



acatech DISKUTIERT

# > EUROPEAN PERSPECTIVES ON SECURITY RESEARCH

KLAUS THOMA (Ed.)



Springer



acatech

GERMAN ACADEMY OF  
SCIENCE AND ENGINEERING

**> EUROPEAN PERSPECTIVES ON  
SECURITY RESEARCH**

**KLAUS THOMA (ED.)**

Prof. Dr. Klaus Thoma  
Fraunhofer-Institut für Kurzezeitdynamik,  
Ernst-Mach-Institut, EMI  
79104 Freiburg

acatech – Deutsche Akademie der Technikwissenschaften, 2011

Head office  
Munich residence  
Hofgartenstraße 2  
80539 Munich, Germany

capital city office  
Unter den Linden 14  
10117 Berlin, Germany

T +49(0)89/5203090  
F +49(0)89/5203099

T +49(0)30/206309610  
F +49(0)30/206309611

E-Mail: [info@acatech.de](mailto:info@acatech.de)  
Internet: [www.acatech.de](http://www.acatech.de)

ISSN 1861-9924/ISBN 978-3-642-18218-1/e-ISBN 978-3-642-18219-8

DOI 10.1007/978-3-642-18219-8

Bibliographic information of the German National Library  
The German National Library lists this publication in the German National Bibliography;  
detailed bibliographic data is available on the Internet under <http://dnb.d-nb.de>.

© Springer-Verlag Berlin Heidelberg 2011

This publication is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, recitation, reuse of figures and tables, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provision of the German Copyright Law of 9th September, 1965, in its current version. It is always subject to a fee. Violations are liable for prosecution under German Copyright Law. The use of registered names, trademarks, etc., in this publication does not imply, even in the absence of specific statement, that such names are exempt from relevant protective laws and regulations and therefore free for general use.

Editor: Guido Zimmer  
Coordination: Dr. Anna Frey  
Layout design: acatech  
Conversion and typesetting: Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS,  
Sankt Augustin, Germany  
Einbandgestaltung: WMX Design GmbH, Heidelberg

Printed on acid-free paper

[springer.com](http://springer.com)

**> EUROPEAN PERSPECTIVES ON  
SECURITY RESEARCH**

**KLAUS THOMA (ED.)**

# CONTENTS

> <b>Foreword</b>	7
Eckehard Schnieder/Petra Winzer	
> <b>Introduction</b>	9
Klaus Thoma/Daniel Hiller	
> <b>A European perspective on security research</b>	13
Khoen Liem/Daniel Hiller/Christoph Castex	
> <b>A German perspective on security research</b>	27
Klaus Thoma/Daniel Hiller/Tobias Leismann/Birgit Drees	
> <b>UK perspectives on security in an age of 'shock and aftershock'</b>	45
Tobias Feakin	
> <b>Defence and security research Coexistence, Coherence, and Convergence</b>	55
Christian Breant/Ulrich Karock	
> <b>An overview of Swiss research on vulnerability of critical infrastructure</b>	67
Wolfgang Kröger	
> <b>Security Research and Safety Aspects in Slovakia</b>	81
Juraj Sinay	
> <b>Engineering infrastructures: Problems of safety and security in the Russian Federation</b>	91
Nikolay A. Makhutov/Dmitry O. Reznikov/Vitaly P. Petrov	
> <b>Conclusion</b>	105
Klaus Thoma/Daniel Hiller/Tobias Leismann/Birgit Drees	
<b>Index of Authors</b>	111

## > FOREWORD

ECKEHARD SCHNIEDER/PETRA WINZER

Safety and security are core values of human society and essential aspects in the evolution of nature. In Maslow's hierarchy the need for safety and security follows right after basic physiological needs.

The acatech topical network *safety and security* has set out to foster order and provide orientation in the general perception of safety and security through interdisciplinary approaches and working groups.

Aside from questions about the terminology pervading manifold professional languages, approaches to form generic principles and concepts based on system-theoretical fundamentals, acquisition of competence through professional training and academic education, organisational and technological instruments to guarantee safety and security (in particular innovative sensor, information and communication technologies) all offer promising opportunities for solutions.

Identifying and articulating concrete needs for safety and security, and addressing them with suitable approaches and measures is not easy. After all, safety and security are always linked to actual circumstances and unique situations in complex environments full of socio-economic and technical peculiarities and challenges – scenarios that individuals, communities and even entire nations all face alike.

Looking at what safety and security mean worldwide, it is clear that any international discussion of the topic will be lively and enlightening, not least due to the different cultural traditions and backgrounds with regard to safety. It thus comes as no surprise that safety and security conform to different systems of concepts in all these different cultures.

Following an initial look at safety and security research on a national level, with an analysis and publication by the topical network on chances and perspectives, the focus now turns to a European view of the topic. Professor Klaus Thoma has coordinated the discussions that lead to the publication of this second volume of contributions to security research in the acatech topical network *safety and security*.

## > INTRODUCTION

KLAUS THOMA/DANIEL HILLER

Security research as a practical discipline has a long-standing history. Faced with myriad hazards throughout its past, mankind has developed sophisticated means to counter such threats. The latter include natural disasters such as earthquakes, floods and fires, but also encompass man-made hazards such as military aggression, terrorist attacks or threats resulting from the malicious application of technological developments. Since the end of the Cold War major armed conflicts between nations of the Western hemisphere have become highly unlikely and genuinely different security issues have become the focus of concern. The terrorist attacks of 2001 against the United States, the train bombings of Madrid in 2004 and the bombings of London in 2005 were horrific embodiments of a new security environment that has evolved on a global scale. One could list numerous other examples of both executed attacks and successfully deterred attempts from around the world. Our modern industrial societies are interlinked with infrastructure networks, providing citizens with mobility, energy and information flows, which also open the door to a whole new dimension of vulnerabilities. Security research, once anything but a practical discipline with a capacity for reacting to short-term demands, has in the span of only a few years evolved into an entirely new scientific discipline uniting various fields of research. Today, security research (in Europe) encompasses a broad community of natural/engineering and social sciences.

Europe's networked societies of today are shaped by a growing interconnection in almost all areas of life and thus share a common vulnerability to such new security threats. The complexity of our infrastructures and the concurrent accessibility to means of destruction by terrorist groups and individual perpetrators call for innovative security solutions, be they human or technological in nature. However, such evolving innovations inevitably raise fundamental questions of concern in our societies. How do we balance the imperatives of securing our citizens and infrastructures on the one hand, and of protecting of our sacredly held civil liberties on the other? In effect, it is the 'cost' – both economic and societal – of security measures that politicians, researchers and citizens need to contemplate.

Within the EU – an alliance of 27 different nations with unique cultural backgrounds, legal practices and historical experiences – there is both disparity and common ground with regard to the way security issues are perceived and handled. Consequently, designing and conducting security research will entail the consideration of different aspects, depending on whether looking at France, Norway or Great Britain, for example. Over the past few years many European countries have launched national security research programmes to build up national capabilities to better protect their societies against modern security threats. At the same time, there has been action on a European level, namely by the European Commission, including work on the topic of security in the seventh European Framework Programme (FP7)<sup>1</sup>, now one of 10 topics funded within the 'specific programme' on cooperation. Over the course of six years, the Commission will fund security related projects worth € 1.4 bn. between 2007 and 2013. Looking further ahead, the security topic has already been approved as part of the next Framework Programme (FP8), which will run from 2014 through 2020. Also, in the fall of 2009, the European Research and Innovation Forum (ESRIF)<sup>2</sup> published its recommendations, outlining the agenda of a future security research programme.

As many of the national security research programmes have moved beyond their initial phases, there has been an aspiration to bring together experts from across Europe to present their national security research efforts. To this end, the topical network 'Safety and Security' of acatech – the German Academy of Science and Engineering – invited experts from the science academies of various European countries to contribute their expertise to this collection of perspectives. Coming from Germany, France, the Netherlands, Great Britain, Norway, Switzerland, Slovakia and Russia, security researchers, representatives of the German Ministry of Education and Research, the European Commission and the European Defence Agency (EDA) shared their perspectives on security research and the aspect of safety with a group of German experts during a two-day workshop hosted by the Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut on 4th and 5th March, 2010. Workshop participants included members of research organizations, universities and the private sector. The result is an overview of various security research programmes in Europe with the aim of revealing both common ground and major differences in security/risk perceptions, cultures and political practices within Europe. This publication is a compilation of contributions made during the workshop.

---

<sup>1</sup> Preliminary action had already been taken by the so-called Group of Personalities (GoP) in 2003, followed by the Preparatory Action on Security Research (PASR) in 2004. Before FP7 was launched in 2007, the European Security Research Advisory Board (ESRAB) has published its final report in 2006, its final recommendations marking the structural design of the European security research programme.

<sup>2</sup> Very similar to ESARB, ESRIF is an advisory body including security experts of the research community, the private sector and governmental organizations.



As the title of this publication already indicates, the perspectives united herein encompass several aspects of security research. The overall attempt of the authors with regard to addressed topics is threefold:

- First, security/risk perceptions within the individual countries will be examined. This aspect also includes possible delineations that are made between the field of security and safety.
- Second, the national security research programmes of each nation will be presented. Furthermore, the institutional framework will be highlighted, identifying the relevant (public, private, corporate) actors involved in the design of the programmes.
- Third, links will be outlined between national security research efforts and the European FP7. That may include a country's participation in European security research projects as well as alignments of national programmes with FP7 topics.

acatech and Fraunhofer EMI pay tribute to all participating members of the Workshop.

# > A EUROPEAN PERSPECTIVE ON SECURITY RESEARCH

KHOEN LIEM/DANIEL HILLER/CHRISTOPH CASTEX

## 1 INTRODUCTION

Tackling the complexity and interdependence of today's security environment in the globalized world of the 21st century is an everlasting challenge. Whereas the end of the Cold War presented a caesura of global dimension for the political and economic architecture and a realignment of power distribution and international relations between former adversaries, September 11th of 2001 may be seen as another caesura. Since then, specifically among countries of the Western hemisphere, traditional security paradigms and theories have been critically questioned and the different security cultures and perceptions have resulted in diverse security and defence policies as well as in security research efforts of individual countries. Consensus, it seems, exists on the question of what the threats are that our modern interconnected societies are facing. Whether looking at international terrorism, organized crime, climate change, the illegal trafficking of goods and people or naturally caused catastrophes, these phenomena all have in common that they are in most cases of transnational nature. Formerly existing dividing lines between internal and external security continue to fade, presenting an enormous challenge for those in charge of designing security policy and even more so for the various institutions safeguarding European security. That is why dissent often revolves around the question on how to get hold of these complex problems. Geographic location, cultural background, ethical make-up of society as well as relations with neighbouring countries are all important aspects to be considered when assessing the security culture and policy of individual countries.

The European Union as it exists today, an alliance of 27 different nations, has never been so strongly consolidated, so economically prosperous and secure. Yet, at the same time, as a Union it has also never been so vulnerable, facing enormous security challenges that are often a result of our globalized and intensely networked societies. Regardless of the origination of a security problem, be it a possible terrorist attack or illegal human trafficking, the EU with its open borders and markets can only successfully conduct security policy and in turn, security research, if acting as strong alliance. Consequently, security and defence policies as well as the respective research agendas must be aligned and especially Europe's external relations must be clearly defined. The Lisbon Treaty represents an important framework towards a more coordinated and

unified organization of the EU's external relations and its security policies overall. For instance, with Baroness Catherine Ashton from the UK, the EU now has a High Representative of the Union for Foreign Affairs and Security Policy, who is supposed to unite Europe's complex security policies and initiatives in one political post. At the same time Ms. Ashton is a Vice President of the European Commission; this is an opportunity unknown before, to align the EU's Security Policy with the extensive means available to the EU. Overall, the EU has taken decisive action to make clear that the field of security and defence is of paramount importance for the Union, asserting itself as a respected key player in global politics.

Aside from this rather strategic policy direction of the EU, the European Commission has taken the initiative to launch the first genuine European security research programme within its 7th Framework Programme (FP 7). With a funding of about € 1.4 bn. for the time period between 2007 and 2013, the Commission supports collaborative projects requiring the co-operation between partners from various different countries to develop innovative technological security solutions as well as concepts related to the complex societal aspects of security. And even beyond that, the so-called European Security Research and Innovation Forum (ESRIF)<sup>1</sup> has published its final report in December 2009, outlining a strategic European Security Research and Innovation Agenda (ESRIA) for the next twenty years. The following article will trace the emergence of this programme as well as elaborate on lessons learned so far. Finally, it aims at shedding light at some special characteristics of European security research thinking.

## 2 THE GENESIS OF EUROPEAN SECURITY RESEARCH

Understanding the path to the first European security research programme, one must bear in mind the specific challenges the EU is facing with regard to its overall security. Especially the enlargement of the Union, now encompassing 27 nations and over 500 million people, presented unprecedented endeavours for all involved security actors. External borders of the Union alone consist of 6.000 km of land borders and 85.000 km of coast lines. Strongly increasing trade trafficking with global markets makes border control a difficult mission. In addition, Europeans are faced with a growing dependence on interconnected infrastructures in areas such as transport, energy, information and communication, resulting in an increased vulnerability of our societies. Concurrently, our networked channels of communication lead to an availability of know-how in the field of technological applications to those intending to use them maliciously.

Again, the threats European nations are facing today are multifaceted, complex, interrelated and as mentioned before, increasingly transnational in their impact. Consequently, no single European country can master the challenges posed by such an

---

<sup>1</sup> See: [www.esrif.eu](http://www.esrif.eu)

environment on its own. Acknowledging these circumstances, in 2004 the European Commission took action in order to bring together owners, operators, industry and research organizations as well as governments to coordinate and structure joint efforts to better protect persons and critical infrastructures against this multiplicity of threats.

### > 2.1 A first approach: ESRAB

Recognizing the different facets that the field of security entails, the Commission soon concluded that the traditionally independent and sector-specific treatment of the topic security would no longer satisfy to tackle the full spectrum of challenges. Therefore, a rather coordinated and holistic approach was needed in order to develop genuinely European security capabilities. In 2003, the so-called Group of Personalities (GoP)<sup>2</sup> was set up. It was comprised of high-level industrialists, Members of the European Parliament as well as representatives of international organizations and research institutes. Its mission was to outline a long-term perspective in the field of security research, gathered in a final report presented to the Commission in 2004. Therein, it was recommended to form the European Security Advisory Board (ESRAB)<sup>3</sup>, an extended yet more 'operational' version of the GoP, which was established in the year of 2005. As a 50-person-strong board, covering the full spectrum of security relevant stakeholders, ESRAB brought together the demand articulators and the research and technology suppliers in one body. Its mission not only included the outlining of a strategic concept for an implementation of the theme security in the Commission's 7th Framework Programme, it was also asked to provide clear implementation rules as well as a communication strategy to promote the awareness of European security research. The board's final report »Meeting the Challenge: the European Security Research Agenda« was published in September of 2006.<sup>4</sup> Aside from clearly defining technological capabilities to be developed, the report presented a first broad picture of the economic, societal, organizational and legal challenges that had to be met when intending to cover the full spectrum of civil security related issues. In parallel to the activities of ESRAB, a so-called Preparatory Action on the Enhancement of the European Industrial Potential in the field of Security Research (PASR) was initiated by the Commission.<sup>5</sup> Between 2004 and 2006 an overall budget of € 45 mill was dedicated to support a total of 23 collaborative projects. During this first project period, the major areas of funded proposal sectors included the field of access control, border control, transport, ICT and surveillance systems. Topics covered more reluctantly included the field of critical infrastructure protection as well as CBRNE protection.

---

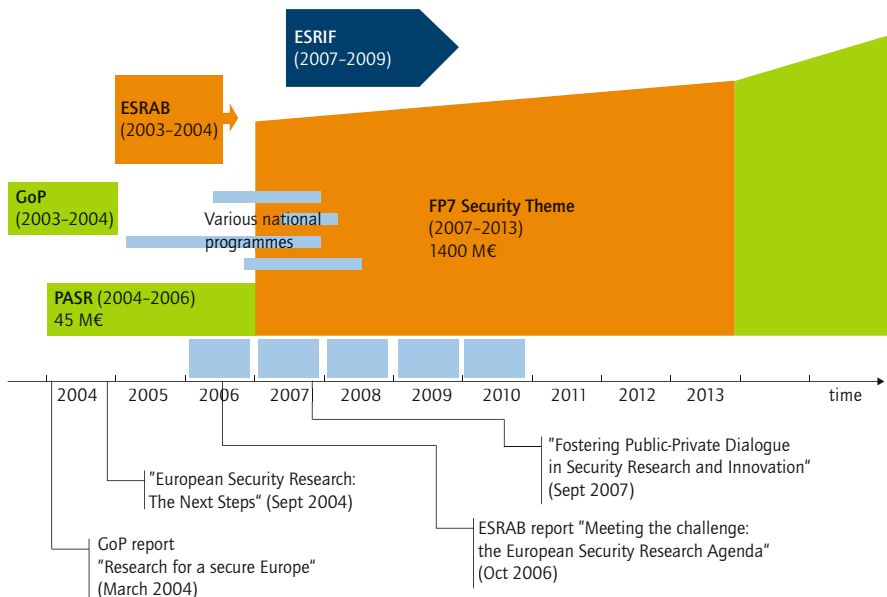
<sup>2</sup> See: [http://ec.europa.eu/enterprise/policies/security/files/doc/gop\\_en.pdf](http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf)

<sup>3</sup> See: [http://ec.europa.eu/enterprise/policies/security/files/esrab\\_report\\_en.pdf](http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf)

<sup>4</sup> Ibid.

<sup>5</sup> See: [http://cordis.europa.eu/fp7/security/pasr-project-leaflets\\_en.html](http://cordis.europa.eu/fp7/security/pasr-project-leaflets_en.html)

Figure 1: Timeline of the evolution of European Security Research



## > 2.2 A capability-based approach for European security research

As a prerequisite to structuring a security research agenda and defining capabilities, ESRAB recognized the importance of clearly defining the frame of its work, therefore it provided a first overall definition of security research. As the report states, ESRAB's work was defined being:

*'...research activities that aim at identifying, preventing, deterring, preparing, and protecting against unlawful or intentional malicious acts harming European societies, human beings, organizations or structures, material and immaterial goods and infrastructures, including mitigation and operational continuity after such an attack (also applicable after natural/industrial disasters).'*

Building on the recommendations of the GoP, the ESRAB-report's premise is a capability-based approach. Acknowledging the wide spectrum of threats European societies are facing, a capability-based approach was chosen to address these threats, moving from the definition of threats to missions and capabilities, which in turn, finally lead to technologies. Accordingly, the document defines four mission areas as well as three areas of cross-cutting interest. The missions are:

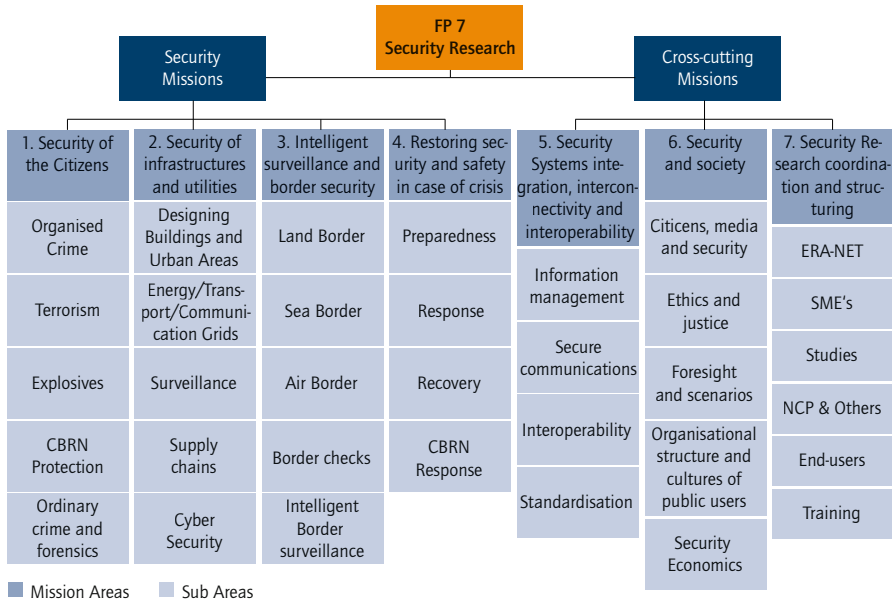
1. Security of citizens
2. Security of infrastructures and utilities
3. Intelligent surveillance and border security
4. Restoring security and safety in case of crisis

The cross-cutting areas include:

1. Security systems integration, interconnectivity and interoperability
2. Security and society
3. Security research coordination and structuring

Each mission as well as cross-cutting area includes additional sub-areas, depicted in the table below:

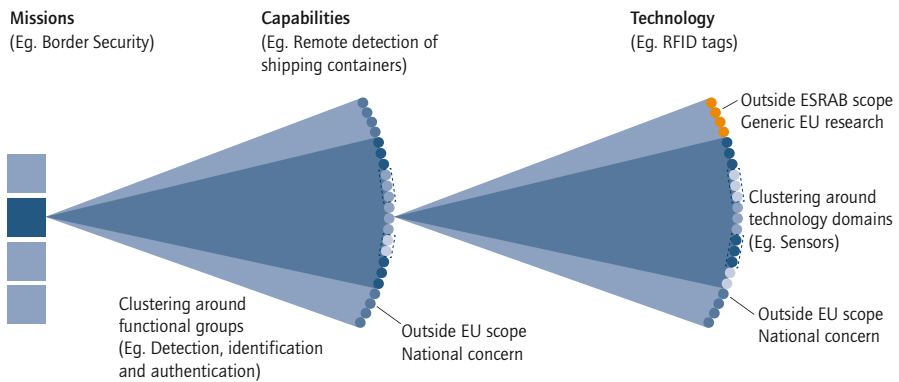
Figure 2: Overview of missions and cross-cutting areas



As previously indicated, capabilities constitute the principal building block for the derivation of technologies. The capabilities themselves were closely linked to the four mission areas. In order to cover the full spectrum of decisive capabilities, ESRAB conducted

an in-depth analysis supported by a large number of end user organizations as well as by research and technology providers. For the conceptualization of the technical research necessary to accomplish the goals defined by the mission areas, ESIRAB has grouped all research efforts in three distinct paths, varying in the maturity level of technologies to be developed, integrated and demonstrated.

