–183.

Roewer, Helmut (1987). *Nachrichtendienstrecht der Bundesrepublik Deutschland*. Köln: Carl Heymanns Verlag.

Roggan, Fredrik & Bergemann, Nils (2007). Die "neue Sicherheitsarchitektur" der Bundesrepublik Deutschland – Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsgesetz, *Neue Juristische Wochenschrift*, 876–881.

Roggan, Fredrik & Kutscha, Martin (eds) (2006). *Handbuch zum Recht der Inneren Sicherheit*. 2nd edition, Berlin: Duncker & Humblodt.

Ronellenfitsch, Michael (2007). Datenschutzrechtliche Schranken bei der Terrorismusbekämpfung. *Datenschutz und Datensicherheit*, 31, 561–570.

Rose-Stahl, Monika (2006). *Recht der Nachrichtendienste*. 2nd edition, Brühl/Rheinland: Fachhochschule des Bundes für öffentliche Verwaltung.

Ruhmannseder, Felix (2007). Informationelle Zusammenarbeit von Polizeibehörden und Nachrichtendiensten auf Grund des "Gemeinsame-Dateien-Gesetzes". *Strafverteidiger-Forum*, 184–190.

Safferling, Christoph J. M. (2006). Verdeckte Ermittler im Strafverfahren – deutsche und europäische Rechtsprechung im Konflikt? *Neue Zeitschrift für Strafrecht*, 75–82.

Satzger, Helmut (2004). Chancen und Risiken einer Reform des strafrechtlichen Ermittlungsverfahrens, Gutachten C für den 65. Juristentag. In Ständige Deputation des Deutschen Juristentags (ed.). *Verhandlungen des Fünfundsechzigsten Deutschen Juristentages* (pp. C1–C148). München: Verlag C. H. Beck.

Schafranek, Frank Peter (2000). *Die Kompetenzverteilung zwischen Polizei- und Verfassungsschutzbehörden in der Bundesrepublik Deutschland*. Aachen: Shaker Verlag.

Schenke, Wolf-Rüdiger (2005). *Polizei- und Ordnungsrecht*. 4th edition, Heidelberg: Müller.

Schily, Otto (2006). Die Bildung von Allianzen gegen Kriminalität und Gewalt als nationale und internationale sicherheitspolitische Herausforderung. In Bundeskriminalamt (ed.), *Neue Allianzen gegen Kriminalität und Gewalt, BKA Herbsttagung 2005* (pp. 7–16). München: Luchterhand.

Schlink, Bernhard (1982). *Die Amtshilfe, Ein Beitrag zu einer Lehre von der Gewaltenteilung in der Verwaltung*. Berlin: Duncker und Humblot.

Schoch, Friedrich (2005). Polizei- und Ordnungsrecht. In Schmidt-Aßmann, Eberhard (ed.), *Besonderes Verwaltungsrecht* (pp. 121–275). 13th edition, Berlin: de Gruyter.

Schreiber, Wolfgang (1996). Polizeiliche Zusammenarbeit zwischen Bund und Ländern – Ausdruck kooperativen Föderalismus. In Kniesel, Michael, Kube, Edwin & Murck, Manfred (eds.), *Handbuch für Führungskräfte der Polizei – Wissenschaft und Praxis* (pp. 137–168). Lübeck: Schmidt-Römhild.

Schünemann, Bernd (2008). Die Liechtensteiner Steueraffäre als Menetekl des Rechtsstaats. *Neue Zeitschrift für Strafrecht*, 305–310.

Schuster, Frank Peter (2006). *Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess*. Berlin: Duncker & Humblodt.

Sieber, Ulrich (2007). Grenzen des Strafrechts. *Zeitschrift für die gesamte Strafrechtswissenschaft*, 119, 1–8.

Sieber, Ulrich (2008). Ermittlungen in Sachen Liechtenstein – Fragen und erste Antworten. *Neue Juristische Wochenschrift*, 881–886.

Singer, Jens Peter (2002). *Die rechtlichen Vorgaben für die Beobachtung der Organisierten Kriminalität durch die Nachrichtendienste der Bundesrepublik Deutschland*. Aachen: Shaker Verlag.

Soiné, Michael (2007). Erkenntnisverwertung von Informanten und V-Personen der Nachrichtendienste in Strafverfahren. *Neue Zeitschrift für Strafrecht*, 247–253.

Staff, Ilse (1999). Sicherheitsrisiko durch Gesetz, Anmerkung zum Urteil des Bundesverfassungsgerichts zum G-10 Gesetz. *Kritische Justiz*, 32, 586–593

Trüg, Gerson & Habetha, Jörg (2008). Die "Liechtensteiner Steueraffäre" – Strafverfolgung durch Begehung von Straftaten? *Neue Juristische Wochenschrift*, 887–890.
Wolff, Heinrich Amadeus, Scheffczyk, Fabian (2008). Verfassungsrechtliche Fragen der gemeinsamen Antiterrordatei von Polizei und Nachrichtendiensten. *Juristische Arbeitsblätter*, 81–88.
Wolter, Jürgen (1999). 35 Jahre Verahrensrechtskultur und Strafprozessverfassungsrecht in Ansehung von Freiheitsentziehung, (DNA-) Identifizierung und Überwachung. Hans Joachim Hirsch zum 70. Geburtstag. *Goltdammer's Archiv*, 158–181.
Würtenberger, Thomas, Heckmann, Dirk (2005). *Polizeirecht in Baden-Württemberg*. 6th edition, Heidelberg: Müller.
Zöller, Mark Alexander (2002). *Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten. Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz*. Heidelberg: Müller.
Zöller, Mark Alexander (2007). Der Rechtsrahmen der Nachrichtendienste bei der "Bekämpfung" des internationalen Terrorismus. Juristenzeitung, 763–771.

Appendixes

18.6 Decisions

In the following, judicial decisions mentioned in the text are listed chronologically supplemented by date and case number. The citations are based primarily on the official collections (BVerfGE, BGHSt, BVerwGE) or on the reprint of the decisions in legal publications (NJW, NStZ, StV). Many of the decisions are also available online.

Decisions of the German Federal Constitutional Court since 1998 are available online without charge (https://www.bundesverfassungsgericht.de/entscheidungen.html). The judgements can be found on the basis of the date and the case number (Table 18.1).

Decisions of the Federal Court of Justice are available online from 2000 onwards without charge (http://www.bundesgerichtshof.de). The judgements can be found on the basis of the date and the case number (Table 18.2).

Decisions of the federal administrative court are available online from 2002 onwards only. Older decisions can be ordered via the website of the court for a small fee (http://www.bundesverwaltungsgericht.de/). The judgement mentioned in the text can be found on the basis of the date and the case number (Table 18.3).

Decisions of the higher regional court of Hamburg (OLG Hamburg) are available online from 2004 onwards without charge (http://lrha.juris.de/cgi-bin/laender_rechtsprechung/ha_frameset.py). The judgement mentioned in the text can be found on the basis of the date and the case number (Table 18.4).

Table 18.1 Decisions of the BVerfG

Citation in the text	Date	Case number
BVerfGE 47, 46	21 December 1977	- 1 BvL 1/75 – (et al.)
BVerfGE 57, 250	26 May 1981	- 2 BvR 215/81 -
BVerfGE 65, 1	15 December 1983	- 1 BvR 209/83 – (et al.)
BVerfGE 67, 299	09 October 1984	- 2 BvL 10/82 -
BVerfGE 97, 217	28 January 1998	- 2 BvF 3/92 -
BVerfGE 100, 313	14 July 1999	- 1 BvR 2226/94 – (et al.)
BVerfGE 104, 249	19 February 2002	- 2 BvG 2/00 -
BVerfGE 103, 21	14 December 2000	- 2 BvR 1741/99 – (et al.)
BVerfGE 110, 33	3 March 2004	- 1 BvF 3/92 -
BVerfG NStZ 2006, 46	30 June 2005	- 2 BvR 1502/04 -
BVerfGE 113, 348	27 July 2005	- 1 BvR 668/04 -
BVerfGE 118, 168	13 June 2007	- 1 BvR 1550/03 – (et al.)
BVerfG, NJW 2008, 822	27 February 2008	- 1 BvR 370/07 – (et al.)
BVerfG, NJW 2008, 1505	11 March 2008	- 1 BvR 2074/05 – (et al.)

Table 18.2 Decisions of the BGH

Citation in the text	Date	Case number
BGHSt 29, 109	10 October 1979	- 3 StR 281/79(S) -
BGHSt 29, 244	18 April 1980	- 2 StR 731/79 -
BGH NJW 1980, 2088	28 May 1980	- 3 StR 155/80 (L) -
BGH NStZ 1983, 181	11 November 1982	- 1 StR 489/81 -
BGHSt 32, 32	1 July 1983	- 1 StR 138/83 -
BGH NJW 1984, 65	12 July 1983	- 1 StR 174/83 -
BGHSt 32, 115	17 October 1983	- GSSt 1/83 -
BGH StV 1989, 284	21 March 1989	- 5 StR 57/89 -
BGH NStZ 1992, 394	4 April 1992	- 3 StR 460/91 -
BGHSt 36, 167	12 April 1989	- 3 StR 453/88 -
BGHSt 38, 237	18 March 1992	- 1 BGs 90/92 – (et al.)
BGHSt 40, 211	21 July 1994	- 1 StR 83/94 -
BGH NStZ 1994, 595	10 August 1994	- 3 StrR 53/94 -
BGH NStZ 1996, 609	24 July 1996	- 3 StR 609/95 -
BGH NJW 1997, 1018	15 January 1997	- StB 27/96 – (et al.)
BGHSt 44, 107	24 June 1998	- 5 AR (VS) 1/98 -
BGH NStZ 2000, 265	11 February 2000	- 3 StR 377/99 -
BGH NStZ 2001, 333	16 January 2001	- 1 StR 523/00 -
BGHSt 47, 172	22 November 2001	- 1 StR 220/01 -
BGH NJW 2003, 74	26 September 2002	- 1 StR 111/02 -
BGHSt 49, 112	4 April 2004	- 3 StR 218/03 -
BGH NStZ 2005, 43	17 August 2005	- 1 StR 315/04 -
BGH NJW 2007, 384	16 November 2006	- 3 StR 139/06 -
BGHSt 51, 211	31 January 2007	- StB 18/06 -

Table 18.3 Decision of the BVerwG

Citation in the text	Date	Case number
BVerwGE 75, 1	19 August 1986	- 1 C 7/85 -

Table 18.4 Decision of the OLG Hamburg

Citation in the text	Date	Case number
OLG Hamburg, NJW 2005, 2326	14 June 2005	- 2 BJs 85/01 – (et al.)

Index