Figure 3: A capability based approach



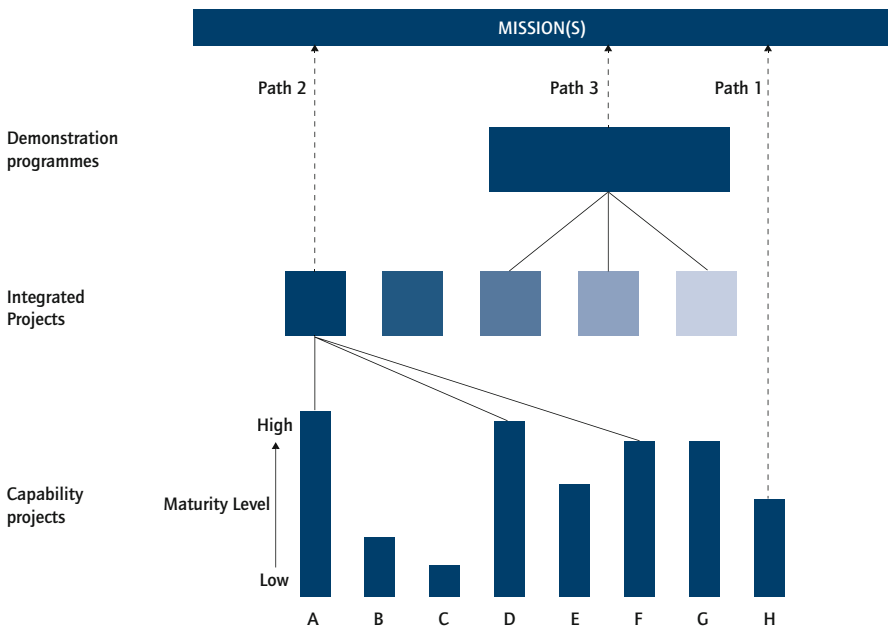
*Capability development* – this first research path, potentially covering multi-mission or mission-specific capabilities, aims at the improvement of the maturity level of an existing technological capability, or even the development of totally new and emerging technologies. These capability projects are designed to have an overall volume of up to € 3.5 mill. in a time period of approx. 2 to 4 years and require the participation of partners of at least three different European countries. Another criteria often required is the involvement of several different entities considered to be critical, i.e. industry, research organizations as well as end-users.

*System development* – in a mission specific approach, the so-called Integrated Projects intend to integrate a number of already accomplished capabilities/technologies in innovative combinations in order to deliver significant operational performance advances. Financially, these Integrated Projects range between € 3.5 mill and € 14 mill.. Throughout the complete period of FP 7 (2007-2013), a total of 20 Integrated Projects are supposed to be funded.

*System of systems demonstration* – the largest project format is presented by so-called Demonstration Projects. With an overall budget ranging between € 30-40 mill, these multi-mission approaches are designed to integrate a number of different sys-

tems into one project, where demonstrating the system-of-systems makes up the majority of the work. As not all previously developed capabilities require treatment on a fully European level – also bearing in mind the limited budget available – the selection of capabilities integrated into such demonstration projects are based on the premise of European added value, meaning they must prove having a European dimension in terms of specific results impossible to be achieved if dealt with only at the national level. As these Demonstration Projects have duration of over 5 years, they are split into two phases. The first preparatory phase, resulting in a strategic roadmap for the realization of the entire demonstration concept, is followed by the main phase, which could last up to four years alone. In total, the Commission intends to launch five of these Demonstration Projects.

Figure 4: Research paths defined by ESRAB



Since the introduction of the theme security within FP 7, the Commission has announced four so-called ‘work programmes’ on an annual basis. Each one of these work programmes contains a list of topics within the four missions and the three cross-cutting areas for which consortia including various partners among European countries can sub-



mit project proposals. The first call for proposals at the end of 2006 resulted in 57 projects worth € 156 mill. The consecutive calls for proposals have seen a strong increase in allocated financial resources, a path that is intended to be continued until the last call at the end of 2012. As far as Demonstration Projects are concerned, the first phases in the field of Mass Transportation (within the mission 'protection of infrastructures and utilities') as well as in border security have been approached in the first call period of the programme. The year 2009 has brought the initiation of first phase Demonstration Projects in the field of supply chain management, CBRNE protection as well in the field of aftermath crisis management.

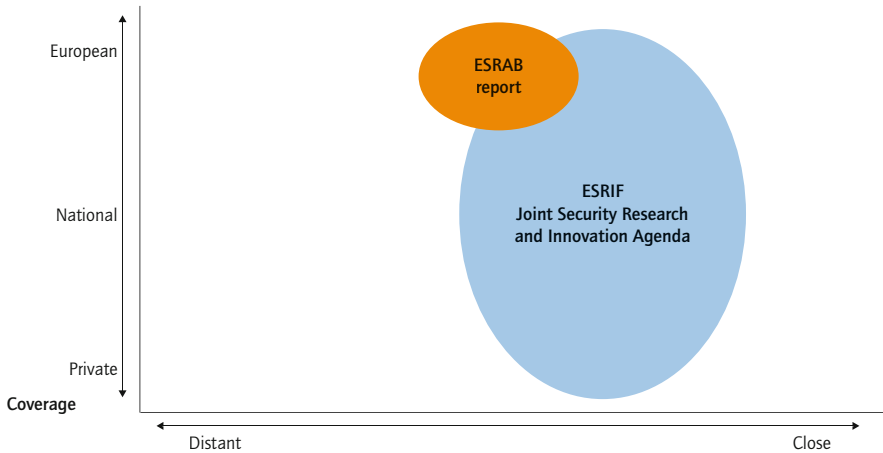
### 3 THE FUTURE CIVIL SECURITY AGENDA – ESRIF AND ESRIA

The final ESRAB report with all its recommendations roadmaps presents an essential milestone for the foundation of security research on a European level. Nevertheless, there remained a consensus among the key players of the community that in order to guarantee a fruitful and effective continuation of security research in Europe, an additional strategic framework needed to be developed. Evident shortcomings included the need for a better coordination of the strategy and implementation of European and national security research programmes. Also, experts acknowledged the necessity of providing a mid and longer term perspective for civil security research in Europe that would go far beyond pure research as defined in ESRAB and put a stronger focus on innovation elements. In addition, the juxtaposition of security policy and its implementation on the one side as well as security research on the other was supposed to result in an improvement of coordination between the two. Consequently, the coordination between the demand and supply side of security technologies/solutions also had to be improved whilst a much stronger involvement of civil society, including a more general consideration of societal aspects within security research. At last, as it is the case in many national security research programmes of EU member states, the delineations as well as commonalities between civil security and military research had to be clearly defined.

To overcome these shortcomings and to reinforce the foundation of European security research, security stakeholders in Europe felt that it is beneficial to set-up another forum commissioned to develop such a long-term perspective and strategic roadmap. In 2007, during the second European Conference on Security Research (SRC'07) in Berlin, then representing the EU Presidency, the German Minister for Education and Research, Ms. Anette Schavan, announced that the European Security Research and Innovation Forum (ESRIF) is founded. The forum's inaugurating meeting took place in September of '07; its first chairman was elected to be Mr. Gijs de Vries, the former EU's counter terrorism co-ordinator. Similar to ESARB, ESRIF members united the majority of security community, including research organizations, industry as well as governmental institutions to unite their expertise in order to accomplish the defined mission. When looking at the

working process of ESRIF and its results, one will observe the close link to the ESRAB report and must concurrently acknowledge the obvious consolidation and enhancement of the concepts and topics developed by ESRAB. The following visualization clearly shows the breadth and scope of ESRIF's work, reaching far beyond the ESRAB report.

Figure 5: A depiction of the scope of ESRIF



After 11 meetings in plenary, the group has published its final report in December of 2009.<sup>6</sup>

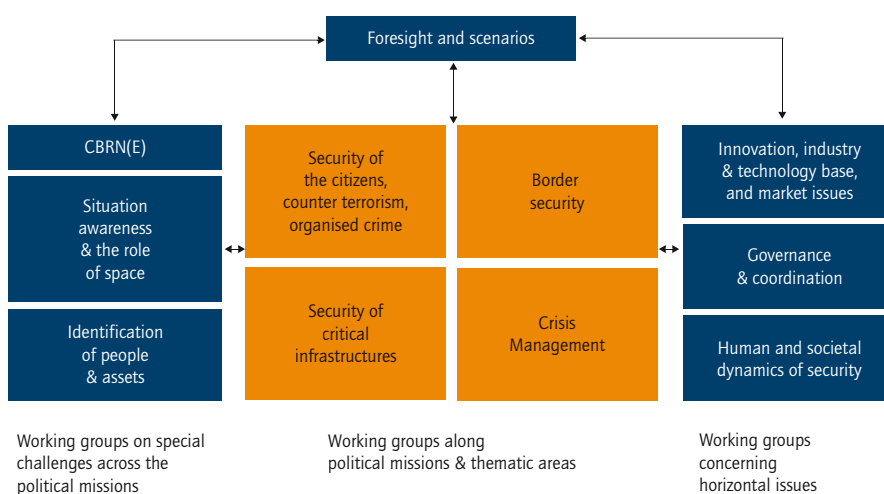
The so-called European Security Research Innovation Agenda (ESRIA) addresses the aforementioned aspects and provides a comprehensive strategic roadmap for the design and implementation of future European security research until the year 2030. But before elaborating on the core results of ESRIA, it is of importance to take a look at the working process of ESRIF. Although much more comprehensive in scope and detail, the organization of ESRIF in working groups aligned to the political missions on the macro level indicates that this is a continuation of a process whose basic foundation was established by ESRAB.

ESRIF's working methodology centred on four major aspects. First, it aimed at identifying the mid- and long-term threats and challenges to European security, taking into account existing policies and strategies as well as building on foresight and scenario techniques, linking predictions and expectations about future developments with the focal areas of the ESRIF working groups. Second, it intended to identify capabilities to enhance security according to the political missions and thematic areas as well as

<sup>6</sup> ESRIF 2009

provide a supporting framework in order to achieve these capabilities. Such a framework includes societal, economic and governance related aspects. Third, as a logical consequence, research requirements needed to be derived from the identification of capabilities, including a prioritization thereof. Self-explanatorily, this prioritization would have to be made along criteria such as effectiveness, acceptability, cost, maturity of technologies, innovation and replacement cycles for large scale systems. Fourth and last, ESRIF was tasked to provide a stringent communication strategy for the results of its work.

Figure 6: ESRIF working groups



There are nine key messages developed throughout the ESRIF process, which are:

1. Societal security – human values ought to present the core of all security related research
2. Societal resilience – Europeans must be prepared for shocks and develop the capacity to recover and adopt
3. Trust – nurturing confidence among European societies in security measures/ technologies
4. Interoperability – establish seamless systems
5. A systematic approach to capability development
6. Industrial policy – develop guidelines to establish a level playing field as well as open market incentives

7. Innovation – establish benchmarks for an effective innovation management
8. Security by design – ensuring that security is an integral part of any system from the outset
9. Awareness raising through education and training

As indicated before, one central task of ESRI is to develop a strategic roadmap geared towards guaranteeing innovation within security research over the next twenty years. The results of this process were aligned in the so-called European Security Research and Innovation Agenda (ESRIA). As a roadmap, it has been integrated into ESRI's final report, broken down in five distinct clusters as well as detailed guidelines to be followed throughout the implementation process of the ESRIA.

ESRIA is organized in the following five clusters:

1. Security cycle preventing, protecting, preparing, responding and recovering
2. Countering different means of attack
3. Securing critical assets
4. Securing identity, access and movement of people and goods
5. Cross-cutting enablers

For all clusters (= missions) functions and capabilities as well as systematic research needs are defined in detail. Furthermore, these research needs are categorized by their technological readiness. Finally, ESRIA provides a roadmap of research needs (2009-2030) for numerous sub-sections of the five clusters.

#### 4 RESUME AND OUTLOOK

Far beyond anchoring the theme security in its overall Framework Programme structure, the European Union and its member states have hitherto accomplished to establish a solid foundation within security research among European actors, involving experts from across the public and the private sector, ranging from small SMEs to infrastructure operators to research organizations and large enterprises.

Such an endeavour is challenging and demanding. In spite of Europe's continues integration in almost all areas of public and corporate sectors, all matters related to security and defence have traditionally been handled at the national levels and in many respects, they still are. Therefore, the first challenge was to persuade member states to cooperate in a field being of such vital importance to the very national interest of individual member states.

A central aspect of our today's global security environment certainly made it easier to overcome such hesitance of a possible 'European-added value' of joint approaches in the field of security research across European borders. The fact that former delineations

between internal and external security continue to fade has lead policy makers as well as researchers, end-users and product developers to support a true European approach to tackle some of the pressing challenges to our security, such as global terrorism, transnationally organized crime or human trafficking. All of these phenomena are indicators of a fundamental shift in our security environment when compared to the 'pre-9/11 era'. In the past, security was mostly thought in territorial terms, those in charge of protecting a nation and its citizens used to have a fairly clear understanding of what there had to be protected and what the specific threats were they were facing. But as Flynn already notes in 2004, terrorist groups, for instance,

*"themselves operate in networks that prey on other networks – the interconnected arteries and nodes of vulnerability that accompany the free flow of people, ideas, goods and services, and the complex interdependent systems on which free societies depend (Flynn 2004: 86).*

Consequently, a promising approach to face this challenge is the concept of 'resilience'. As policy-makers and researches acknowledge the impossibility to protect neither all citizens nor the critical nodes of our infrastructures completely against the multiplicity of threats we are facing, resilience seems a sound a realistic approach as a guiding principle within the field of security research. We cannot fully avoid the occurrence of terrorist attacks nor of natural disasters, but we can make sure our societies and infrastructures are able to absorb and recover from disturbances and to retain essentially the same function, structure and identity after having experienced a shocking event – and in the end, learn and adapt. That is why resilience has been chosen as a central element of ESRIF and ESRIA respectively and its importance will continue to rise in the near future.

As a Union of 27 member states, tackling the pressing security challenges of our networked and globalized societies is a tremendous challenge that can only be mastered through a genuine European approach. That is why the European Commission has decided to include security in its FP 7 for the first time in 2007. As outlined above, a comprehensive approach was chosen to process and align the needs and requirements with regard to common security concerns of all member states. Through the establishment of ESRAB, it was ensured that all relevant actors would be involved in this process. The outcome of this process, including the initial ESRAB report as well as the recently published ESRIF report may truly be concerned a comprehensive and holistic approach to design and implement security research initiatives on a transnational level unprecedented in European history and certainly unique on a global scale.

As FP7 is at about half-time of its overall period (2007-2013) it is time for a first review and assessment of activities launched so far. Throughout the first four calls that have been published by the Commission, a total of € 527 mill. € funding have been de-

voted to a total number of 130 collaborative research projects. At least the first phases of demonstration projects have been launched in all mission areas and although being at such an early stage, one may well consider the outcome of the funded projects so far a true success. Never before in the field of security research has such a vast effort been made, bringing together the expertise and experience of numerous actors of public and private sectors across Europe.

Today, civil security research within the European Union may be considered a field with a well established foundation. Even more than that, ESRIA is already outlining strategic guidelines for the forthcoming twenty years of European security research. Nonetheless, the content and volume of the Commission's Framework Programmes of the future will always be the result of a complex political process, its outcome often represents a compromise of 27 different concerns and priority settings. Quite logically that also implies that future funding of security research may not necessarily be expected to rise linear.

Currently, the Commission is already dedicated to outline the content and volume of FP8. A contentious issue that is heatedly discussed is the question on whether to include defence research as an individual topic in general or not. Obviously, as national budgets for defence research continue to shrink, some representatives strongly favour an engagement of the European Union, similar to the one in the field of civil security research. Numerous questions remain open in this respect and continue to feed debates among policy makers. Nevertheless one may argue for the benefits that EU-funded research and development can create to better support the EU's CFDP missions. In FP8 one may also expect the strengthening of efforts to develop technologies and procedures to support our civil protection forces (the 'blue-light' forces or the 'heroes' as some calls them). The debate has also started as how to improve implementation mechanisms relevant to areas of FP8 that are inherently 'non-free-market' orientated - Security research is one of these.

A concrete result, and, one may certainly note, success of the first civil security research programme on a European level is the emergence of very broad and versatile networks of experts, joining their efforts and expertise within the field to achieve a tangible 'European-added value' so that in the end, visions and ideas transform from being mere ideas into manifest reality. This publication is one visible example of such promising efforts.

## 5 REFERENCES

### ESRAB 2006

European Security Research Advisory Board (ESRAB): Meeting the Challenge: The European Security Research Agenda. Office of the Publications of the European Communities, Luxembourg: 2006

### **Flynn 2004**

Flynn, Stephen: "America the Vulnerable: How our government is failing to protect us from terrorism." New York: Harper Collins, 2004

### **Internet Sources**

#### **ESRIF 2010**

European Security Research Innovation Forum. Online available at: <http://www.esrif.eu>

# > A GERMAN PERSPECTIVE ON SECURITY RESEARCH

KLAUS THOMA/DANIEL HILLER/TOBIAS LEISMANN/BIRGIT DREES

## 1 INTRODUCTION

Prior to 2007, there was no coherent federal approach to conceptualise and fund security research in Germany. This changed with the initiation of the national program for civil security research, managed by the German Ministry for Education and Research (BMBF). Over the course of only four years a continuous build-up of national capacities on civil security was established to better protect German citizens, commodities and infrastructures against terrorism, organised crime and the effects of man-made and natural disasters.

Research and technology organisations, universities, and many public and private actors such as fire fighting organisations, the police, technology providers or airport operators have since been developing innovative concepts and technologies that cover a wide spectrum of scenarios related to the security of citizens and infrastructures. There has been a rise in the number of interest groups and advisory bodies looking to influence the policy-making process in the field.

One aim of this chapter is to depict the political and institutional structures among the actors in the German security research community. Following an outline of the basic structure of the national civil security programme, links to security research on the European level, namely within the European Commission's Framework Programme 7 (FP7), will be described. The final section of this chapter is devoted to an alternative security approach that has been drawing increased attention in security research communities of late. In contrast to traditional security paradigms and frameworks, the concept of a resilient society offers promising ideas on new ways to address today's complex security environment. Theoretical approaches will be highlighted before an outlook summarises the major challenges that lie ahead.

## 2 THE GERMAN PROGRAMME ON CIVIL SECURITY

The first civil security research programme in German history marks a caesura: It is the first genuine interagency approach by a German government to manage and fund security research as a unique discipline on a federal level. Prior to the programme, German actors in the security sector (researchers, public authorities, infrastructure owners and operators, etc.) had no common framework at their disposal to jointly and systemati-



cally develop technological solutions or societal concepts for successfully detecting and deterring pending threats. Even the fundamental premise of such a framework, a common agreement on the categorisation and prioritisation of threats, was lacking. Consequently, this national programme on civil security is a resolute approach to overcome the fragmented structure of the German security sector and its diverse perceptions and practices.

In its so-called 'High-Tech Strategy' – a national effort to support the development of innovative technologies for a sustainable future – the German federal government has identified security research as one of the top five research priorities of the future<sup>1</sup>. Between 2007 and 2010<sup>2</sup> funding of 123 million euro was allocated to foster security research and, indirectly, industrial competitiveness. To date, a wide range of topics has been addressed in various collaborative projects throughout the country. A number of projects even span national borders, as the programme also aims at funding bi-national research efforts, specifically between Germany and France, Israel and the United States. The first programme period will end in 2010, but the relevant actors are currently discussing possible adjustments for a continuation of the programme.

### > 2.1 Institutional organisation – A cross-departmental approach

In Western democracies, providing the key public good of security is first and foremost a fundamental imperative of the political leadership. The public justifiably expects any administration to institutionally gear the country's security apparatus to thwarting both existing and emerging threats. When catastrophic events occur, all involved federal institutions must work collaboratively and without turf battles to ensure that recovery and restoration efforts are implemented as quickly and effectively as possible. Equally important, however, is collaboration between the public and the private sectors since the latter owns and operates a large share of the interconnected infrastructures, ranging from local water supply reservoirs and public transportation networks to transnational oil pipelines.

Accordingly, and in light of the complexity of today's security environment, the German government has embedded its security research programme in the national High-Tech Strategy, which, in effect, involves almost all federal departments and specifically endorses the involvement of the private sector wherever necessary. The security research topic is thus institutionally organised using a genuinely cross-departmental approach with the BMBF holding the reins of overall management. The BMBF has installed a sub-unit in the Key Technologies – Research for Innovation directorate, which is responsible for the security topic. Research, legislation, regulatory support, international cooperation and procurement in the area of civil security are strategically managed by one lead-agency with the aim of forming an integrated unit. The organisation and realisation

---

<sup>1</sup> BMBF 2006.

<sup>2</sup> BMBF 2007.

of the different programme announcements, as well as the subsequent monitoring of approved projects is jointly managed with the Association of German Engineers (VDI), a major player in the field of large project organisation in Germany and an ideal broker between the public and the private sectors.

In addition to the human resources at the BMBF, a programme committee, the Scientific Programme Board Security Research (WPA), comprising experts from academia, research organisations, federal government departments, industry and operators of infrastructures, accompanies the security research programme. The WPA's overall mission is to advise the federal government in matters concerning security research. Furthermore, it also guarantees oversight on the overall orientation of security research based on the central missions outlined in the research programme. Finally, the Board ensures that German civil security activities dovetail with European efforts. Chaired by Klaus Thoma from the Fraunhofer Ernst-Mach-Institut EMI, the Board convenes on a bi-annual basis. So far, it has proved to be an important body, helping to streamline German efforts in security research by ensuring a continuous dialogue between all relevant disciplines. While consultations currently focus on the continuation of the national programme, the WPA recently published a position paper that defines the guiding principles of the next civil security research programme<sup>3</sup>.

## > 2.2 Strategic objectives

When outlining strategic objectives of a research agenda, the fundamental premises need to be clearly defined. The framework of these premises is shaped by our modern way of life, which has direct repercussions on our security environment. First, there is a strong trend of increasing population concentrations in large urban areas. This leads to tremendous backlashes on security aspects since urban areas are more vulnerable to a multiplicity of threats, expressed in the number of casualties when crisis situations arise. Second, modern societies are characterised by a growing interconnection of manifold aspects of life. Thus, our highly sophisticated networked infrastructures (communication and information, energy supply, transportation infrastructure, etc.) have become the critical nodes of society. Their incapacitation could potentially lead to a collapse of vital supply infrastructures with unforeseeable consequences. Third, the global information and service evolution is continuously transforming modern societies, generating hitherto unknown potential for economic growth and expansion, but at the same time opening the door to new types of vulnerabilities from similarly evolving threats.

---

<sup>3</sup> BMBF 2010a.

Keeping this in mind, the civil security research programme clearly defines the objectives of all research efforts to coincide with the guiding principles of German security policy:

- Protecting the population
- Reducing the country's vulnerabilities
- Developing solutions to minimise the effects of natural catastrophes or major incidents on society
- Combating terrorism and organised crime

In addition to these strategic objectives, the programme lists specific guidelines that attempt to do justice to the complex challenges that policy-makers, researchers, end-users and industry face. Concentrated effort will be required to:

- Reinforce interdepartmental co-operation
- Gear to end users and markets
- Create links between technology and social issues
- Pursue European cooperation, as well as international research alliances in the field

### > 2.3 Two programme lines

To accomplish the strategic objectives listed above, the framework of the programme is organised in two supporting programme lines, 'scenario-oriented security research' and 'technology networks'.

'Scenario-oriented security research' emphasises technology solutions for complex security scenarios that aim at incorporating end user perspectives. These end users include service providers (as in many Western countries, in Germany a large number of critical infrastructures are owned and operated by the private sector) and public security actors such as the police or fire brigades. In this way collaboration between both security solution providers and end users is ensured and results in jointly developed security solutions that bring together the requirements and solutions perspectives. Moreover, this scenario-oriented approach aims at uniting technology, science, humanities and social science disciplines and gearing them to common goals. Ultimately, it will guarantee that the research community, instead of focusing on isolated research topics, focuses sharply on real system innovations based on threats, while taking into account cost-benefit analyses<sup>4</sup>.

The second programme line, 'technology networks', encompasses security technologies that are required in almost all of the previously described scenarios. Approaching the multiplicity of challenges on the application level, it aims at involving the entire innovation chain, including the research community, the industry as well as the end

---

<sup>4</sup> BMBF 2007.

users. Aside from transferring basic technological know-how from existing and new technologies into the development of innovative technology systems, societal research is consistently endorsed. It particularly addresses questions of possible ethical and legal consequences that the application of innovative security technologies might implicate. Also, light needs to be shed on the societal significance of possible advancements of existing and newly developed technologies. The overall goal of all such efforts is to assess the societal impact of technology innovations, specifically focusing on questions regarding the societal acceptance of and/or opposition against the introduction of certain technologies<sup>5</sup>.

As emphasised by the responsible BMBF, in both programme lines high priority will be given to supplementary research efforts on questions such as data protection or the impact of applying technological developments on human rights and civil liberties. The ministry intends to raise these security-related issues in the research community by initiating workshops, discourses and publications to ultimately support research-policy decision-making.

#### > 2.4 Funded topics

Each of the programme lines described above contains a list of prioritised topics – the result of a comprehensive agenda-process incorporating the perspectives of more than 250 security experts from science, business and the public sector.

The four major topics in 'scenario-oriented security research' are:

1. Rescue and protection of people
2. Protection of transport infrastructures
3. Protection against failure of supply infrastructures
4. Securing supply chains

A definition of the essential challenges within every scenario is followed by a comprehensive list of relevant research topics.

The prioritised missions of the 'technology networks' programme line are:

1. Protection systems for security and emergency services
2. Detection of hazardous substances
3. Pattern Recognition
4. Biometrics

Funding for all of these topics is granted on a competitive basis. The topics are announced publicly, specifying the criteria project partners need to fulfil in order to participate. Given the fact that security research as an entirely new discipline is still at such

---

<sup>5</sup> BMBF 2007.

an early stage of development, a wide array of projects within the different programme lines has already been launched. Altogether, 66 collaborative projects have been initiated since 2007. These comprise more than 377 individual projects, with 103 of these performed in SMEs (as of May 2010). In addition to a total funding of 173 million euro by the BMBF, the industry invests more than 50 million euro in these R&D efforts.

Aside from these programme lines, the BMBF has also set up additional funding opportunities to foster international cooperation with a selected group of partnering countries, namely the United States, France and Israel. Furthermore, in 2008 a public announcement was made on the societal dimensions of security research, with three projects already approved and nine additional ones in preparation. The BMBF specifically promotes the involvement of SME's in security research projects and has launched a public announcement in 2010 to support the participation of SME's through a specific funding scheme.

### > 2.5 A Growing number of players within the security research community

The emergence of security research as a new discipline has also lead to a growing expert community encompassing research alliances, independent think tanks, advisory groups and industry interest groups. Apparently, the economic potential of security technologies results in substantial assets and jobs. As indicators show, the market potential for security technologies is continuously growing. So far, reliable estimates on the overall volume of a clearly defined security market in Germany are lacking; figures of estimates deviate strongly. Generally speaking, the state is the most important market driver. It opens up new market opportunities, which in the end increase the competitiveness of the German economy. But aside from economic interests articulated to the BMBF by special interest groups, other non-profit organisations and alliances have initiated security research networks so that the political agenda process can be realigned with innovative input from various disciplines relevant to security. One important framework specifically provided by the BMBF comprises the so-called innovation platforms, an instrument to facilitate and foster networking between all relevant actors within the security research community.

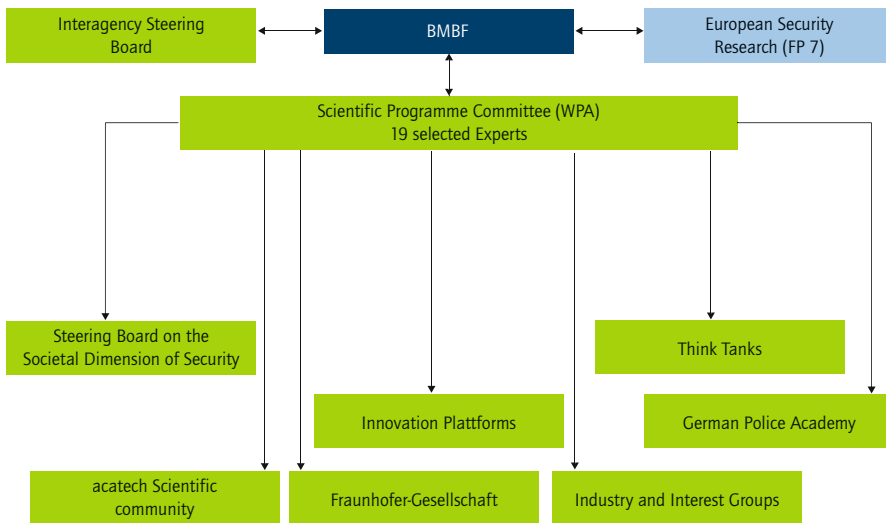
### INNOVATION PLATFORMS

A central institution already defined in the High-Tech Strategy – a national effort to support the development of innovative technologies for a sustainable future – are the so-called innovation platforms. Organised by the BMBF, these alliances have been established to facilitate the creation of strategic partnerships between end-users, industry and the research community. Taken together, they provide an effective platform for a continuous dialogue on the development of the whole innovation process within security research. Selected experts from the public and private sectors take advan-

tage of these platforms to exchange ideas and discuss future challenges related to on-going project activities and conceptual questions regarding the security research framework<sup>6</sup>.

End-user orientation is a central element in security research and many end users take very active part in the innovation platforms. Organisations such as federal and state law-enforcement authorities, as well as emergency services and relief organisations are strongly involved in the various projects. Around 80% of Germany's security-relevant infrastructure is owned and operated by the private sector; a fact that underscores the importance of the platforms' overall strategic directive of streamlining public and private efforts to successfully meet the demands of today's complex security environment.

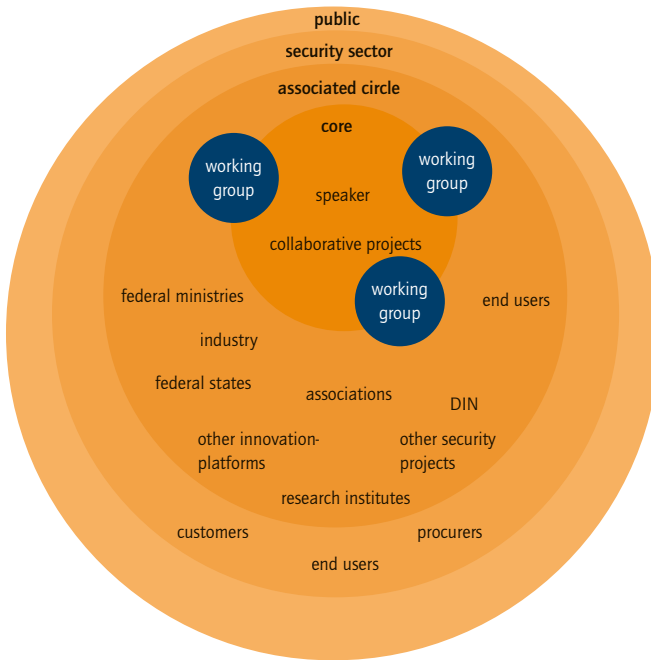
Figure 1: Linkage between the national players in the field of civil security research



Two innovation platforms have been successfully established to date. The innovation platform 'transport infrastructure protection' was initiated in September 2008. It centres on the 10 projects already approved in this area. Four working groups have been established to cover all modes of transportation, i.e. air, rail, sea and road. In June 2009 the second innovation platform, 'protection and rescue of people', was called into life. It includes the working groups for 'medical first aid' and 'strategy'.

<sup>6</sup> BMBF 2010b.

Figure 2: Structure of the innovation platforms



### 3 LINKS TO EUROPEAN SECURITY RESEARCH

A fundamental characteristic of today's security environment is the transnational nature of current and especially future threats. At the same time, our infrastructures (energy, transport, supply chains, etc.) are also transnationally networked, which has immense implications with regard to their vulnerability towards such threats. The phenomena of terrorism, organised crime and man-made or natural disasters all share the characteristic of not stopping at national borders. Accordingly, only cooperative efforts by alliances of countries will succeed in tackling these problems.

The European Union, an alliance of 27 countries sharing a common market, common borders and commonly formulated foreign and security policy goals, faces unique challenges. Acknowledging the complexity of the member states' diverging security concerns, perceptions and policies, the European Commission has taken the initiative in creating a European security research programme within its 7th Framework Programme (FP7). Over a period of six years between 2007 and 2013, the EU will spend 1.4 billion euro on security research. The programme is geared to four 'missions':

- Security of citizens
- Security of infrastructures and utilities
- Intelligent surveillance and border security
- Restoring security and safety in case of crisis

In addition, three cross-cutting missions have been defined to acknowledge the political and societal dimensions of technology-based research and improve the overall effectiveness and efficiency of all research activities. Each mission is addressed in corresponding collaborative projects. The three cross-cutting missions are:

- Security systems integration, interconnectivity and interoperability
- Security and society
- Security Research coordination and structuring

The European and the German security research programmes were initiated at around the same time. Both concentrate specifically on civil security solutions and both have a strong focus on the involvement of end-users and the private sector. Aligning the German research programme with the EU programme makes perfect sense, as many security solutions will only be effective if implemented on a European-wide level. Furthermore, standardisation processes, as well as legislation and regulation initiatives on a European level, must accompany the introduction of such common solutions. This is essential for an emerging European security industry and the respective market, which, according to a 2009 study conducted for the Directorate of Enterprise & Industry of the European Commission, has an annual volume of about 30 billion euro<sup>7</sup>. However, EU efforts in this field cannot serve as a substitute for national activities. Just like all member states, Germany has its own security interests and concerns. Aspects that need to be targeted when formulating the national security research agenda include Germany's central geographical location in Europe and the highly developed infrastructures in connection with its strength as an export champion, as well as social and cultural peculiarities. Notwithstanding, there is a visible alignment in the overall structure and specific programme lines of German and other national security research programmes within the EU. Past comparisons have shown strong agreement in selected technology areas when matching German, French and the EU security research programmes<sup>8</sup>.

#### **4 ORGANISING FOR A RESILIENT SOCIETY – A HOLISTIC APPROACH TO SECURITY**

Over the past decade, traditional concepts and paradigms within the field of security have been subject to critical scrutiny. The range of issues to consider in the discipline has been broadened in numerous ways. Two fundamental aspects characterise the secu-

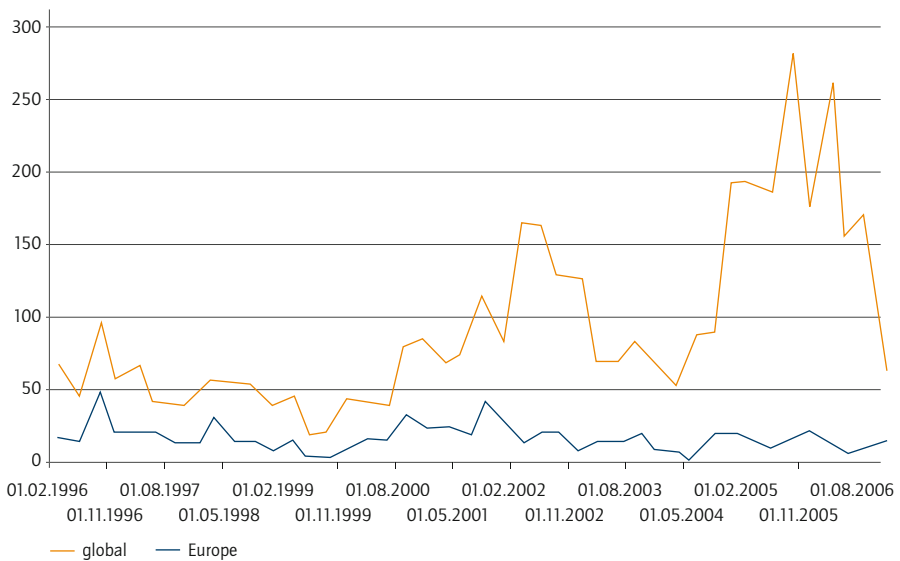
<sup>7</sup> ECORYS 2009.

<sup>8</sup> acatech 2010a.



ity environment of the 21st century: threats and risks we are facing have changed significantly while, at the same time, the vulnerabilities within society have changed. The former, including phenomena such as transnational terrorism, strongly challenge the foundations our liberal democracies rest upon. The increasing number of transnationally active terrorist groups is a significant symbolic indicator of this new environment.

Figure 3. Terrorist attacks committed by internationally operating terrorist organisations between 1996 and 2006<sup>9</sup>.



As a consequence, trade-offs involving the limitation of civil liberties or the granting of extensive powers to the public security apparatus are a contentious issue heatedly debated among Western democratic societies. In the end, the transnational nature of these threats is responsible for the fact that former distinctions between internal and external security, between the realms of public and private spheres or between the jurisdiction of security relevant agencies and institutions continue to dissolve. The consequences of these developments for those in charge of security, i.e. governments, security institutions, but also research organisations and industry, are manifold.

Considering the interdependence between the public and the private sectors leads to a second important aspect: the new types of vulnerabilities our societies are facing. Actions taken by governmental security institutions to reduce the vulnerabilities of our

<sup>9</sup> Siebold 2010.

modern infrastructures – be it our energy and water supply systems, our transportation and supply chain systems or our complex ICT networks – will have limited success, unless the private sector is directly involved in such efforts. Many vulnerabilities in our networked societies result from the way our economies function. Large parts of our central infrastructures on local, state or federal levels are either owned or operated by a highly fragmented private sector (a good example is the networked structure of local water and power suppliers). In turn, this complex system of interconnected critical nodes, with security responsibilities spread among so many different actors, results in a multiplicity of vulnerabilities.

Governments and related security institutions design and implement strategic concepts and programmes in response to the challenges posed by these highly complex environments. At the same time, the aforementioned efforts over the past few years have led to the establishment of security research as an entirely new discipline in which research organisations, private industry and end-users cooperate in developing innovative security concepts and technologies helping to reduce vulnerabilities in our societies and provide means to respond effectively to man-made and natural catastrophes. Perspectives and opinions vary strongly with regard to the scope and application of security technologies, and their effects on society as a whole. Consensus seems to exist only on the fact that absolute security is not possible. Accordingly, there is a broad range of approaches on how best to tackle the security challenges we face.

One particular approach that is attracting increased international attention of late is the concept of resilience. Historically, resilience has found application in disciplines such as psychology, engineering, ecology and management. Great Britain and the United States have taken the lead in integrating the idea of a resilient society into their respective security policy-making processes. The general premise of this concept is that a blanket guarantee for security is not possible given the complexity, diversity and unpredictability of modern risks. The concept of resilience involves increasing the general resistance and regeneration capacity of societal and technical systems in a holistic approach. In other words, resilient societies develop comprehensive cultures of awareness and anticipation regarding threats to their security. They 'bounce back' to normal status following man-made or naturally caused crisis situations.

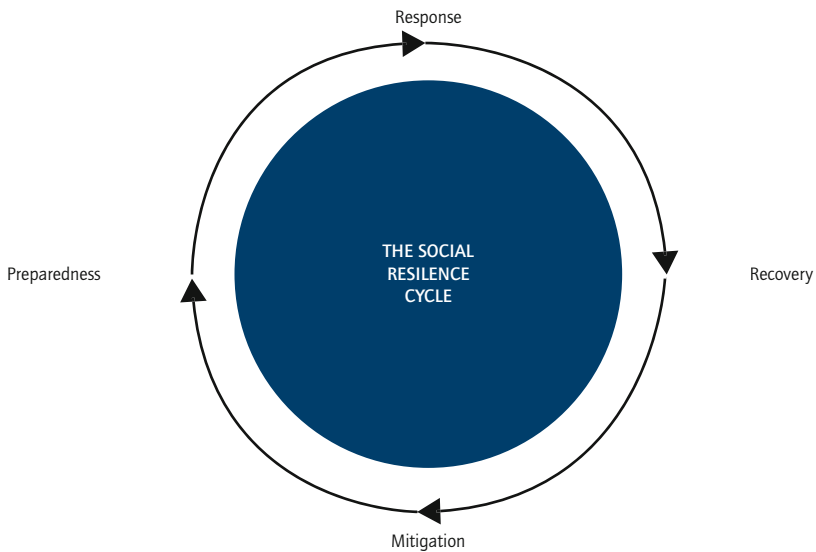
Recent studies on resilience even call for expanding the concept. For instance, in his pamphlet 'Resilient Nation', Charlie Edwards, a British expert in the field of resilience, persuasively argues the case<sup>10</sup>. Rather than thinking of resilience in a mechanistic way, as some sort of a political strategy designed and implemented by state institutions, there should be a much stronger focus on the role of the individual citizen within the societal system as a whole. According to his analysis, viewing resilience as the capability of a society to respond to and cope with major shocks and then 'bounce back' to pre-shock status is too narrow, short-term and reactive when considering the full scope

---

<sup>10</sup> Edwards 2009.

of resilience. Instead, Edwards focuses on the human capacity for learning and adapting, going beyond a mere 'bounce-back' factor. Instead of premising the concept of resilience on a command and control approach designed and implemented from the top down by government institutions, he calls for an approach that revolves about the role of individual citizens within their community. A prerequisite for establishing this resilience concept is the presence of the four 'Es': *engagement, education, empowerment* and *encouragement*.<sup>11</sup> Although Edward's assessments focus on the UK approach to resilience, they offer promising potential for adoption by other European countries. To conceptualise the idea of social resilience in crisis situations, Edwards developed the so-called 'social resilience cycle', which provides a conceptual framework to increase societal resilience at a very local level<sup>12</sup>.

Figure 4: The social resilience cycle



Michael Bruneau, director of the Multidisciplinary Center of Earthquake Engineering Research (MCEER) in Buffalo (USA), places more emphasis on the macro level in applying the concept of resilience and has developed an organisational resilience framework that is geared specifically to 'disaster resilience'. The concept entails the ability of larger social units to mitigate hazards, contain the effects of disasters and carry out recovery

<sup>11</sup> Edwards 2009.

<sup>12</sup> Edwards 2009.

activities in ways that minimise social disruption, while mitigating the effects of future disasters<sup>13</sup>. In sum, Bruneau has designed the four 'Rs' to highlight the general idea with specific properties.

- **Robustness:** The ability of an economic entity to resist or forestall damaging or catastrophic events.
- **Redundancy:** An organisational unit's ability to provide alternative processes for inline or critical systems.
- **Resourcefulness:** A characteristic of an entity's tenacious response to and creative solutions for a disaster related instance.
- **Rapidity:** The ability to quickly restore systems or processes

More generally speaking, these approaches indicate the breadth in scope that the whole concept encompasses. Whereas some, such as Edwards, emphasize the role of individuals embedded in communities and social networks as paramount to the role of state institutions, others, such as Bruneau, point to the importance of the systemic resilience of larger organisations and networks, stressing the macro level in the effective application of the resilience concept.

The fundamental characteristics of a resilient society are:

- **Thinking and behaviour** of citizens – Creating shock and awe is a key objective of terrorism. Societies that foster awareness for avoiding panic and facilitating quick recovery to pre-attack status are much less vulnerable to attack. They are also less prone to overreact with restrictive measures, which terrorists often specifically intend to trigger.
- **Design of critical infrastructure** – Making the critical nodes of our modern networked societies secure and resilient 'by design' is no trivial task. It involves a broad range of aspects, including the reduction of possible cascade effects in case of a crisis and blast-resistant critical infrastructure buildings. Resilience by design may appear to be purely reactive in nature, but in reality it involves a strongly proactive approach that
  - Anticipates crisis situations
  - Has strategies to survive these situations
  - Constantly derives improvements for the future from occurring crises
- **Crisis management and communication between all involved actors** – Crisis situations can arise any time and at any system level. The resilience concept provides a guideline for emergency management, disaster relief and damage control. In highly resilient societies there is a consensus on the challenges, re-

---

<sup>13</sup> Bruneau 2006.

sponsibilities are clearly assigned to various actors and emergency responses are centrally coordinated. These societies practice strategic risk management and generally have a risk communication strategy at their disposal. It goes without saying that adaptability and flexibility are key characteristics of a highly resilient society<sup>14</sup>.

- **Economic dimension of security** – Investments must always withstand the scrutiny of cost-benefit analyses. In the past, security regulations and measures often came under fire because they were perceived as a burden that slows down business processes: The time and money invested outweighed the benefits by far. Recently, however, there has been a change in decision-makers' mindsets. They are now much more open to the idea of integrating security aspects into their business models. In the end, they have come to realise that sustainable, long-term success can only be guaranteed by maximizing the synergy between security and efficiency.

#### 4 OUTLOOK

With the initiation of its first national civil security research programme, Germany laid an important foundation in its quest to better protect its citizens against a multiplicity of modern threats. Boosting research capabilities has led to significant progress on the long road to a more secure and resilient nation. It has also spawned numerous innovative concepts and technologies to thwart or minimise risks and threats, and to recover from crisis following catastrophic events. Substantial funding, from both government and private sector, is being allocated to a variety of projects spanning a wide array of topics. The projects from the first round of funding are currently in their final phases. Now is the time to take the established framework to the next step, ensuring the continuation of successful research. A specific strength of the German civil security programme is the incorporation of all relevant disciplines, including the technical and social sciences. Past experience with crisis situations and phenomena, such as public reaction to terrorist attacks, has shown that the societal impact of security related issues is every bit as important as the development of technological solutions.

With the inception of its first national civil security programme, Germany has seen the emergence of a broad security research community, including the establishment of various think tanks, interest groups and advisory bodies. As the ministry in charge of the security research programme, the BMBF has direct access to extensive expertise in the field. The ministry itself has established the so-called innovation platforms, providing a forum for discussion and the exchange of innovative ideas and solutions between researchers, end-users and industry. At the same time, the community has come to realise that substantial results can be realised only with well-structured communication networks of the various actors. A jointly accepted process of coordination must ensure the optimal

---

<sup>14</sup> CSS Analysen 2009.

dispersal of existing ideas and innovations throughout the security research community. We have argued that a national civil security programme that caters to German security concerns, perceptions and culture is a necessary counterpart to European efforts in the field. Going beyond that, the national programme has also been specifically designed to prepare and strengthen German partners for successful participation in the EU's FP 7 projects. At the end of the day, a successfully implemented national security research programme will increase Germany's influence on the agenda setting process of future security research programmes within the EU.

A fundamental conclusion of all security research related activities is that security is inevitably linked to many other topics relevant to the overall functioning of our modern societies. Whether in the field of energy, mobility, health or communication, any future concepts and scenarios that lack integration of security aspects may have a very short validity. This challenge can only be met with a holistic approach to security. In this context holistic refers to the integration of security concerns right from the 'design stage' of technological innovations or conceptual frameworks in all of the aforementioned fields. Security research remains a cross-sectional and cross-departmental topic. It unites various disciplines of the natural, technical and social sciences to master the challenges of today's highly complex civil security environment.

On a macro level, traditional concepts and paradigms of security are at the heart of rigorous discourse among policy makers, as well as researchers, end-users and private players. A relatively young concept in the field of security that is attracting a lot of attention is the concept of a resilient society. The fundamental premise of resilience is that blanket guarantees of security are not possible given the complexity, diversity and unpredictability of modern risks. Instead, the concept of resilience aims to increase the general resistance and regeneration capacity of societal and technical systems.

In Germany, research in field of resilience has been limited. Profound theoretical assumptions and practical ramifications are still lacking. However, current developments indicate that the German security research community will increasingly adopt and enhance the concept of resilience, as it is already widely applied in countries such as the UK and the United States. Ultimately, the resilience model comprises ideas that may prove crucial in the design and implementation of future security concepts and related security research agendas.

## 5 REFERENCES

### acatech 2010a

Thoma, Klaus/Drees, Birgit/Leismann, Tobias: Zukunftstechnologien in der Sicherheitsforschung. In: Winzer, Petra/Schnieder, Eckehard/Bach, Friedrich-Wilhelm (eds.): Sicherheitsforschung – Chancen und Perspektiven. München, 2009

**acatech 2010b**

Hoffknecht, Andreas/Teichert, Olav/Zweck, Axel: 'Forschung für die zivile Sicherheit' – Das nationale Sicherheitsforschungsprogramm. In: Winzer, Petra/Schnieder, Eckehard/Bach, Friedrich-Wilhelm (eds.): Sicherheitsforschung – Chancen und Perspektiven. München, 2010

**BMBF 2006**

Bundesministerium für Bildung und Forschung, BMBF (ed): Die Hightech-Strategie für Deutschland. Berlin: 2006.

**BMBF 2007**

Bundesministerium für Bildung und Forschung, BMBF (ed): Forschung für die zivile Sicherheit – Programm der Bundesregierung. Berlin: 2007.

**Bruneau 2006**

Bruneau, Michael, director of the Multidisciplinary Center of Earthquake Engineering Research (MCEER), MCEER Resilience Framework. Buffalo 2006 online available at: [http://mceer.buffalo.edu/research/resilience/Resilience\\_10-24-06.pdf](http://mceer.buffalo.edu/research/resilience/Resilience_10-24-06.pdf)

**CSS Analysen 2009**

Trachsler, Daniel: Resilienz: Konzept zur Krisen- und Katastrophenbewältigung. CSS-ETH Zürich – CSS Analysen zur Sicherheitspolitik, Nr. 60 September 2009. Zürich 2009

**ECORYS 2009**

ECORYS 2009: Study on the Competitiveness of the EU security industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054. Conducted for the Directorate-General Enterprise & Industry, European Commission. Brussels: 2009.

**Edwards 2009**

Edwards, Charlie: Resilient Nation. Demos. London: 2009.

**Siebold 2010**

Albrecht, Hans-Jörg/Arnold, Harald/Haverkamp, Rita (ed.): 'The prediction of terrorist attacks - Is it possible to identify pre-incident indicators for these crimes?'. Freiburg: 2010

## Internet Sources

### **BMBF 2010a**

Bundesministerium für Bildung und Forschung, BMBF: Scientific Programme Board Security Research available at: <http://www.bmbf.de/en/11781.php> (status of: 14.04.2010).

### **BMBF 2010b**

Bundesministerium für Bildung und Forschung, BMBF: Innovationsplattformen: Von der Forschung aus vorausdenken available at: <http://www.bmbf.de/de/12907.php> (status of: 20.04.2010).

### **BMBF 2010c**

Bundesministerium für Bildung und Forschung, BMBF: Innovationsplattform Schutz von Verkehrsinfrastrukturen available at: <http://www.bmbf.de/de/12913.php> (status of: 26.04.2010).

### **BMBF 2010d**

Bundesministerium für Bildung und Forschung, BMBF: Innovationsplattform Schutz und Rettung von Menschen available at: <http://www.bmbf.de/de/12909.php> (status of: 26.04.2010).



## > UK PERSPECTIVES ON SECURITY IN AN AGE OF 'SHOCK AND AFTERSHOCK'

TOBIAS FEAKIN

In many European languages the terms 'security' and 'safety' are represented by the same word and carry the same meaning: Sécurité (French), Veiligheid (Dutch), Sicherheit (German), Sikkerhet (Danish), Seguridad (Spanish), Sicurezza (Italian), Bezpiecze stwo (Polish), Segurança (Portuguese). Whilst the words have very similar meanings in the English language they have very different connotations and are used in different ways.

**Security - noun** (pl. **securities**) **1** the state of being or feeling secure. **2** the safety of a state or organization against criminal activity such as terrorism or espionage.

**Safety - noun** (pl. **safeties**) **1** the condition of being safe. **2** before another noun denoting something designed to prevent injury or damage: *a safety barrier*

In the same way that Josephs Nye's concepts of 'hard' and 'soft' power differentiates between methods that require force or coercion and those that require diplomatic action, one can distinguish between the two terms 'security' and 'safety' in terms of the connotations that the words have. While 'security' conjures images of terrorism, policing, intelligence agencies and hard-edged responses, 'safety' conveys a more benign, paternal image of the parent that wants to keep its child from harm.

However, both concepts have become debated at the European level, with 'public safety' used in many European countries to describe what is referred to as 'Homeland Security' in the US and 'National Security' in the UK. In fact, many European policy makers prefer to use terms such as internal security, civil protection, or collaborative security when referring to intra-EU security issues. This reflects sensitivities in the language used in this paradigm within Europe.

### UK PERCEPTIONS OF SECURITY THROUGH A NATIONAL SECURITY STRATEGY

Eric Hobsbawm, one of the most notable historians of recent times, has characterised the twentieth century as 'The Age of Extremes'.<sup>1</sup> These extremes were viewed both in terms of the technological and social change that took place during that era, as well as in reference to the extreme political cultures that shaped the two World Wars and the Cold War between ideologically opposed nations.<sup>2</sup> Yet, despite the magnitude of these trends and the impact they had on global security, the processes of gestation were often considerable. Governments thus had relatively long periods of time to prepare for and

---

<sup>1</sup> Hobsbawm 1994.

<sup>2</sup> Hobsbawm 1994.

respond to security threats. This is a stark contrast to the unfolding twenty-first century, which could well be characterised as 'The Age of Shock and Aftershock'. Unexpected events, aided by the speed of modern technology and media reporting, have dramatically shaped the international security scene over a very short period of time – changing the way in which both governments and citizens view their security.

The most prominent example of 'shock and aftershock' was the terrorist attack of 11 September 2001 and the impact it had on US domestic and foreign policy. Following the London attacks in July 2005, the UK started to perceive a terrorist threat that emanated from within its own population, leading to an overhaul of counter-terrorism approaches by the government. The phenomenon of globalisation is synonymous with the unprecedented interconnection of countries, as well as individuals. As a result, governments and citizens feel the aftershocks of events acutely, even when the initial shock occurs on the other side of the globe. Rethinking the ways in which governments view and respond to this new era of 'shock and aftershock' – conceptually and practically – has thus taken on a new significance.

Over the past two years discussions about the changing nature of the national security agenda have gathered a great deal of momentum within both academic spheres and UK government circles.<sup>3</sup> This is by no means a new debate: indeed, the security agenda burgeoned with the end of the Cold War, leading to the inclusion of economic and environmental security aspects. Security thinkers and strategists entered a new period of relative freedom, exploring security issues outside of the traditional military realm. However, the UK government's first attempt<sup>4</sup> to conceptualise this new security environment, linking both the defence and security agendas in one document, did not materialise until March 2008 when it published its first National Security Strategy.<sup>5</sup> This document laid the foundation for cross-departmental thinking on approaches to tackling the security issues of the day. In the government's own words:

*This groundbreaking approach to tackling security challenges reflected a profound and developing shift in our understanding of national security: broadening the concept beyond the traditional focus of the protection of the state and its interests from attacks by other states, to include threats to individual citizens and our way of life.<sup>6</sup>*

The document was certainly 'groundbreaking' with regard to the scope of security issues addressed: only few countries have national security strategies that cover such a wide range of security and defence issues in one place. The document was criticised for being too general and not actually containing a strategy on responding to new complex

<sup>3</sup> IPPR 2009, Edwards 2007

<sup>4</sup> Notwithstanding the Strategic Defence Review, which examined the linkages between foreign and domestic policy from a military perspective.

<sup>5</sup> Cabinet Office 2008

<sup>6</sup> Cabinet Office 2009

security threats of the twenty-first century.<sup>7</sup> To a certain extent this is true; no clear planning guidelines and assumptions were provided. However, the strategy did provide a valuable building block for pan-departmental thinking and a potentially more coherent approach to national security issues in the future.

Building on this initial effort, an updated version of the strategy was published in June 2009. It expanded on the first both intellectually and by providing planning assumptions to guide security priorities. Although the document is now starting to look more like a strategy, it is still lacking the kind of practical guidelines one would expect. Nonetheless, two key factors are worth noting. First, the global economic crisis is increasingly shaping government thinking on future types of national security threats and the ability of the government to adequately fund responses to those threats. Secondly, there appears to be a linked focus on more traditional security issues, such as the large defence sector programmes, public and private sector espionage, and the growth and spread of serious organised crime. This demonstrates how quickly national security priorities are changing in the twenty-first century. The 'shock' of the economic crisis has led to a re-focus of thinking in the UK from counter-terrorist issues to issues with short- to medium-term financial implications.

The National Security Strategy strongly reflects the wave of scholarly debate in the UK regarding our perceptions of security. The term 'security' is no longer defined merely along the narrow Westphalian notions of the 'nation state' and the protection of national sovereignty. Since the late 1990s, writers like Barry Buzan have examined how the term has evolved to encompass a far wider range of threats – both 'hard' and 'soft' – to individuals, communities, towns, cities or nations.<sup>8</sup> There is a danger, however, of the definition becoming so broad as to render it meaningless. In the end, what constitutes security or a threat to security is subjective. It ultimately depends on the perception of which communities, values and institutions really matter.

### UK RESILIENCE – THE 'ALL HAZARDS' APPROACH

The UK conducts its assessment of the key threats and hazards to the UK through the Civil Contingencies Secretariat, a department of the Cabinet Office. The secretariat was established in 2001 in response to the foot and mouth disease outbreak in the UK, together with the fuel strikes and blockades that brought the country to a near standstill in 2000. It became clear that the UK required a body with the authority to prepare, respond and recover from any kind of emergency, be it man made or natural. The Civil Contingencies Secretariat uses what is commonly referred to as the 'all-hazards' approach, meaning preparations should be sufficiently flexible to cover both natural and

---

<sup>7</sup> BBC 2008, Cornish 2008

<sup>8</sup> Buzan 1991.

man-made threats. 'Resilience' lies at the heart of the UK philosophy of emergency response. This refers to the ability of a nation and its population to absorb shocks and 'bounce back' to a normal state as quickly as possible. Some analysts consider this definition to be too narrow. Indeed, Adger believes the definition should extend beyond this as humans have the capacity to change and modify their behaviour. Rather than just 'bouncing back', societies can move forward and actually improve after a disaster:

*Resilience is the ability of a system to absorb change while retaining essential function; to have the ability for self-organisation; and the capacity to adapt and learn.<sup>9</sup>*

Every year the Civil Contingencies Secretariat assesses and publishes the National Risk Register, which sets out the government assessment of the likelihood and potential impact of risks that will directly impact the UK. Figure 1 shows [an excerpt from] the 2009 risk register. Although it was classified in the past, the document is now made public to encourage not only public debate on security issues, but also to assist individuals, families and communities in preparing for emergencies. This idea was to promote increased 'community resilience', the ability of local individuals to respond directly to emergencies in the early stages of a disaster, rather than having to rely completely on government response mechanisms. The risk register gives visual indication of the relative likelihood and impact an event would have on the UK, should it occur. The highest risk on the register is for influenza. This may come as a surprise to the reader, since terrorism is often perceived as the number one threat in the UK. Yet, in terms of the potential widespread impact, influenza is a more serious threat from the perspective of a government trying to protect its population.

### **CASE STUDY – COUNTERING TERRORISM – THE OFFICE FOR SECURITY AND COUNTER-TERRORISM (OSCT)**

The National Risk Register serves as the strategic context in defining the UK research agenda for science and technology (S&T). Individual government departments align their S & T agendas with this strategic vision.

The agenda is driven by the government's counter-terrorism (CT) and S&T requirements. This happens primarily through the Office for Security and Counter-Terrorism (OSCT), which is responsible for coordinating the UK's counter-terrorism efforts. This domain has been very much at the forefront of attempts to harness applicable and innovative UK technologies.

---

<sup>9</sup> Adger 2010.

The UK approach to counter-terrorism is defined in the CONTEST strategy built on the four pillars:

- Pursue - Stop terrorist attacks
- Prevent - Stop people from becoming terrorists or supporting violent extremism
- Protect - Strengthen UK protection against attacks
- Prepare - Mitigate the impact of attacks

The OSCT launched the 2009 UK Science and Technology Strategy for Countering International Terrorism. This strategy is a subset of CONTEST and has three objectives. The first is the use of horizon scanning to identify future scientific and technical threats and opportunities, and to communicate the government's policy on counter-terrorism. This kind of work is vital to understanding which technologies under development are likely to pose threats or provide solutions in the future. General scanning is not enough, though. It is essential that early signs of a technology coming to fruition be recognised so that the government has ample time to respond. The strategy makes identifying these triggers a priority.

The second objective is to ensure the development and delivery of effective counter-terrorism solutions by identifying and sharing priority science and technology requirements. Since many different departments work in the counter-terrorism domain, there are also numerous competing requirements that might be addressed with science or technology. Prioritising these requirements is not an easy task but mechanisms have been set up over the past few years to ensure that the government understands which challenges are the key priorities. This allows the government to collaborate with industry, SMEs and academia to ensure that they know what is needed, and understand how to open avenues to market for their products.

The third objective of the strategy is to enhance international collaboration on counter-terrorism related science and technology. Since modern terrorism is by nature international, the need for an international response is obvious. Collaboration between agencies in the UK and their counterparts overseas is vital to the enactment of CONTEST overall, and to the science and technology aspects in particular. The technology necessary to counter terrorism will not just be developed in the UK, thus a co-ordinated approach to counter-terrorism research will optimise government resources in the long term. The bulk of this work will be in partnership with the US and the EU. However, the UK government is committed to looking across the board for science and technology that may help meet shared objectives.<sup>10</sup>

---

<sup>10</sup> HM Government 2009.

The strategy signals a new way of communicating with industry and academia, committing to a series of brochures that discuss aspects of counter-terrorism in language making it accessible to industry and academia. Although security will always be an issue, it is possible to outline the main challenges without revealing classified information. This is clearly demonstrated in the first of these brochures, which was published alongside the strategy. In 'Ideas and innovation: How industry and academia can play their part'<sup>11</sup>, the government outlines key challenges, vital technologies and various routes to market. To ensure movement beyond the defence industries, the brochure has been sent to bodies that represent industries not normally associated with counter-terrorism, including health, finance and construction. The brochure has also been sent directly to academic institutions to ensure the government engages broadly with the cutting-edge of technology development. Future brochures will cover the work of the social and behavioural sciences in counter-terrorism and how science can help defend against chemical, biological, radiological, nuclear and enhanced conventional (CBRNe) terrorism.

In addition to its objectives, the strategy outlines key challenges – a subset of those discussed in CONTEST itself. The four challenges discussed in detail in the industry brochure are protecting the national infrastructure, reducing the vulnerability of crowded places, protecting against cyber terrorism and improving analytical tools. These areas can be addressed primarily by applying the physical sciences, but the next brochure will consider how social and behavioural sciences can support the government in countering terrorism.

### OSCT DIALOGUE WITH THE PRIVATE SECTOR AND ACADEMIA

It is no surprise that the OSCT has become a leader in the area of security-related S&T innovation. This is a direct result of the sheer level of investment. The single security and intelligence budget, which includes government spending on counter-terrorism and intelligence, was announced as part of the 2007 Comprehensive Spending Review. It was forecast to rise from £2.5 billion in 2008/09 to £3.5 billion in 2010/11.

Furthermore, the OSCT has been building relationships with the private sector – something it has been less comfortable with in the past. The UK Security and Resilience Industry Supplier's Community (RISC) – an alliance of trade bodies, think tanks and key industry bodies – have been active to create an atmosphere of 'trust' leading to a more wholesome dialogue between the Home Office and industry. This partnership has grown to an extent that RISC are used as a sounding board for new ideas and approaches. RISC have set up a number of bodies responsible for innovating in specific the areas of CNI, the Olympics, stand-off detection, CBRN and ICT.<sup>12</sup>

<sup>11</sup> HM Government 2009.

<sup>12</sup> More information on RISC and their work can be found at [www.riscuk.org](http://www.riscuk.org).

The government also maintains links to academia through various academic research councils, such as:

- Biotechnology & Biological Sciences Research Council (BBSRC);
- Economic & Social Research Council (ESRC);
- Engineering & Physical Sciences Research Council (EPSRC);
- Medical Research Council (MRC);
- Natural Environment Research Council (NERC);
- Science & Technology Facilities Council (STFC).

## CONCLUSIONS

### CITIZEN-CENTRIC SECURITY – THE ISSUE OF TRUST

In UK national security documentation there is a growing onus on individuals to take responsibility for their own security by being prepared and aware of potential threats and hazards in their immediate vicinity or online. When it comes to security, sharing responsibility between the state and society makes good sense. Unfortunately, growing civic independence and decreasing trust in state functions since the end of the last century tend to hamper this kind of burden sharing. At the community level, the government has actively sought engagement with regions at risk from natural disaster through the Civil Contingencies Secretariat. Local Resilience Forums also conduct workshops to raise awareness of emergency preparedness. Yet, the people who attend these workshops are usually those who are already actively involved in community projects. The question of how the government can best reach those who do not engage remains open.

Will the government departmental cuts expected over the next six months lead to a reassessment of how money is spent on security? Counter-terrorist activity receives a sizable portion of budget, since the government has perceived this as a priority area in recent years. However, can this level of investment be sustained in the coming years? How can the government encourage the high levels of innovation and technology development required in this area if budgets are cut? This may become clearer as the Strategic Security and Defence Review takes place in the UK. However, at present the only thing that seems certain is that spending will be cut in most areas – and priorities will shift as a result.

A bigger problem is the historically low level of public trust in the government's strategic risk communication, the parliamentary system and the presiding MPs. Therein lies the crux: The government wants to place citizens at the heart of security, encouraging them to assume more responsibility for their own security, while entrusting the government with other areas of their safety. How can this position be reconciled with

the public's distrust of the government and its communicated policies? One of the most pressing issues in the current national security debate is the question of how the government can re-establish public trust in its policies and communications. The answer to this question will be pivotal in making real national security advances in the months to come. Should the government not get it right, it will have to brace for the 'aftershock' of an electorate who have little faith in the decisions that it takes.

## REFERENCES

### **Adger 2010**

Adger, W. N.: Climate change, human well-being and insecurity. *New Political Economy* 15, in press.

### **BBC 2008**

BBC: "Brown unveils security strategy", BBC News Online, 19th March 2008. Available online: [http://news.bbc.co.uk/1/hi/uk\\_politics/7303846.stm](http://news.bbc.co.uk/1/hi/uk_politics/7303846.stm)

### **Buzan 1991**

Buzan, B.: *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, 2nd Edition. Hemel Hempstead, Harvester Wheatsheaf, 1991.

### **Cabinet Office 2008**

Cabinet Office: *The National Security Strategy of the United Kingdom – Security in an interdependent world*. Crown Copyright, UK, 2008.

### **Cabinet Office 2009**

Cabinet Office: *The National Security of the United Kingdom: Update 2009 – Security for the Next Generation*. Crown copyright, UK, 2009.

### **Cornish 2008**

Cornish, Paul: "The national security strategy of the United Kingdom – How radical can Britain be?", Chatham House Experts Comments, 26th March 2008. Available online: <http://www.chathamhouse.org.uk/media/comment/nss/>

### **Edwards 2007**

Edwards, Charlie: "The case for a national security strategy". DEMOS Report, London February 2007.



**Hobsbawm 1994**

Hobsbawm, Eric: Age of Extremes – The Short Twentieth Century 1914-1991. Abacus, London, 1994.

**HM Government 2009a**

HM Government: The United Kingdom's Science and Technology Strategy for Countering International Terrorism. London, UK, 2009.

**HM Government 2009b**

HM Government: Countering the Terrorist Threat - Ideas and innovation Countering the terrorist threat - How industry and academia can play their part. London, UK, 2009.

**IPPR 2009**

IPPR Commission on National Security in the 21st Century: Shared Responsibilities – A national security strategy for the UK. IPPR, London, 2009.

# > DEFENCE AND SECURITY RESEARCH COEXISTENCE, COHERENCE, AND CONVERGENCE

CHRISTIAN BREANT/ULRICH KAROCK

## INTRODUCTION

Defence and security research have coexisted at the European Union level since the inception of the European Defence Agency (EDA). The agency was established under a Joint Action of the Council of Ministers on 12 July 2004, "to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future".<sup>1</sup> The political decision to create the EDA was taken at the Thessaloniki European Council on 19 and 20 June 2003. Heads of State or Government tasked the Council bodies to undertake the requisite actions, in the course of 2004, to create an intergovernmental agency in the field of defence capabilities development, research, acquisition and armaments. The EDA has been located in Brussels right from the start. It is an intergovernmental EU agency under the Council's authority within the single institutional framework of the Union. It performs its mission in close cooperation with its participating Member States (pMS) and the European institutional actors.

Since the Lisbon Treaty came into force on 1 December 2009, the European Defence Agency and its tasks have been enshrined in the treaties, specifically Article 42 (3) and Article 45 of the Treaty on European Union (TEU). Article 42 (3) of the Treaty on European Union stipulates that the Agency "shall identify operational requirements, shall promote measures to satisfy those requirements, shall contribute to identifying and, where appropriate, implementing any measure needed to strengthen the industrial and technological base of the defence sector, shall participate in defining a European capabilities and armaments policy, and shall assist the Council in evaluating the improvement of military capabilities".

The EDA has a special status in the single institutional framework of the EU. It is the only Union agency founded in the treaties – otherwise only the case for the institutions – and the agency has an intergovernmental ministerial governance structure with representatives from all participating Member States' ministries of defence. In contrast to the other Union agencies, which have no role in policymaking, the EDA is tasked to participate in defining a European capabilities and armaments policy, and has the corresponding capacity of initiative and recommendation.<sup>2</sup>

---

<sup>1</sup> See article 2 of the Joint Action 2004/551/CFSP of the Council.

<sup>2</sup> See articles 42(3) and 45 TEU and to article 4(5) Joint Action 2004/551/CFSP of the Council.

## THE CAPABILITY DRIVEN APPROACH

The EDA's mission is to support the Council and the Member States in their effort to improve the European Union's defence capabilities for the Common Security and Defence Policy (CSDP). Thus, the Agency has a capability-driven approach. Everything it does is underpinned by the acid test of whether the activities will improve European defence capabilities.

The capability-driven approach starts by developing an understanding of the defence capabilities required to meet the needs of contemporary and future operations. What challenges and threats will European forces face? What impact will technology have, both on European capacities but also to the advantage of adversaries? What can be learned from on-going crisis management operations? In essence, European capability development needs to be approached from a common perspective.

The Capability Development Plan (CDP) serves as the basis for the agency's capability-driven approach. It was developed collectively with the participating Member States, the Council General Secretariat and the EU Military Committee (EUMC), supported by the EU Military Staff (EUMS). The EDA Steering Board provided the guidance and endorsed the CDP in July 2008.

Figure 1: Priority actions of the CDP.

12 SELECTED PRIORITY ACTIONS	OTHER PRIORITY ACTIONS
Counter Man Portable Air Defence Systems	Information Management
Computer Network Operations	Fuel & Power
Mine Counter-Measures in littoral sea areas	Deployable Air Power for ESDP Operations
Comprehensive Approach – military implications	Rapid Land Manoeuvre in the 21st Century
Military Human Intelligence & Cultural/language Training	Sea-basing
Intelligence, Surveillance, Target Acquisition & Reconnaissance Architecture	Open Source Intelligence (OSINT)
Medical Support	Space
Chemical, Biological, Radiological & Nuclear Defence	ISR Sensors and Collectors
Third Party Logistic Support	Electromagnetic Spectrum Management
Counter-Improvised Explosive Device	Wide-area Maritime Surveillance
Increased availability of helicopters	Reception Staging and Onward Movement
Network Enabled Capability	Non-lethal Capabilities

The Capability Development Plan gives an auditable depiction of the EU's ability to undertake all of the defence tasks required for CSDP over the short, medium and longer terms. The inputs come from the Headline Goal 2010 Progress Catalogue, lessons learned from crisis management operations, Member States' programmes to address capability improvement and finally from a focused, long term analysis (2025+). A series of conclusions were drawn from this depiction and, in turn, 12 priority actions in capabilities formation selected by the Steering Board (see to Figure 1).

In brief, the CDP conclusions emphasise the need for agility and adaptability. This involves not only developing capabilities such as precision engagement and strategic reach, but also includes developing appropriate force structures that can meet the operational needs. Maintaining the initiative in an asymmetric environment calls for both appropriate tactics and force protection assets. Knowledge-based operations are paramount to better understanding future complex operating environments. This ranges from high technology solutions to training all deployed forces to understand their mission environment. Comprehensive and coordinated actions are key factors in conducting the operations of today and tomorrow, and involve a mix of military and civilian actors, with network enabled capability vital for the synchronisation of effects. People remain the critical asset and the human factor underpins all operations, as does the need for a common understanding, derived from harmonised concepts and doctrines, of how operations should be conducted.

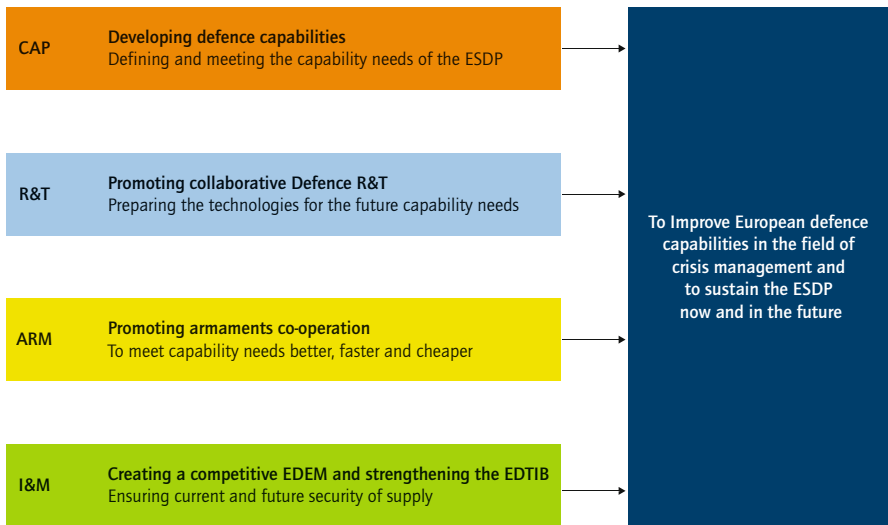
### **EDA'S INTEGRATED MODE OF WORKING**

Capability development starts with the harmonisation of military requirements. This is essential to prevent fragmentation of demand that ultimately leads to national capabilities without interoperability and standardisation – the last thing needed in today's and tomorrow's multinational operations. Harmonisation of military requirements is the core business of EDA's Capability Directorate.

However, three other functional areas are indispensable for providing capabilities: Research & Technology, Armaments Cooperation, and Industry and Market. Science and new technologies can offer great scope for improving military capabilities and addressing technological challenges posed by adversaries. Promoting more collaborative R&T is a key activity of the Agency, for which it has an R&T Directorate. Once military requirements have been harmonised and, where applicable, R&T results have been taken on board, the preparation phase of Armaments Cooperation begins. The EDA Armaments Directorate plays the central role in facilitating these programme preparation phases, during which options to meet the requirements are considered, procurement strategies are identified, industrial aspects are taken into account and, ultimately, a way forward is recommended.

Finally, without industrial supply there would be no equipment or other material required to carry out operations. Industry must be capability driven. At the same time industrial-technological capacities will impact capability needs, which is very welcome as long as they fit in the CDP context. Strengthening a capability-driven, competent and competitive European defence technology and industry base, as well as promoting a more transparent and competitive European defence equipment market is the central task of the EDA Industry and Market Directorate.

Figure 2: Key tasks of the EDA functional directorates<sup>3</sup>



A unique feature of the Agency is the integrated approach these four functional areas use to collaborate closely. The involvement of each of the four functional Directorates is not sequential, but iterative. Military capability planners, research and technology experts, armament cooperation programme managers and industries can no longer operate in their own 'stove-pipes' – they have to work closely together right from the start. In other words, supply and demand both need to sit at the table from the initial phase of requirements definition to the production phase. This unique way of working allows the Agency and its participating Member States to develop truly common requirements that amount to more than just the sum of national requirements. Harmonising requirements early on allows for incorporation of national demands, which at a later stage would

<sup>3</sup> CAP: Capabilities, R&T: Research and Technology, ARM: Armaments, I&M: Industry and Market.

lead to longer production cycles and rising costs. With defence budgets under severe constraints everywhere across Europe, the EDA's integrated way of working enables its Member States to engage in more affordable programmes and shorter development cycles, and to realise more flexible operational capabilities.

### THE EDA AND ITS PARTICIPATING MEMBER STATES

Twenty-six EU Member States participate in the EDA<sup>4</sup> (EDA26). As the Agency's "shareholders", they sit on the EDA Steering Board, they pay the annual budget, their national experts participate in EDA activities and they invest in projects and programmes. The Agency is an 'instrument' in the hands of the participating Member States, in particular of their ministries of defence.

The participating Member States 'own' the EDA. Their engagement in its activities is crucial for its success. That is why the Agency works with decision-makers and experts from capitals; they are the key actors in defence planning, R&T investment, equipment procurement and defence industrial and market issues. The Agency falls under the authority of the Council, to which it reports and from which it receives guidelines once per year. The Steering Board is the EDA governing body and comprises the pMS defence ministers plus a representative from the Commission (without voting rights). It represents the decision-making level in the seats of government. The Steering Board usually meets in further configurations with capability directors, national armaments directors and R&T directors. The Steering Boards are supported by a permanent network of national points of contacts (POCs) in the functional areas and for organisational, institutional and budgetary matters.

Beneath the decision-making level, the Agency operates in topical areas with various working level bodies. This is the level of the experts. They participate in line with the principle of "géométrie variable", depending on their national interests. Logically, the more general the area, the more Member States participate; the more specific the area, the fewer Member States participate.

### PROMOTING DEFENCE RESEARCH

In research and technology there is also a network of experts that operate at a level below the Steering Board in R&T formation and the R&T POCs. The CapTechs were designed for this purpose in the early days of the Agency. Each of them focuses on particular technologies associated with different military domains and bring together a network of experts from the Member States, industry, research institutes, academic institutions and agencies (both European and national).

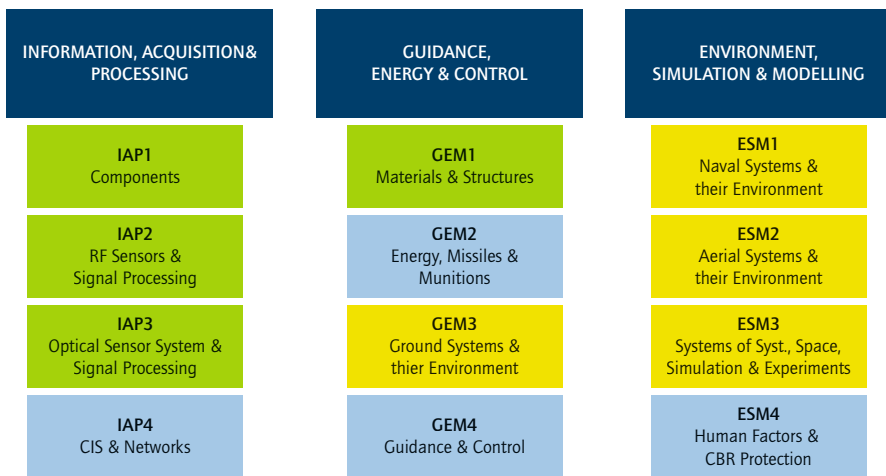
---

<sup>4</sup> All EU member states except Denmark; Denmark does not participate in the Agency due to its opt-out from the military aspects of CSDP.

There are twelve CapTechs<sup>5</sup> in total, grouped in three main areas (see Figure 3<sup>6</sup>). All CapTechs operate under the supervision of an EDA CapTech moderator. They meet regularly but also communicate on a daily basis via the Agency's extranet fora.

The aim of the CapTechs is to propose R&T activities in response to agreed on defence capability needs and to generate projects accordingly. Management and planning of research activity in each technology domain contributes to the Strategic Research Agendas (SRA), thus to improving the R&T collaboration between Member States.

Figure 3: The R&T CapTechs



## DEVELOPMENT OF EUROPEAN DEFENCE RESEARCH

Promoting defence research at European level has been at the heart of the Agency's task since its early years. In 2005 it took over the operational activities of the Western European Armaments Group (WEAG) and unfolded its own R&T activities. To date the total contracted volume amounts to over 300 million euro (see Figure 4).

<sup>5</sup> A CAPTECH is both a Technology Area focused on a particular military domain and the technologies associated with it, and a Network of Experts drawn from Member States, Industry, Research Institutes, Academic Institutions and Agencies (International, European and National).

<sup>6</sup> Green: underpinning technologies – blue: applied technologies – yellow: system technologies.

Figure 4: Development of EDA's Research, Technology Development and Demonstration activities

YEAR	STUFF	OPERATIONAL BUDGET (MILLION €)	CATEGORY A (OPTOUT) (MILLION €)	CATEGORY B (OPTIN) (MILLION €)	TOTAL (MILLION €)
2004	8	No operational activities of EDA			
2005	79	3	End of WEAC activities		3
2006	94	5	0	0	5
2007	98	5	16	55	76
2008	99	6	21	76	103
2009	109	8	41	131	180

The funding instruments of EDA are:

- *Operational budget studies and projects* – for procuring external advice, including operational analysis, essential for the Agency to discharge its tasks, and for specific research and technology activities for the common benefit of all participating Member States, notably technical case-studies and pre-feasibility studies.
- *Ad hoc projects and programmes* – a flexible instrument for any kind of collaborative research and development activity. Category A includes projects or programmes to which, in principle, all pMS contribute (but opting out is possible). Category B includes projects to which only the initiators contribute (but opting in is possible at the discretion of the initiators). The EDA can only initiate category A projects or programmes

However, collaborative defence research at the EDA represents only a small part of defence research done overall in Europe. Most of defence research remains national, and the level of defence research investment varies widely across Europe (see Figure 5).

The six biggest R&T investors among the participating Member States account for about 90% of the overall defence R&T spent, whereas the other 20 pMS contribute the remaining 10%. And, contrary to what might be expected, it is primarily the big six who participate in the European collaborative R&T, with some of the smaller R&T investors aiming mainly at European collaboration, rather than doing purely national defence research<sup>7</sup>.

<sup>7</sup> See <http://www.eda.europa.eu/defencefacts/> for more information.



Figure 5: Development of the Defence R&T Investment of the EDA26. (Figures in million euro – EDA6 are the six biggest investors in defence research among EDA pMS – No. 1 is the pMS with the highest defence research investment in a particular year.)

YEAR	NO. 1	NO. 2	NO. 3	NO. 4	NO. 5	NO. 6	EDA26	EDA6	6/26 %
2005	695	654	405	110	85	N/A	2200	1950	89%
2006	899	762	522	140	112	104	2656	2538	96%
2007	895	814	455	129	108	107	2613	2508	96%
2008	835	649	470	124	119	105	2479	2302	92%

## WORKING WITH THE EUROPEAN STAKEHOLDERS

Defence research may be considered, in general terms, as a specific functional development of certain technologies available for broader application. The Agency, therefore, needs to work closely with other international actors. Some of them are organisations working for civilian user communities, such as the European Commission and the European Space Agency. Increasingly, the EDA is synchronising its R&T investment with those two organisations to prevent taxpayers' money being spent twice on research in dual-use technologies. In November 2009, the Council underscored the added value of dual-use capabilities and gave further impetus to work related to identifying synergies between the EU civil and military capability development. In the stricter defence area, the EDA also closely interacts with a wide variety of international organisations, including NATO. All of these organisations, as well as others, are the Agency's stakeholders – they are important partners in improving European capabilities.

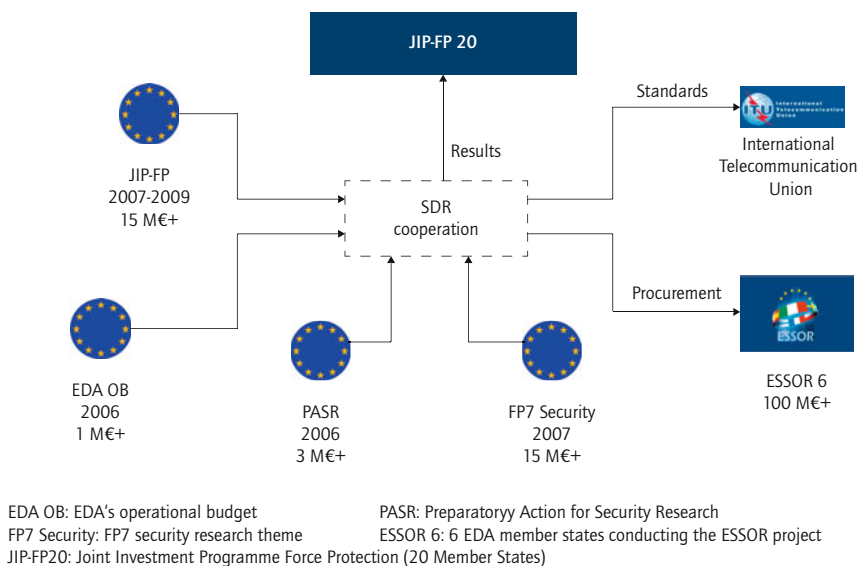
From its inception, the Agency has worked closely with the European Commission (EC) on its Industry & Market agendas. But the EDA and the EC also cooperate on capability development, in particular in areas where military and civilian users have overlapping requirements. This is the case in areas like communications, information, protection, transport and logistics.

Concerning R&T, the Agency has established an exchange of information with the Commission's Security Research Programme that involves cross-participation in respective fora. Commission representatives participate in the CapTechs and the Management Committees of the EDA Joint Investment Programmes "Force Protection" (JIP-FP, 2007-2009) and "Innovative Concepts and Emerging Technologies" (JIP-ICET, 2008-2010).

Within the context of the JIP-FP and the Security Research theme of FP 7<sup>8</sup>, the Agency and the EC's Directorate General Enterprise and Industry (DG ENTR) have developed an approach for better mutual harmonisation and synchronisation of research investments and activities in the Software Defined Radio (SDR) domain.

The initiative dates back to 2006, when the EDA and the DG ENTR both contracted SDR studies and identified the need for close coordination to prevent duplication and diverging requirements that might jeopardize the European position in international standardisation, in particular. Since then, more than €34 million have been invested in dual-use SDR technology research, and more than €100 million in subsequent development work (see Figure 6).

Figure 6: The EDA-DG ENTR SDR cooperation.



The approach taken also allowed the EDA to secure use rights for all contributing Members of the JIP-FP, while leaving the IPR ownership with the research performers, in full compliance with the specific rules of the FP7 and of the JIP-FP.

<sup>8</sup> Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013).

The European Space Agency, the European Commission and the European Defence Agency joined forces in 2008 to address in a collaborative effort the issue of critical space technologies for European non-dependence, an area in which uncoordinated public investment would have severe negative impacts. The work resulted in a common strategic agenda with separate but coordinated technology investments, thereby strengthening the European technological and industrial base in the domain.

With the launch of the European Framework Cooperation (EFC) in November 2009, the EDA Ministerial Steering Board expressed its political will to systematically ensure that technology investment by the EDA, the EC and the European Space Agency are synchronised. This is imperative to making best use of the limited resources available for R&T, to avoid the duplication of effort and to increase civil-military standardisation and interoperability. The first identified areas of common interest are CBRN protection<sup>9</sup> and the air traffic insertion of Unmanned Aircraft Systems (UAS), key assets for both civil border security and military capabilities<sup>10</sup>.

## DEFENCE AND SECURITY RESEARCH IN THE FUTURE

Prior to the establishment of the EDA, the relationship between defence and security research at a European level could be best characterised by "coexistence". Since going into operation, the EDA has worked towards better coherence between defence and security research, with the first tangible results achieved in collaboration with the Commission, and later with the European Space Agency, as well.

The EFC is a key step in the direction of systematically yielding synergies that greater coherence of investments can bring in the improvement of capabilities. The cooperation between the European institutional actors in defence and security research is of utmost importance in a world of budgets under increasing pressure and with national and European developments that require good coordination to ensure the effectiveness of public expenditure.

In the 2006, the EC was the ninth biggest investor<sup>11</sup> in "dual use" technologies (see Figure 7). In the 2009, the EDA and the Commission ranked sixth and seventh, respectively, contracting more R&T work than the 21 pMS. In 2013, the Commission will likely be number three, outperforming all EDA participating Member States, save for the top two investors. These figures and projections do not reflect today's situation with defence budgets under severe pressure.

<sup>9</sup> Chemical, Biological, Radiological and Nuclear protection.

<sup>10</sup> E.g. maritime surveillance, border security, asset, infrastructure and environment monitoring.

<sup>11</sup> Security research only; aeronautics and space research not considered, even though these are domains with a high dual-use potential.

Figure 7: Development of "dual use" R&T spent (The figures are based on the assumption that the actual planning of defence and security research budgets remains valid and that the technical scope of the projects in defence research and civilian security research continues to follow current trends. No. 1 is the actor with the highest commitment appropriations for a particular year.)

YEAR	NO. 1	NO. 2	NO. 3	NO. 4	NO. 5	NO. 6	NO. 7	NO. 8	NO. 9
2006	pMS	pMS	pMS	pMS	pMS	pMS	pMS	pMS	EC
2007	pMS	pMS	pMS	pMS	pMS	pMS	EC	EDA	pMS
2008	pMS	pMS	pMS	pMS	pMS	pMS	EDA	EC	pMS
2009	pMS	pMS	pMS	pMS	pMS	EDA	EC	pMS	pMS
2013	pMS	pMS	EC	pMS	pMS/ EDA	pMS/ EDA	pMS/ EDA	pMS	pMS

pMS: EDA Member State EC: European Commission EDA: EDA Cat. A+B+op. Budget

Under the Lisbon Treaty, the EDA's role in defence research is set to increase<sup>12</sup>. The TEU tasks the EDA to:

- Support defence technology research, and coordinate and plan joint research activities and the study of technical solutions meeting future operational needs.
- Contribute to identifying and, if necessary, implementing any useful measure for strengthening the industrial and technological base of the defence sector and for improving the effectiveness of military expenditure.

The Lisbon Treaty also paves the way for considering defence research at the Union level<sup>13</sup>. This would require defence research to converge with the other Union research, notably with security-related research. Looking ahead to the next research framework programme, a political debate of all stakeholders is needed. The European Defence Agency stands ready to take part this debate.

<sup>12</sup> See Article 45 (1) of the Treaty on European Union (TEU).

<sup>13</sup> See Article 179 (1) and (3) of the Treaty on the Functioning of the EU (TFEU).

# > AN OVERVIEW OF SWISS RESEARCH ON VULNERABILITY OF CRITICAL INFRASTRUCTURE

WOLFGANG KRÖGER

## 1 GENERAL SETTING

Throughout history, mankind has developed technologies and integrated them into systems to be deployed for human welfare and security – albeit at the price of becoming dependent on these very same technologies and systems. In recent decades these systems have grown into a large-scale array of interconnected networks that span large distances and are, for the most part, privately owned or operated. These so-called infrastructures function collaboratively and synergistically to produce and/or distribute a continuous flow of goods and services. Infrastructures so vital to a country that their incapacity or destruction would have a debilitating impact on the health, safety, security, economy and social well being of the country, including the effective functioning the government<sup>1</sup>, are labelled critical. The failure of only a single infrastructure or an interruption of its service can inflict significant damage on a society and its economy. However, cross-boundary cascading bears the potential for multi-infrastructural collapse with unprecedented consequences.

Protecting such infrastructures is nothing new to Switzerland: Within their respective remits, a large number of bodies have long been engaged in the protection of important assets and facilities. Yet, both overall coordination and a uniform set of procedures are lacking on a national level.

In a move to ensure collaboration between the involved entities, the federal council in July 2005 mandated the Federal Office for Civil Protection (FOCP) with the coordination of all activities for the protection of critical infrastructures on national level. Subsequently, the FOCP created a working group of 24 members from all seven ministries, as well as the Federal Chancellery. Currently, representatives of the cantons and the private sector also are also involved. Work in the program for the protection of critical infrastructures (PCI) focuses on developing a national PCI strategy by the end of 2011 (for further details visit: [www.bevoelkerungsschutz.admin.ch](http://www.bevoelkerungsschutz.admin.ch)). Research projects have been contracted to assist the FOCP in defining a national strategy for critical infrastructure protection.

---

<sup>1</sup> Definition refers to PCCIP 1997 and EC 2004 but was slightly modified by the author.

## 2 SYSTEM CHARACTERISTICS AND LESSONS LEARNED FROM TRANSPIRED EVENTS

Critical infrastructures (CIs) vary by their nature (e.g. physically engineered, cybernetic or organizational systems), environment (geographical or natural) and operational context (e.g. political/legal/institutional or economic). This contribution to the book will focus on examples of engineered, physically networked CIs, often called lifeline systems. Examples are CIs for the provision of:

- Energy (electricity, oil and gas)
- Transportation (rail, road, air, sea)
- Drinking water, including waste water treatment
- Information and telecommunication (e.g. internet)

To varying degrees, all but the last rely on information and communication technology (ICT) for data acquisition and industrial control (SCADA).

These critical infrastructures are subject to a wide array of hazards and potentially asymmetrical threats (technical-human, natural, physical, cyber or contextual; either unintentional or malicious) that exploit weakness and vulnerabilities, respectively. Furthermore CIs may pose their own risks during normal operation (e.g. electromagnetic fields (EMF)) or accidents (e.g. rupture of gas pipelines). Most critical infrastructures have dynamic structures. They are subject to extensive change, both technological and organisational, and incorporate technologies soon after they become (commercially) available. These CIs share neither a common owner/operator/regulator nor a common base of logic.

Experience from transpired events shows that "critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host technology"<sup>2</sup>. Identifying, understanding and analyzing these features poses a major challenge – a challenge that is amplified by the scope and complexity of most infrastructures.

CIs have proved highly reliable in and beneficial to Western societies. Nevertheless, major breakdowns have occurred and illustrate the complexity of the event sequences they can trigger. In *electrical transmission* CIs, for example, an analysis of recent *major blackouts* from 2003 to 2006 (**Table 1**) brings to light a number of common behaviour patterns:

- Technical failures (Denmark/Sweden: Two independent failures), external impacts (Tokyo, construction work; Brazil, extreme weather conditions) and adverse behaviour of protective devices (London) are important triggering events in systems not protected by the N-1 security criterion<sup>3</sup> and/or in combination with high load conditions (Moscow).

<sup>2</sup> Rinaldi et al. 2001.

<sup>3</sup> The N-1 security criterion specifies, "any probable single event leading to a loss of a power system element should not endanger the security of the interconnected operation, that is, trigger a cascade of trippings or the loss of a significant amount of consumption" ([www.ucte.org](http://www.ucte.org), visited 08).

- Organisational factors, such as market liberalization and short term contracting, which lead to systems operating beyond their original design parameters (e.g. Great Lakes and Italy), and strained operating conditions stemming from reduced maintenance and/or inadequate integration of intermittent power generation (e.g. Western Europe) are prime causes of breakdowns.
- Since transmission system operators (TSO) play a decisive role in contingency management, the lack of situational awareness and short-term preparedness, as well as limited real time monitoring outside of control areas and poor, non-expedient cross-border coordination (e.g. Great Lakes, Italy and Switzerland (rail)) represent aggravating factors.
- The inadequacy of the N-1 security criterion and, more importantly, its evaluation/implementation in a variety of cases has bolstered the argument for making the criterion more stringent and legally binding.

Also, a lack of investment brought on by increased economic pressure, public resistance, etc. can be observed in many countries and areas. The result is insufficient system monitoring, control and automation, grid extension and maintenance (including tree cutting programs (Great Lakes, Switzerland/Italy)), all of which have contributed significantly to blackouts in the past.

This evaluation clearly indicates that, even for individual infrastructures like electrical transmission grids, classical approaches to system modelling and preventive risk analysis are no longer adequate. This pertains to quasi-static logic trees, as well as the neglect of contextual factors.

The importance of (inter-)dependencies is exemplified by experience from actual incidents. Rinaldi, Peerenboom and Kelly<sup>4</sup> define *dependency* as a unidirectional relationship between two infrastructures: Infrastructure *i* depends on *j* through a link, but *j* does not depend on *i* through the same link. *Interdependency*, in contrast, is defined as a bidirectional relationship: Infrastructure *i* depends on *j* through a number of links, and *j* likewise depends on *i* through the same and/or other links.

Details of the mini *telecommunication* blackout in Rome, Tor Pagnotta Street, at 5.30 a.m. on January 2, 2004 demonstrate the challenges in interdependency analysis:<sup>5</sup>

A Telecom Italia major telecommunication service node was flooded after a metallic pipe carrying cooling water for the air conditioning plant burst. The flooding led to the failure of several boards and devices through short circuits and main power supply failure. Diesel generators, part of the emergency power supply, did not start because of the water; only batteries, which ultimately fell out, powered the functioning boards and devices.

---

<sup>4</sup> Rinaldi et al. 2001.

<sup>5</sup> Ciancamerla & Minichino 2006.

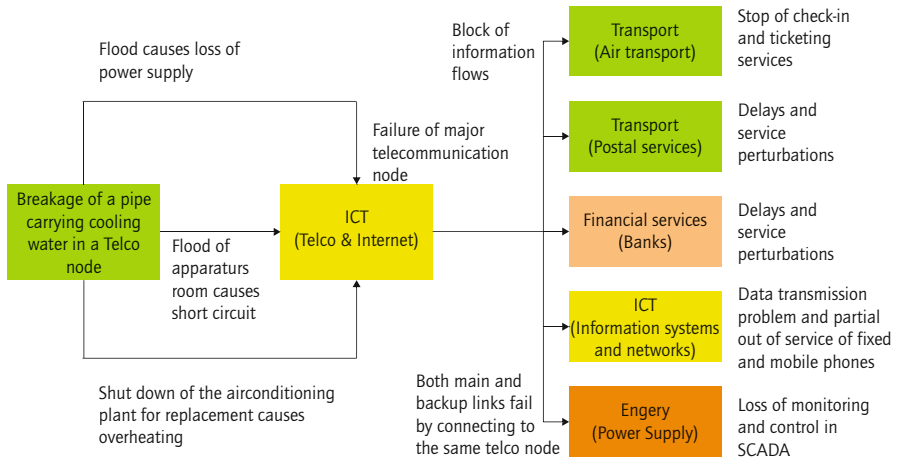
The fire brigade arrived at 7.30 a.m., started pumping out water and finally located the break in the pipe. To initiate the repairs the technicians had to shut down the air conditioning plant. The mini blackout caused problems and delays in various infrastructures, including Fiumicino Airport, ANSI print agency, post offices and banks, ACEA power distribution and the communication network (both fixed-to-fixed and fixed-to-mobile) connecting the main Italian research institutions (see Fig.1) for affected infrastructures).

Table 1: Recent major blackouts of electric power supply systems

BLACKOUT		LOAD LOSS [GW]	DURATI-ON [h]	PEOPLE AFFECTED	MAIN CAUSES
Aug. 14, 2003	Great Lakes, NYC	~60	~16	50 Mio	Inadequate right-of-way maintenance, EMS failure, poor coordination among neighboring TSOs
Aug. 28, 2003	London	0,72	1	500,000	Incorrect line protection device setting
Sept. 23, 2003	Denmark/Sweden	6,4	~7	4,2 Mio	Two independent component failures (not covered by N-1 rule)
Sept. 28, 2003	Italy	~30	up to 18	56 Mio	High load flow CH-I, line flashovers, poor coordination among neighboring TSOs
July 12, 2004	Athens	~9	~3	5 Mio	Voltage collapse
May 25, 2005	Moscow	2,5	~4	4 Mio	Transformer fire, high demand leading to overload conditions
June 22, 2005	Switzerland (railway supply)	0,2	~3	200.000 passengers	Non-fulfillment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing
August 14, 2006	Tokyo	?	~5	0.8 Mio households	Damage of a main line due to construction work
Nov. 4, 2006	Western Europe ("controlled" line cut off)	~14	~2	15 Mio households	High load flow D-NL, violation of the N-1 rule, poor inter TSO - coordination
Nov. 10, 2009	Brazil, Paraguay	~14	~4	60 Mio	Short circuit on key power line due to bad weather, Itaipu hydrostation (18 GW) shut down



Figure 1: Infrastructures affected by the mini telecommunication blackout in Rome, January 2004



### 3 INTERDEPENDENCIES AND COMPLEXITY

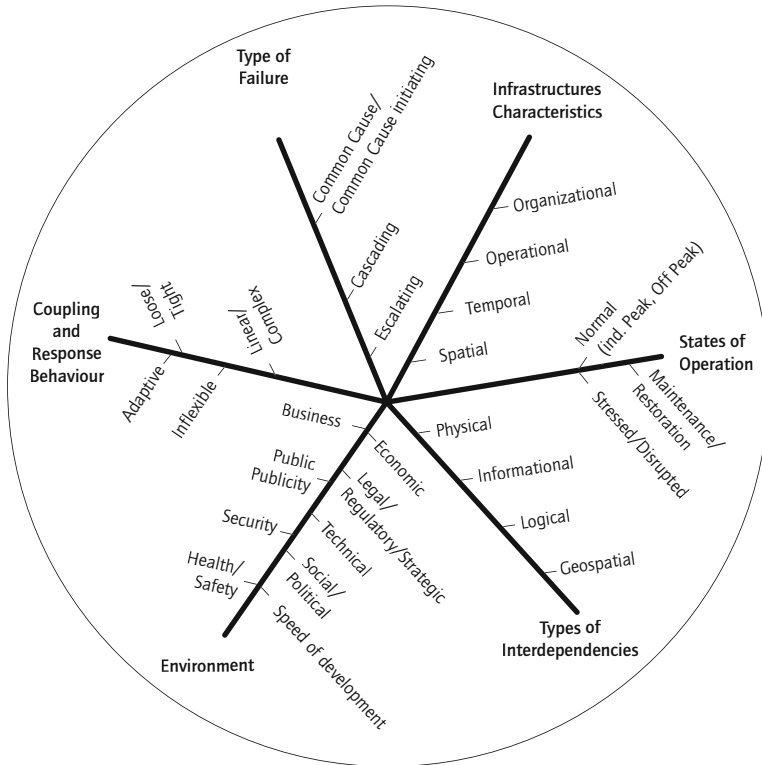
As clearly demonstrated by events experienced, interdependencies are more than just a (fairly) new theoretical concept: They bear significant practical relevance. Rinaldi, Parenboom and Kelly<sup>6</sup> introduced six dimensions for their description and a categorization into four general "types of interdependencies". Although these still seem appropriate for facilitating the identification, understanding and analysis of interdependencies, and for framing requirements in modelling and simulation approaches, the author has modified them slightly (see Fig. 2). The four types distinguish between:

- Physical interdependencies: The state of each depends on the material output(s)/ flows(s) of the other, e.g., a pipeline network provides gas to fuel a gas-fired power station while the electricity generated is used to power compressors and controls the gas supply network.
- Geospatial interdependencies: Elements are in close spatial proximity and a local environmental event, e.g. an earthquake, affects components across multiple infrastructures.
- Informational interdependencies: Infrastructures connected to one another via electronic informational links, e.g. a SCADA system that monitors and controls elements of the electric power grid, and those that provide information to support other infrastructures.

<sup>6</sup> Rinaldi et al. 2001.

- Logical interdependencies: These exist between infrastructures that do not fall into one of the categories above and include interdependencies that lack diversity, functional interdependencies, etc.

Figure 2: Dimensions for describing infrastructure interdependencies



Failures (negative impact) that arise from interdependencies may be classified as follows:

- One event causes failure or loss of service in more than one infrastructure, e.g. areal external events, due to spatial proximity (referred to as common cause initiating events)
- Failure of one infrastructure causes the failure or loss of service in at least one other infrastructure, e.g. rupture of mains in the water supply system (referred to as cascade initiating events)

- Failure or loss of service resulting from an event in another infrastructure, e.g. failure of gas lines resulting from a loss of the main electricity supply to compressors (referred to as cascade resulting events)
- Failure or loss of service in one infrastructure escalates because of failure in another affected infrastructure, e.g. failure of the electric power system resulting in failure of the SCADA system, which, in turn, affects restoration of the electric power system (referred to as *escalating events*)

As indicated above, most infrastructures have a high degree of degree of complexity that stems not only from interdependencies. **Table 2** highlights the very essence of complex systems in contrast to complicated systems. As interactions between the parts are mostly essential, with overall behaviour emerging from these interactions, systems must be analyzed as a whole. "Decomposing the system and analyzing subsystems does not necessarily give a clue as to the behaviour of the whole."<sup>7</sup>

Table 2: Traits of complicated and complex systems, both entailing a large number of highly connected components

COMPLICATED SYSTEMS (MECHANICAL WATCHES, AIRCRAFT, POWER PLANTS, ETC.)	COMPLEX SYSTEMS (STOCK MARKET, WWW, POWER GRID, ETC.)
Components have well-defined roles and are governed by prescribed interactions.	Rules of interaction between the components may change over time and may not be well understood.
Structure remains stable over the time. Low dynamics.	Connectivity of the components may be quite plastic and roles may be fluid. Interactions are not always obvious.
No adaption. One key defect may bring system to a halt.	System responds to external conditions and evolves.
Limited range of responses to changes in their environment.	Display organization without a central organizing principle (self-organization/emergence).
Decomposing the system and analyzing sub-parts can give us an understanding of the behavior of the whole, i.e. the whole can be reassembled from its parts.	Respond to and interact with their environment.
Problems can be solved through analytical thinking and diligence work.	Inadequate information about the state of the influencing variables, nonlinearities.
	Overall behavior cannot be simplified in terms of their building blocks. The whole is much more than the sum of its parts.

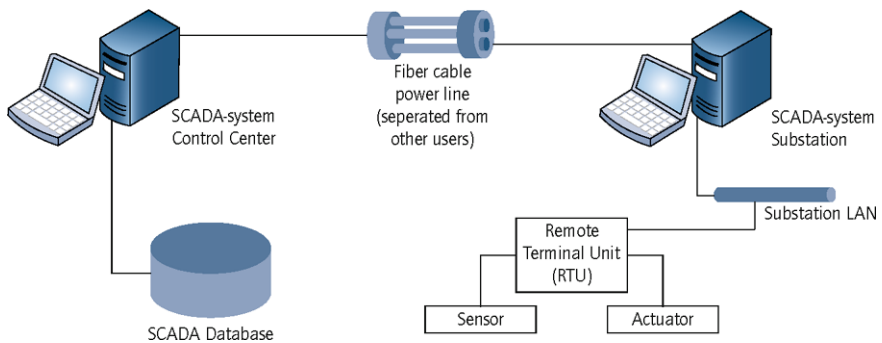
<sup>7</sup> Guckenheimer & Ottino 2008.

Observable trends may lead to even greater system integration and complexity. This is not negative for system performance and robustness per se. Most prominently, the pervasive use of information and communication technology (ICT) and its integration into transmission/distribution networks leads to "system-of-systems" that:

- Make large integrated systems operable
- Control devices and collect data (SCADA)
- Monitor and make decisions on real-time basis
- Increase exchange of data among the parties involved
- Prevent breakdowns and cascading failures

However, the benefits reaped from replacing the formerly dedicated systems come at the price of new risks, e.g. the susceptibility to cyber attacks and the increased potential for common cause failures. Thus, "systems under control" and "industrial control systems" (SCADA) must be understood in detail and analyzed with regard to vulnerabilities, i.e. entry points for outside hackers. **Fig. 3** outlines the SCADA system of a Swiss regional transmission operator. Its robustness would be significantly reduced if, for example, the internet were used for data and command transmission or business (trading) systems and control systems were merged.

Figure 3: SCADA System for a Swiss bulk electricity transmission



- 1) Dedicated data exchange between utilities and Swiss TSO (PIA system)
- 2) Trading/office systems separated from SCADA
- 3) Own control systems - can be operated via own telephone lines; protective systems/devices independent from SCADA

#### 4 MODELLING APPROACHES

Research is aimed at developing advanced methods and techniques to model and simulate complex infrastructures and the interactions between them at a single system level (the system-of-systems level). Systems dynamics often result from relatively slow initial system degradations that escalate into an avalanche of component failures.<sup>8</sup> The application of such advanced methods, together with a good understanding of the systems involved, will allow system vulnerability indicators to be quantified and critical elements to be identified. A number of approaches to CI vulnerability assessment are conceivable, depending on system type and potential interactions, objectives of the analysis, and available information. However, the complex behaviour of systems renders questionable the suitability of "classical" methods for reliability and risk analysis, e.g. logic trees, including deduction mechanisms and predefined causal chains. Although simulation techniques can be used as "scenario generators", the computational cost for real-sized systems may be excessive.

In practice, there is no "silver bullet solution" to the problem of analyzing the risks associated with critical infrastructures. Instead, an analysis framework seems necessary to effectively integrate the different methods into a problem-driven solution approach. Based on a survey of the literature and the author's experience in the electric power sector<sup>9</sup>, topology-driven analysis of vulnerabilities can provide essential details for a kind of screening analysis aimed at identifying system connection patterns, shortest connection paths, local and global specifics, etc. The techniques used typically build on *network theory*<sup>10</sup>. In this view, the power transmission infrastructure may be represented as a network of  $N$  nodes (here substations) interconnected by  $K$  links (here overhead lines). Mathematically, this defines a graph  $G(N,K)$  whose connections are defined in an  $N \times N$  adjacency matrix  $\{a_{ij}\}$  with entries equal to 1 if there is an edge joining nodes  $i$  and  $j$  and 0, otherwise. Each link between two nodes is of unit length so that the distance between two nodes is represented solely by the number of edges traversed in the path from  $i$  to  $j$ . In addition to the shortest path and distribution lengths, further insights on the connectivity properties of a network are given by its degree distribution,  $P(k)$ , i.e. the distribution of the number of substations  $k$  connected to an arbitrary substation. Network architectures follow one of two degree distributions, either Poisson, or power law, resulting in a random graph or scale-free network. The power transmission infrastructure that has evolved over decades has a random graph structure, making it more susceptible to random failures than to targeted attacks (see Fig. 4).

The object-oriented approach to modelling and simulation of critical infrastructures is highly promising for in-depth analysis. It allows the incorporation of physical laws into simulations and emulation of infrastructure behaviour emanating from the behaviour of

<sup>8</sup> Eusgeld & Dietz 2010.

<sup>9</sup> See Eusgeld et al. 2009 for details.

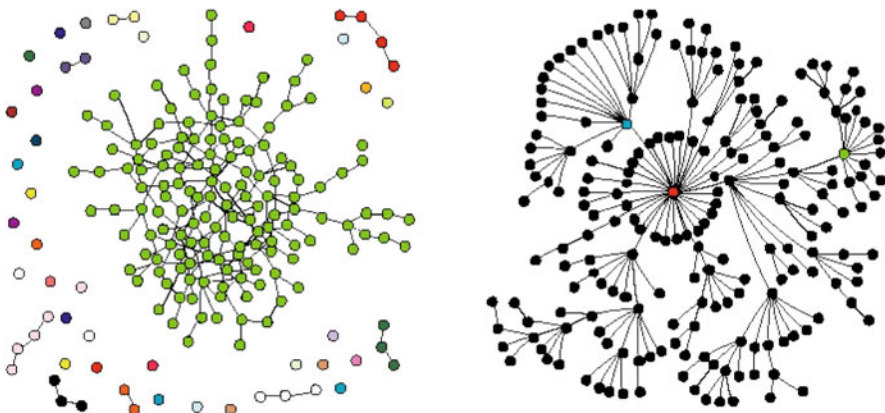
<sup>10</sup> See e.g. Barabasi 2002.

individual objects and their interactions. In other words, overall system behaviour results from interactions between multiple individual objects that make up the system. A two-layer object-oriented modelling approach has been proposed to integrate stochastic, time-dependent technical and non-technical factors into the vulnerability assessment of the electric power system<sup>11</sup>. Objects are used to model both technical components such as generators, and non-technical components such as grid operators. The objects interact with each other directly (e.g. generator dispatch) or indirectly (e.g. via the physical network). In the two-layer concept (Fig. 5), the lower layer represents the separate modelling of the physical components by means of conventional, deterministic techniques such as power flow calculations, whereas the upper layer represents the abstraction of the electric power system with all components represented by individual objects. Some simulation results regarding the complementary cumulative blackout frequency, FC (CE), versus event size CE are depicted in Fig. 6. The curves are exponential as long as the initial loads do not exceed 110%, but changes to a power-law shape for higher loads. This shows the sensitivity to initial stress conditions and confirms statistical investigations.

Interestingly, findings from a network theory analysis of the system structure do not match those from a detailed, in-depth model of the system's physical behaviour using object-oriented methods. This suggests that additional investigations must be carried out to identify appropriate static indicators of the system's physical behaviour that can be used as representative weights of the connections in the network structure<sup>12</sup>.

Figure 4: Network architectures for typical degree distributions [Strogatz, 01]

Left: random graph (Poisson), right: scale-free (power law). Topological studies indicate that random graph networks are susceptible to random failures and scale-free networks to targeted attacks



<sup>11</sup> Schläpfer et al. 2008.

<sup>12</sup> Eusgeld et al. 2009.

Figure 5: Two-layers concept applied to the electric power system [Schläpfer et al., 2008]

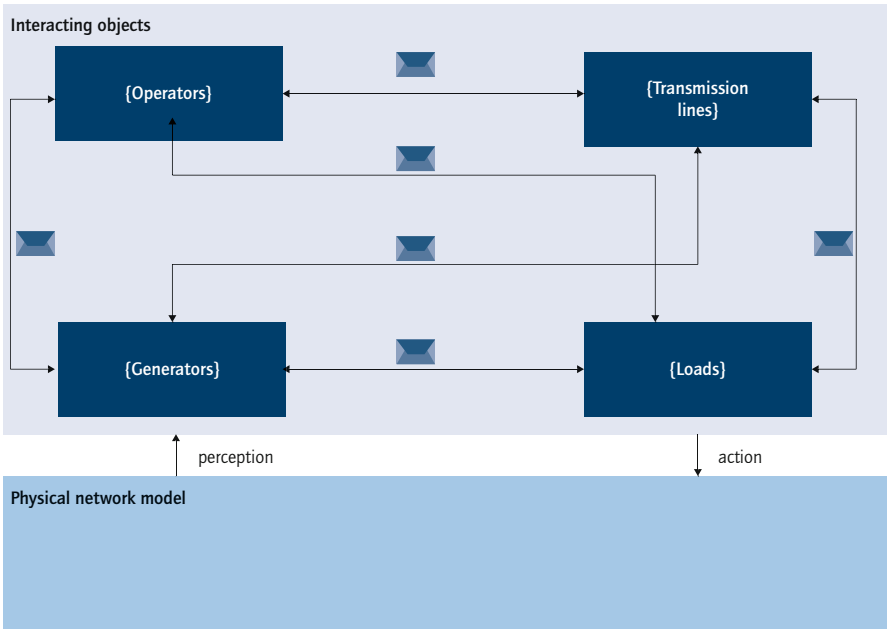
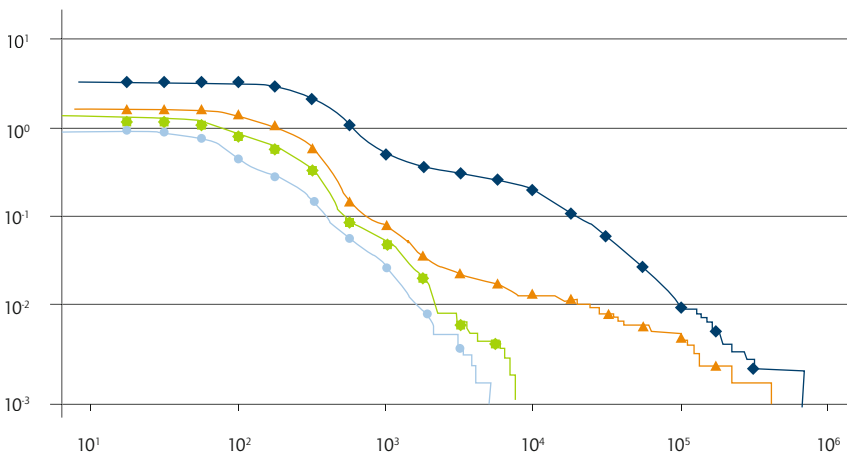


Figure 6: Sensitivity of complementary cumulative blackout frequencies and event size to increased grid loads [Schläpfer et al., 2008]



## 5 CONCLUSIONS

Vulnerability assessment of infrastructure systems vital to our society is an important and challenging subject that necessitates inter alia a thorough understanding of system (inter-) dependencies. Empirical investigations are useful in this context, but taken alone, they are insufficient, while the capabilities of "classical" methods in reliability and risk analysis have been clearly outgrown. Thus, more advanced modelling and simulation techniques must be applied and/or further developed to facilitate vulnerability analyses of such complex systems. The Swiss CIP program encompasses research that ultimately also supports strategy development. Results based on a model of the Swiss high-voltage transmission grid demonstrate the potential of network theory in identifying structural/topological criticalities while the potential of object-oriented modelling lies in the detailed description of dynamic infrastructure behaviour. The results confirm the applicability of these methods, but also their limitations, which call for further refinements.

## REFERENCES

### Rinaldi et.al. 2001

Rinaldi, Steven M./Peerenboom, James P./Kelly, Terrence K.: "Critical Infrastructure Interdependencies", IEEE Control Systems Magazine 21, 2001.

### Guckenheimer & Ottino 2008

Guckenheimer, John/Ottino, Julio M.: "Foundation for Complex Systems Research in the Physical Sciences and Engineering", report from an NSF workshop, Sept. 2008.

### Eusgeld & Dietz 2010

Eusgeld, Irene/Dietz, Sven: "System of systems", approach for interdependent critical infrastructures; Reliability, Risk and Safety: Theory and Applications, Briš, Guedes, Soares & Martorell (eds), Taylor & Francis Group, London, 2010.

### Barabasi 2002

Barabasi, Albert Laszlo: "Linked: the new science of networks", Cambridge, MA: Perseus Publishing; 2002.

### Schläpfer et. al. 2008

Schläpfer, Markus/Kessler, Tom/Kröger, Wolfgang: "Reliability analysis of electric power systems using an object-oriented hybrid modeling approach", in: Proceedings of the 16th power systems computation conference, Glasgow, 2008.



**Eusgeld et. al. 2009**

Eusgeld, Irene/Kröger, Wolfgang/Sansavini, Giovanni/Schläpfer, Markus/Zio, Enrico: "The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures", in: journal: Reliability Engineering & Systems Safety, Elsevier, Vol. 94, No 5, pp. 954-963, 2009.

**Strogatz 2001**

Strogatz, Steven H.: "Exploring complex networks", Nature 410, 268-276, 8 March 2001.

**Ciancamerla/Minichino 2006**

Ciancamerla, E./Minichino, M.: Deliverable D2.2.2, "Tools and techniques for interdependency analysis", Integrated Project IRRIS Integrated Risk Reduction of Information-based Infrastructure Systems, July 2006.

**PCCIP 1997**

Critical Foundations: "Protecting America's Infrastructures", Report of the President's Commission on Critical Infrastructure Protection, Washington D.C., 1997.

**EC 2004**

EU Document, 702 final concerning: "Critical Infrastructure Protection in the fight against terrorism", COM, 2004.

# > SECURITY RESEARCH AND SAFETY ASPECTS IN SLOVAKIA

JURAJ SINAY

## 1 INTRODUCTION

In 2004 the Slovak Republic joined the European Community. This accession called for changes in the new member state's internal and external processes, as well as the acceptance of the European Community regulatory framework and its implementation in Slovakian national legislation. Even though Slovakia had started with step-by-step integration of specific regulations during accession negotiations, final implementation was only concluded upon admission into the European Community. The process spanned the fields of occupational health and safety (Safety) and civil security (Security), notwithstanding that professionals in these areas had already been working in line with the European legislation.

However, full acceptance of the new legislation also implied a transformation in the fundamental mindset of the Slovakian society as a whole, especially with regard to areas like Security and Safety that have a direct effect on individual citizens. Raising the level of awareness for changes in the basic conditions of everyday life is a lifelong learning process – it takes time and requires regular training with subsequent testing to determine the degree to which safety habits have indeed been adopted.

Slovakia has always placed great value on encouraging accident prevention through modern legislation. As such, the prerequisites for accepting European legislation pertaining to safety and health were largely given by a culture of safety already in place and actively exercised by all social players, i.e. employees, employers and government institutions.

Slovakia provides an entry gate into the European Union along its border with the Ukraine. Even though the border is relatively short, it does open opportunities for migration from a number of countries. With the accession of Slovakia, the border to the Ukraine became a part of the Schengen Zone border. Consequently, security standards need to be observed in this area to ensure strictly monitored cross-border traffic.

Both oil and gas pipelines that supply the European Union cross the Slovak-Ukraine border, making it highly relevant with regard to energy security, a sub-domain of civil security. Thus, from a civil security point of view Slovakia is a strategically significant country.

Figure 1: Geopolitical location of the Slovak Republic



## 1 SAFETY VERSUS SECURITY

### > 1.1 Safety

The word 'safety' ('safe') stems from the Old French *sauf* and means 'uninjured'. In our context it refers to a safe state in which hazards in human-machine-environment systems are minimised, with particular emphasis on human safety.

Safety is the manifestation of a chain of measures, including their embodiments and their interactions, that leads to the minimisation of physical, social, financial, mechanical, chemical, psychological and other types of threats (risks that represent the potential of threats). It results from the creation of systems for averting the risk of injury or death, and material damage.

A classic example is aircraft safety, which comprises measures for eliminating or at least minimising risks from, e.g. pilot error or equipment failure, both in the aircraft and in supporting ground systems. An obvious safety measure is the application of redundant systems in aircraft control systems.

## > 1.2 Security

Security refers to a system of measures, including their embodiments and their interactions, designed to ward off intentionally destructive activity resulting in injury or material damage. Although humans are the prime initiators of security threats, environmental security threats stem largely from processes beyond human control (e.g. natural disasters like earthquakes, floods, volcanic eruptions, etc.) and ultimately hold the potential for massive human and material damage.

Civil aviation security serves as an excellent example. It comprises activities to protect all aspects of aircraft operations against deliberate destructive activity by humans. Airport security checks of passengers and baggage, for example, are effective security measures in staving off hijack attempts. A recent example of an environmental security threat is the Haiti earthquake.

Effective security management processes must be both proactive and reactive. The primary aim is the prevention of negative phenomena, whether from intentional human activity or from natural disasters. When this first line of defence fails the emphasis immediately shifts to minimising the consequences of the transpired event.

The threats and ensuing consequences that security officials face are frequently cross-border in nature, with organised activity managed and controlled from diverse geographical areas across the globe. Thus, effective security measures are often possible only in closely coordinated transnational collaboration. Slovakia is playing its part to make such efforts possible and to ensure their effective implementation.

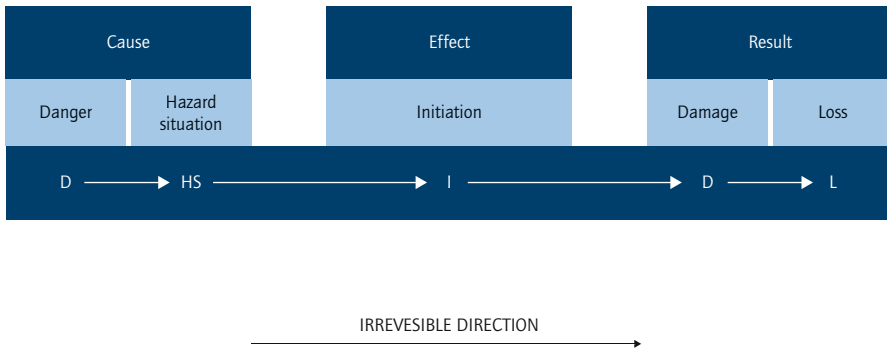
## 2 CAUSAL DEPENDENCY IN THE OCCURRENCE OF NEGATIVE PHENOMENA

Today, the sequences of developments leading to the occurrence of negative phenomena usually show strong causal dependencies that can be explained using causal theory. Figure 2 illustrates the principal of causal dependency originating from danger as a passive component. The hazard situation is causally related to the passive component and can be viewed as an activation of the passive component. For a negative phenomenon to occur, a whole chain of events must take place, from the initiation, i.e. the critical starting point of the destruction process, to the final stages of damage and loss.<sup>1</sup>

It is important to realise that negative phenomena never occur purely by chance. They are always the result of causal dependencies. When causes leading to an effect are not apparent, it is due to a lack of knowledge, not the absence of causality. This lack of knowledge provides the motivation for scientific research in the quest to uncover unknown dependencies, which can then be factored into the implementation of activities in the domains of safety and security.

<sup>1</sup> Causal dependency is described in detail in [Sinay, Nagora 2010], as well as in the follow-up works [Sinay 1998] and [Sinay 1997].

Figure 2: Causal dependency in the occurrence of negative phenomena<sup>2</sup>



Knowledge about causal dependencies in the occurrence of negative phenomena is a prerequisite for developing methodologies for minimising risk (hazard situations) and subsequent damage. Efficient and effective methods involve interrupting causal dependencies in the early stages, i.e. during the danger and activated hazard phases. In practice, intervention at later stages of the causal dependency chain is also possible, albeit at a higher cost and with decreased efficiency in counteracting the consequences of the negative phenomena.

> 2.1 The human component in security and safety analysis

From a safety and security management point of view, the human factor plays a crucial role in the human-machine-environment system. In a safety context, negative phenomena are usually the unintentional result of activities directly or indirectly attributable to human failure. In a security context, on the other hand, there is an intentional aim to generate a causal dependency chain leading to a negative phenomenon with the greatest possible infliction of damage. The notion of a 'dangerous person' is both applicable and appropriate.

When looking at the overlap between safety and security management, it is important to focus on the integral evaluation of the relationship between the human activity factor and fulfilment of the ultimate goal: protecting all components in the human-machine-environment system.

This can be nicely illustrated in a fire-fighting example. The aim of a fire fighter's actions is to minimise the consequences of a fire – clearly a security aim. However, in executing his duties, the fire fighter must be secured to an extent that he is reasonably well protected from injury or death – a safety issue. Neglecting the safety of the fire fighter puts the security of others in peril since the fire fighter can only do his job if he himself remains unharmed.

<sup>2</sup> Sinay, Nagyova 2010.

Safety and security share a common footing in their damage minimising approaches. Both concentrate on pinpointing options and developing methodologies to interrupt causal dependency chains leading to negative phenomena. These approaches must be the subject of scientific research activities by individual states (here mainly in the security domain) and by international research consortia. The relative importance of security research to the European Union is reflected by the high priority it gives to science and research in the field, e.g. 7 RP EU.

### 3 RELATIONSHIP BETWEEN SECURITY AND SAFETY IN CIVIL SECURITY RESEARCH IN SLOVAKIA

The Slovak Republic, as a constituent part of European structures, derives legislative support for security activities from the following national laws:

- Constitution of the Slovak Republic
- Act 129/2002 on Integrated Emergency Systems
- Act 579/2004 on Emergency Medical Services
- Act on the Protection of Critical Infrastructure (pending)

The Ministry of Interior acts as the hub for civil security activities in Slovakia. Civil security training and requisite document publishing is organised at this level for all areas.

A clear deficiency in the Slovakian security apparatus is the lack of an interdepartmental security management system. Such a system would serve to refer research activities to global structures both within the European Union and outside of Europe. Only by integrating research activities will the conditions for defining projects by state institutions become an internal concern of the Slovakian state. These conditions must be fulfilled to effectively collaborate with research entities within the European research landscape. Due to capacity limitations, not all Slovakian research entities will be able to participate in the same degree. It is thus important that Slovakia define the strategic areas in which it can provide both personnel and material support. This is the key motivation for the National Research Infrastructure Map that will become available in 2011 (Version 2010).

In 2005 Slovakia drafted a "Security Strategy" that elaborates a policy to ensure the security of the Slovakian State and its citizens in a stable and foreseeable environment by applying methodologies and measures for civil security. The trend towards globalisation in the Slovakian security strategy is summed up nicely in the following quotation<sup>3</sup>: "Membership of the Slovak republic in the OSCE (Organisation for Security and Cooperation in Europe), NATO and the Organization for Economic Cooperation and Development (OECD), as well as the geopolitical position of the Slovak Republic in Central Europe defines its security policy. Security hazards and challenges are changing. The

---

<sup>3</sup> Security Strategy 2005.

security of the Republic and its citizens is inseparably tied to the security policy of its allies as it faces threats and challenges similar to those of other states in the Euro-Atlantic area." These statements apply to all civil security activities within the Slovak Republic.

A shortcoming of the Security Strategy is that the need for research in the field of security, be it in the Slovakian or the European domain, is nowhere mentioned. There is a lack of emphasis on the issue of globalisation. However, this would be important to raise awareness for a class of risks that have been hitherto unknown, or only marginally relevant, in Slovakia. Ultimately these risks cause a shift the relationship between internal and external security. Both unions and individual states are becoming increasingly dependent on vitally important sources including foodstuffs. This is a key driver for common policy decisions and the implementation of measures for civil security. The main issue for Slovakia in this context is energy supply, in particular for natural gas and oil. Slovakia must ensure the safe and reliable transit of these energy sources to its allies in Europe.

#### 4 THE INTEGRATED EMERGENCY SYSTEM IN SLOVAKIA

The driving force behind drafting and implementing the hitherto non-existent Integrated Emergency System (IES) was Slovakia's membership in various international unions along with a fundamental desire for integration in this area.

IES comprises fire brigades, emergency medical services, the police force and civil defence units, as well as mountain and mine rescue services. The latter two services are somewhat specific to Slovakia and reflect the fact that it is a relatively mountainous state with a high level of mining activity. The basic strategy is geared towards providing well-organised rescue operations in situations where life, health, property or the environment are in peril. It covers all elements in the human-machine-environment system and applies to extraordinary situations, including natural disasters. This system will bolster the security of the state and all elements of society to protect and support the development of human life and the environment as a part of European and worldwide structures. IES reacts only after the onset of negative phenomena – it is only marginally concerned with prevention issues. The system is set up for the following events in Slovakia:

- Natural disasters (floods, earthquakes, avalanches)
- Large-scale industrial disasters
- Major traffic accidents
- Aircraft accidents, nuclear accidents
- Fires
- Epidemics and pandemics
- Migration
- Terrorist attacks.

The following bodies of the Slovakian government are responsible for drafting concepts, carrying out analyses and making proposals for legal regulation in a civil security context:

- Ministry of the Interior
- Ministry of Defence

Specific areas of society are covered by other government bodies:

- Ministry of the Environment – Floods and industrial disasters
- Office of Nuclear Control – Field of nuclear energy
- Ministry of Agriculture – Economic mobilisation
- Ministry of Health – Health protection

## 5 EXAMPLES OF PARTICIPATION BY SLOVAKIAN RESEARCH ENTITIES IN GLOBAL CIVIL SECURITY ACTION PLANS

As members of European consortia, a number of Slovakian research entities currently participate in the development of solutions in the field of security. These include the Slovak Academy of Sciences (SAS), Slovenská Akadémia Vied (SAV) and various universities.

The SECRIKOM (Seamless Communication for Crisis Management) project focusses on information and communication technology and deals with strategies for minimising problems in the crisis communication infrastructure. A key element is the development of new intelligent functions to enhance the effectiveness of communication for users of the system. The project, run by the Institute of Informatics at SAS, will implement security “mediators” (security agents).

SAS also runs the EUSAS (European Urban Simulation for Asymmetric Scenarios) project for developing new approaches to mission analysis and training of units in their preventive function in urban environments. The emphasis lies on human behaviour modelling with the aim of creating a virtual reality environment adequate for training purposes. The SAS is developing a framework and tools for intelligent data analysis to link the various behaviour models.

The faculty of Electrical Engineering at the Technical University of Košice runs the INDECT (Intelligent Information System Supporting Searching and Detection for Security of Citizens in Urban Environment) project, which targets the development of a platform for operational data registration and exchange, multimedia content acquisition, intelligent data processing and automatic threat detection, as well as the development of tools for dangerous and violent behaviour recognition. Staff of the Multimedia Department is developing a new type of scanner that combines direct scanning of images and videos stored as digital watermarks.



University workplaces handle some of the ad hoc projects from the security field, but unfortunately not in the context of systematic projects with financial support from the central Slovakian budget sources. Active university workplaces include:

- Žilina University – Object-oriented safety projects
- Technical University in Zvolen – Fire safety focusing on security, safety and health interfaces
- Technical University of Košice – Application of risk analysis methods to safety and security conditions, integrated safety of pipeline constructions (gas and oil), nuclear power plant safety, design support for road tunnel rescue systems
- Slovak Technical University in Bratislava – Mainly fire safety
- Slovak Police Academy in Bratislava – Civil safety

## 6 SUMMARY

As one of the youngest members of the European Union and NATO, the Slovak Republic has quickly and successfully integrated into international structures, thereby becoming a constituent part of the complex security management apparatus that ensures global civil security. It has gradually assumed obligations arising from its membership in the EU and NATO, adopted required legislation and created conditions conducive to the development of a security culture in everyday life in the Slovakian society. With a long-standing tradition of research and innovation in the field of occupational safety and health, the development and application of verified risk analysis procedures in a security context comes naturally. Even though Slovakia, as a part of the international community, takes an active part in European research teams, the absence of a systematic approach to research projects in strategic action plans is seen as shortcoming. This poses a challenge for all players in the field of safety and security research to create a system that encompasses the strategic tasks in science, research and innovation.

This article was written in the context of VEGA project number 1/0240/09 "Výskum metód integrovaných systémov riadenia rizík technických zariadení a priemyselných technológií".

## 7 REFERENCES

### Security Strategy 2005

Bezpečnostná stratégia Slovenskej republiky (Slovensky)/Security Strategy of the Slovak republic (Slovak. Národná rada Slovenskej repubiky, 27. September 2005 National Parliament of the Slovak Republic 27. September 2005

**Sinay 1997**

Sinay, J.a kol.: Riziká technických zariadení – manažérstvo rizika (slovensky). Risks of technical facilities (Slovak). OTA Košice, 1997 also on CD, 40% ISBN 80-967783-0-7

**Sinay 1998**

Sinay, J.: Risk assessment and Safety Management in Industry. Chapter V – Karwowski,W., Maras,W.S.: The occupational ergonomics handbook, CRC Press LLC, Boca Raton, Florida, 1998, ISBN 0-8493-2641-9

**Sinay, Nagyova 2010**

Sinay, J., Nagyova,A.:Causal relation of negative event occurrence – injury and/or Failure. Conference "AHFE 2010", Miami, USA 15.-18. July 2010

## > ENGINEERING INFRASTRUCTURES: PROBLEMS OF SAFETY AND SECURITY IN THE RUSSIAN FEDERATION

NIKOLAY A. MAKHUTOV/DMITRY O. REZNIKOV/VITALY P. PETROV

Modern society cannot exist without stable and reliable engineering infrastructures (EI), whose operation is vital for any national economy. These infrastructures include energy, transportation, water and gas supply systems, telecommunication and cyber systems, etc. Their performance is commensurate with storing and processing huge amounts of information, energy and hazardous substances. Ageing infrastructures are deteriorating – with operating conditions declining from normal to emergency and catastrophic. The complexity of engineering infrastructures and their interdependence with other technical systems makes them vulnerable to emergency situations triggered by natural and manmade catastrophes or terrorist attacks.

Specialists from many countries have worked to successfully create a broad scientific base for analysing safety related problems in engineering infrastructures. These problems include assessing extreme situations triggered by natural and manmade disasters, studying scenarios in which these phenomena might originate and develop, and reducing the vulnerability of engineering infrastructures to natural and manmade disasters.

### SAFETY RELATED PROBLEMS FOR ENGINEERING INFRASTRUCTURES

The failure to ensure the basic characteristics of strength, reliability, resilience and robustness with regard to a range of criteria will result in the increased probability of accidents and catastrophic situations surfacing and developing at all stages in the life cycle of engineering infrastructures. Over the past decade, institutes of the Russian Academy of Sciences, the Russian Ministry of Emergency Situations, the Russian Ministry of Education and Science, have compiled a sizable volume of fundamental information on industrial and natural accidents and catastrophes as part of the State Scientific-Technical Program for *Safety for the Population and Economic Objects Considering the Risk of Natural and Manmade Disasters* ("SSTP Safety"). These efforts were continued in the context of the Federal Research Program *Reduction of Risks and Mitigation of Consequences of Natural and Manmade Emergencies in the Russian Federation*. In carrying out these programs, participants analysed and generalized information on the basic characteristics, conditions and scenarios leading to the onset of accidents and catastrophes in natural and industrial domains engendered by complex dangerous phenomena and processes in various regions of the world. Hazardous components of engineering

infrastructures (atomic power stations, trunk pipelines) may lead to catastrophes in the following classes (from 7 to 1): planetary, global, national, regional, local, facility-level, and localized (Figure 1). Potential losses and occurrence periodicity were evaluated as a function of the accident and catastrophe class (ranging from global to localized).<sup>1</sup>

Official documents of the Russian Federation use six catastrophe classes (from 6 to 1): transborder (equivalent to global), federal (equivalent to national), regional, local, facility-level, and localized.

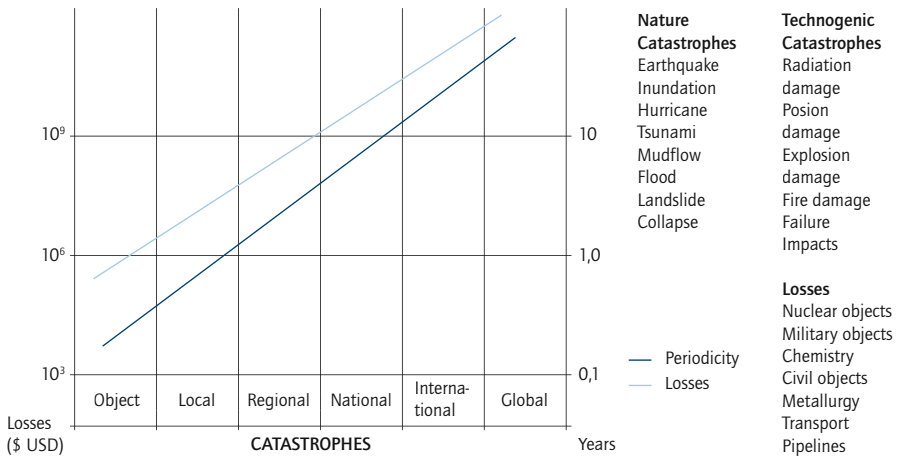
A classification of catastrophes was constructed based on the results of this summary analysis and taking into account the losses  $U$  and respective periodicities  $\Delta T$  (see Table 1). Here the magnitude  $U$  for each catastrophe decreases from 10<sup>10</sup>-10<sup>11</sup> to 10<sup>3</sup>-10<sup>4</sup> dollars, while the periodicity of their occurrence declines from (3 - 5) × 10<sup>1</sup> to 10<sup>-1</sup> years. Thus, the variation in losses (dollars per catastrophe) for different types of disasters is seven orders of magnitude while the variation in the probability of occurrence  $P = 1 / \Delta T$  (1/year) is three orders of magnitude.

Risk is a key concept in resolving problems related to ensuring safety. Risk is defined using the function  $F_R$  of the probability that a catastrophe will occur and the magnitude of loss inflicted when the catastrophe occurs.

$R$  represents the risk associated with a natural or manmade catastrophe,  $P$  is the probability of occurrence, and  $U$  is the associated loss (1).

$$R = F_R\{P, U\} = \sum_{i=1}^n R_i = \sum_{i=1}^n P_i \cdot U_i = \int U(P) \cdot P dP = \int P(U) \cdot U dU$$

Figure 1. Losses and periodicity of natural and manmade catastrophes



<sup>1</sup> Makhutov 2006 a.

Table 1. Risk of accidents and catastrophes

NO.	CLASS OF ACCIDENTS AND CATASTROPHES	$P$ (1/YEAR)	$U$ (DOLLARS)	$R$ (DOLLARS/YEAR)
1	Localized	$5.0 \cdot 10^0$	$5.0 \cdot 10^3$	$2.5 \cdot 10^4$
2	Facility-level	$1.2 \cdot 10^0$	$4.0 \cdot 10^5$	$4.8 \cdot 10^5$
3	Local	$5.0 \cdot 10^{-1}$	$7.0 \cdot 10^6$	$3.5 \cdot 10^6$
4	Regional	$1.6 \cdot 10^{-1}$	$1.0 \cdot 10^8$	$1.6 \cdot 10^7$
5	National	$1.2 \cdot 10^{-1}$	$1.5 \cdot 10^9$	$1.8 \cdot 10^8$
6	Global	$8.0 \cdot 10^{-2}$	$1.0 \cdot 10^{10}$	$8.0 \cdot 10^8$

The risks vary by four orders of magnitude. In Russia the occurrence probabilities of national and regional extreme situations differ by 1.4 times and are approximately an order of magnitude lower than the risk for local situations; the likelihoods of local and facility-level accidents differ by 5 times.

The assessment of probability  $P$ , loss  $U$ , and risk  $R$  for accidents and catastrophic situations involves a group of risk identification methods, including various methods for analysing statistical information on natural and manmade catastrophes of a particular type in the region being studied, as well as methods for analysing the reliability of equipment and technological processes and the effectiveness of management and control. Methods for calculating the magnitude of loss differ substantially for technical facilities and for natural systems. Specialists in Russia and other countries have thus developed a group of methods geared towards analysing natural-manmade processes that could potentially lead to accidents and catastrophic situations in engineering infrastructures.

## 2 PRINCIPLES OF ADDRESSING SECURITY RELATED PROBLEMS IN ENGINEERING INFRASTRUCTURES

The scientific base developed for assessing safety related problems in engineering infrastructures must be applied as broadly as possible in the effort to ensure against the impacts of terrorism. This approach to analysing security related problems assumes that emergency situations initiated by terrorist acts develop analogously to "ordinary" emergency situations triggered by natural or manmade disasters. Hence, they may be analysed using the same methods and models used to address classical safety problems.

The threat of terrorist acts must be included in the system of possible scenarios when studying the ways in which emergency situations might develop. In particular, scenario trees used for safety analyses in engineering infrastructures must be augmented

with scenarios that take terrorist attacks into account. These substantially change the scenarios themselves, as well as the structure of primary initiating factors in emergency situations. They also lead to cascading processes in the development of accidents and catastrophes with the biggest hits on the population, economic objects and other vital resources.

Including an analysis of security problems and terrorist mechanisms during the initiation of extreme situations aimed at critical targets in the national security infrastructure will necessitate adaptations to existing models and methods to allow special characteristics to be accounted for. When analysing terrorist related security problems, the initiation stage of the extreme situation and the structure of impact factors must first be compared with those in a traditional emergency caused by a natural or industrial disaster.<sup>2,3</sup>

It should also be noted that the modern strategy for ensuring safety, which calls for focusing efforts not on eliminating the consequences of extreme situations but on predicting and preventing them, must also be extended to cover situations in which emergencies are triggered by terrorist actions. In this case, scientific developments regarding methods for managing the risks of terrorism must be accorded great significance in integrated risk management mechanisms.

Most of components of existing engineering infrastructures are implemented in conformance with national and international regulations and norms for design, construction and maintenance without direct consideration of terrorist hazards.<sup>4,5</sup> This gives rise to two major security related problems of scientific-technical and social-economic nature in this context:

1. Provision and improvement of protection for the existing engineering infrastructures against terrorist attacks.
2. Design and construction of new engineering infrastructures with input parameters for protection against terrorist attacks.

Coping with these fundamental problems requires a special analysis of methods and scenarios for terrorist acts and a study of how existing and new defence systems respond to such acts to determine the level of EI vulnerability.

Conventional EI safety analysis focuses on the question: How can an accident scenario be realised in a given system? When addressing security problems for engineering infrastructure one must also consider the situation from the terrorist's standpoint. Hence, the modified question for security analysis becomes: What needs to happen for the given scenario to be realized in EI?

---

<sup>2</sup> Makhutov et al 2009.

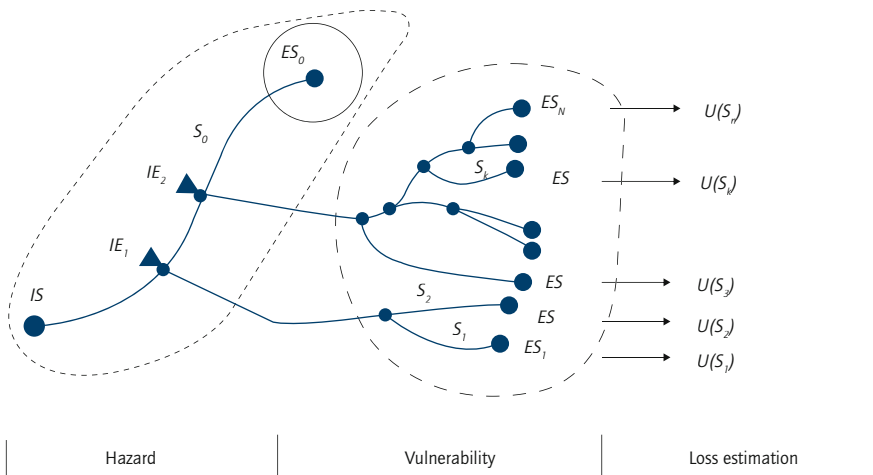
<sup>3</sup> Makhutov 2006 b.

<sup>4</sup> Makhutov 2007.

<sup>5</sup> Makhutov 2008.

We will attempt to the answer to this question using special graph models known as scenario trees. The system is designed to fulfil a so-called success scenario  $S_0$  (i.e. a transition from its initial start  $IS$  to the designed end state  $ES_0$ ). Since any scenario of a failure  $S_i$  represents a deviation from the success scenario  $S_0$  that corresponds to the successful functioning of the EI, the  $S_i$  scenario must have a disturbance point at which an extreme event, or, in the case of terrorism, an initiating event (IE), occurs (Figure 2). This initiating impact can be either internal (inflicted within the system boundaries) or external (inflicted from outside the system). Each initiating impact gives rise to a scenario tree, with each branch corresponding to a scenario  $S_i$  and ending with an end state (ES).

Figure 2. General risk assessment framework



Solving the above security analysis problem requires an assessment of terrorist resources. In security analysis, resources include a broad set of factors that determine the potential of a terrorist organization. These include:

- Material resources: technical means, equipment, 'human material' that can be used for terrorist attack
- Nonmaterial resources: experience, skills, knowledge, access to EI internal modes

- To answer the question of security analysis, experts should consider the quality of equipment available to the terrorists, their skills in and knowledge of engineering infrastructure, and their ability to exploit existing vulnerabilities (or create new ones) to organise the attack.

### 3 SPECIFIC FEATURES OF SECURITY RELATED THREATS

When assessing security related problems for engineering infrastructures the following characteristics of terrorist threat should be accounted for<sup>6</sup>:

**High level of dynamism:** Terrorist attack scenarios and impact factors are more dynamic in nature than those for natural and manmade disasters that a system is subjected to. A change in the spectrum and intensity of terrorism-related extreme effects on the system is significantly more powerful than a natural or manmade threat. This stems from the capacity of terrorists for constantly expanding their arsenal of mechanisms for initiating emergency situations using modern means of attack, reacting to changes in protection systems and learning from mistakes made in previous attacks on the system or others like it.

**High level of uncertainty:** There is a higher level of uncertainty involved in modeling terrorist scenarios and impact factors. In addition to the uncertainty factors inherent in natural or manmade threats, terrorist threats entail uncertainty factors resulting from the complexity of evaluating terrorist value systems and behavioural logic, as well as the organizational-technical potential and the resources at their disposal.

**Ability of terrorists to choose attack scenarios deliberately:** This refers to the deliberate selection of attack scenarios (places, times and types of actions) by terrorists, taking into account system vulnerability parameters and losses expected from a successfully executed attack. In other words, terrorists are able to analyse the vulnerability matrix and structure of losses for various types of actions against a system and select the attack scenario that maximizes the harm to society (taking secondary and cascade losses into account). Here, in addition to probability analysis, game theory must be applied to account for the deliberate terrorist actions.

**Complex nature of the terrorist threat:** The presence of a terrorist organization in a region may give rise to a broad spectrum of attack scenarios, including the time, place and character of the attack. Thus, countering terrorist threats and terrorist mechanisms in initiating emergency situations requires a complex systems approach to develop an optimal strategy for counterterrorism force and resource deployment and ensure security. Inasmuch, concentrating resources on protecting individual system elements (or protecting targets from one type of terrorist action) might prove useless since, upon re-evaluating the situation, a terrorist could either redirect the attack against another element of the target or switch to a different type of attack. In this case, counterterrorism efforts will not lead to reducing the risk and increasing the level of protection for the target.

---

<sup>6</sup> Makhutov et al. 2009.



In addressing traditional tasks of ensuring safety from natural and manmade disasters, the prevailing types of impact factors can be highlighted for the engineering infrastructure at hand, e.g. threats from seismic activity, flooding, chemical contamination, etc. Hardening a system against these impact factors will lead to the desired result. However, the spectrum of potential threats is significantly wider in protecting a given system from the manifestations of terrorism. Here, terrorists can analyse a system's level of protection against various types of impact factors, identify impact factors against which the target is least protected and concentrate their efforts on carrying out an attack that will bring these very factors to bear.

Furthermore, there are classes of terrorist actions without analogues in the impact factor structures typical for natural and manmade disasters (e.g. cyber terrorism or electromagnetic actions aimed at knocking out control systems).

*Presence of two-way linkages between the terrorist threat and system vulnerability:* One differentiating feature of a terrorist threat to a given system is the presence of two-way linkage between the threat and:

- a) Vulnerability of the system to that threat
- a) Magnitude of expected losses should threat be successfully realized

This characteristic of terrorist mechanisms must be examined in more detail, inasmuch as it opens up additional possibilities for reducing terrorism risks.

The formula for assessing the risk of a traditional emergency situation initiated by a natural or manmade disaster can be represented in simplified form as:

$$R_c = P_{IE} \times P_{(ID|IE)} \times U_{(Loss|IE \& ID)}$$

Here  $P_{IE}$  is the threat to the system, expressed as the probability of an initiating event (the failure of a particular element, a hazard factor passing a threshold value, extreme natural phenomena, and so forth).

$P_{(ID|IE)}$  is the vulnerability of the system to the given initiating event, expressed as the conditional probability that loss will be inflicted if the initiating event occurs.

$U_{(Loss|IE \& ID)}$  is the loss to the system should the initiating event occur and cause a loss.

Thus, for traditional natural and manmade disasters, vulnerability is determined by a specific threat, but the consequences depend on both the type of threat and the vulnerability of the system to that type of threat. Here it should be noted that this model has no two-way linkages, e.g. the dependence of the threat on vulnerability (inasmuch as the probability of a spontaneously initiated event has no relation to system vulnerability to that action) or dependence of the threat on the consequences (by the same logic). The system of linkages between risk factors for the given system in a natural or manmade emergency is presented in Figure 3a.

If the initiating event is a terrorist attack, the interactions among the various factors included in the risk assessment equation are more complex [4]. Similar to the expression above, terrorism risk is presented as follows:

$$R_T = P_A \times P_{(ID|A)} \times U_{(LossA\&ID)} \quad (3)$$

$P_A$  is the terrorist threat to the given system, expressed as the probability that a terrorist attack of a particular type will be carried out.

$P_{(ID|A)}$  is the vulnerability of the system to a terrorist attack of the given type, expressed as the conditional probability that damage will be inflicted if the attack is carried out.

$U_{(LossA\&ID)}$  is the loss inflicted on the system should the terrorist attack be carried out and cause a loss.

If a terrorist action occurs, the presence of powerful two-way linkages among the risk factors should be noted (see Figure 3b). In particular, reducing the vulnerability of a given system makes it possible to reduce substantially the level of the terrorist threat it faces.

Figure 3a: System of linkages between risk factors for emergency situations initiated by natural or manmade disasters (safety context)

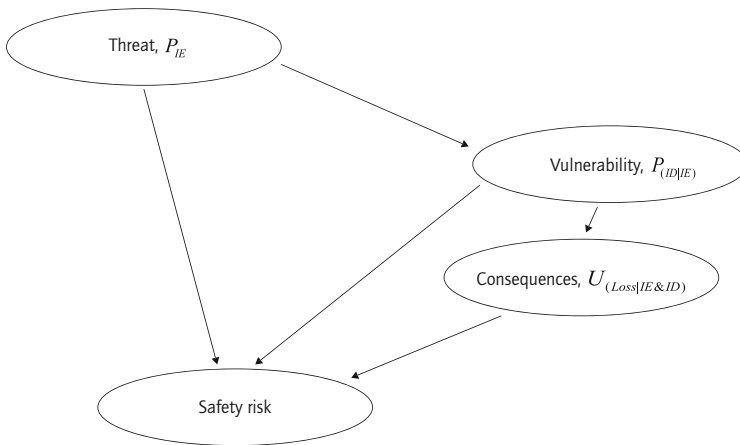
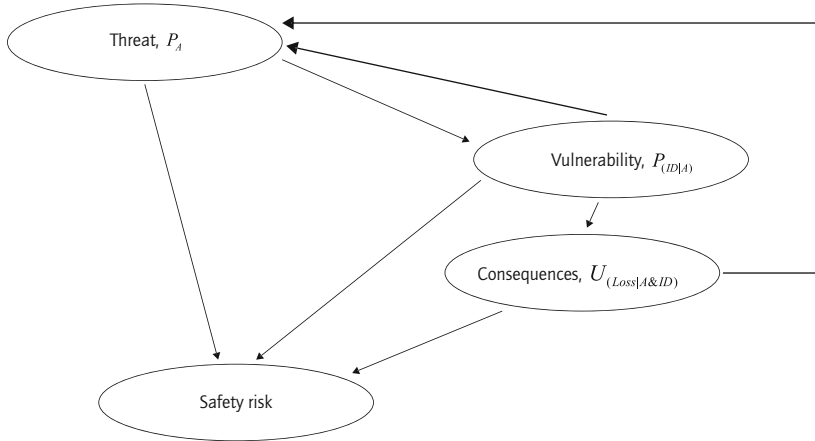


Figure 3b: System of linkages between risk factors for emergency situations initiated by terrorist attack (security context)



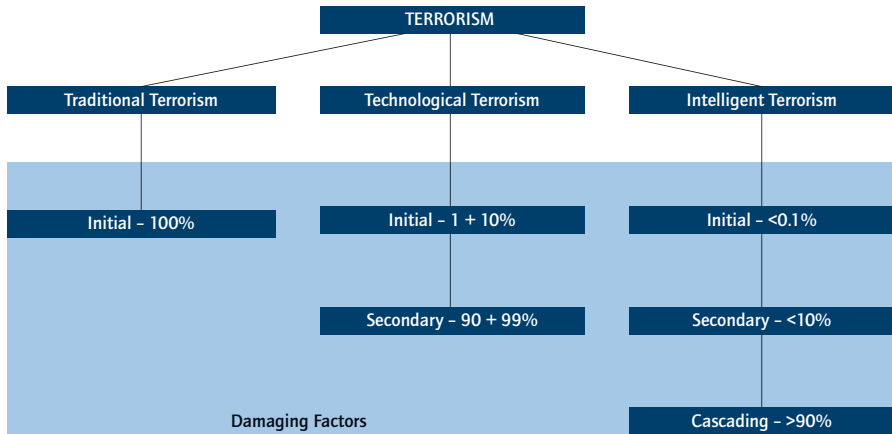
*Presence of aftereffects in the flow of terrorist actions:* In contrast to natural and man-made disasters, which may often be viewed as chains of Poisson events, after a major terrorist act the condition of the system defined as "terrorist organization—protected object—protection system" is substantially changed. On the one hand, the terrorist organization achieves its goals to one degree or another and expends a significant part of its resources, while, on the other hand, law enforcement agencies intensify the protection regime. Therefore, after a major terrorist act the situation fundamentally changes and the likelihood of a subsequent attack is significantly altered as well (generally, it is reduced). Therefore, the sequence of terrorist attacks could be described with the help of a Markov chain model. For the purpose of this model, the activities of antiterrorist forces aimed at countering the terrorist threat are understood as under control. The Markov process model makes it possible to describe the dynamics of cycles of terrorist activity.

*Terrorists' capacity for self-learning:* Because terrorists are capable of analysing the results of previous attacks and drawing conclusions from them, their experience in "successful" and "unsuccessful" attacks can have a noticeable effect on the selection of a scenario for the next attack. (Attack scenarios that have proven effective in the past have a greater likelihood of being repeated by terrorists in the future, while scenarios that ended unsuccessfully will most likely be less attractive to terrorists and will consequently be less likely to be repeated.) Therefore, in assessing the chances that various attack scenarios will be realised, statistical self-learning models are more effective than traditional frequency methods.

#### 4 TYPES OF MODERN TERRORISM

Modern terrorism can tentatively be divided into three levels: traditional terrorism, technological terrorism and intelligent terrorism. These differ by their resources, attack scenarios and structure of losses (Figure 4).<sup>7,8</sup> Traditional terrorism implies the organization of explosions, fires, assassinations of officials, public figures and people at large in order to intimidate the population and destabilize the political situation in a country or region. Risks pertaining to traditional terrorism are not considered in this paper since terrorism on this level does not involve engineering infrastructures to trigger secondary catastrophic processes in EIs. We will deal with two other levels of terrorism that are directly related to attacks on EIs.

Figure 4. Types and damaging factors of modern terrorism



#### > Technological terrorism

Technological terrorism (TT) implies powerful, unauthorized impacts on *engineering infrastructures* capable of:

- Penetrating the EI protection system;
- Initiating secondary catastrophic processes due to hazardous substances (W), energy (E), and information (I) stored or processed in the EI;
- Escalation of the accident outside the EI boundaries with substantially increased secondary and cascade losses.

<sup>7</sup> Makhutov 2006 a.

<sup>8</sup> Garrick et al. 2004.

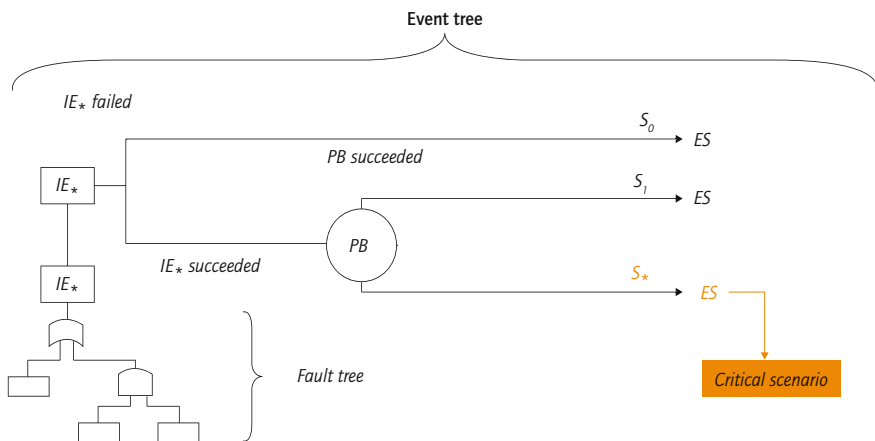
Technological terrorism is based on taking advantage of the existing vulnerabilities of a system. To perform an act of technological terrorism requires, in advance:

- Analysing the EI structure and vulnerabilities, i.e., revealing potential sources of secondary catastrophic processes (stocks of W, E, I) and the weak points in the EI protection systems, and devising the most efficient attack scenarios
- Identifying key EI elements and links whose failure would disrupt the infrastructure
- Calculating the strength of the initial impacts that might penetrate the EI protection systems (PS)
- Assessing the EI scenario tree and determining the end states  $ES_*$  capable of initiating major secondary catastrophic processes outside the EI

In the case of TT, the attacking party do not have insider information and cannot inflict point impacts imperceptible to the EI monitoring systems. A powerful action capable of overcoming the EI protection systems must therefore be prepared. The terrorists must select the method of attack resulting in the EI end state that would initiate accident propagation outside the EI boundaries.

The selection of the attack scenario is done using a hybrid scenario tree<sup>9,10,11</sup> that, in case of TT, can be quite simple. It incorporates several fault trees describing the abilities and resources of the terrorists and the event tree describing the EI vulnerability (Figure 5).

Figure 5. The Hybrid Scenario tree for technological terrorism



<sup>9</sup> Kaplan 2002.

<sup>10</sup> Garrick et al. 2004

<sup>11</sup> Pate-Cornell 2002.

### > Intelligent (or highly-sophisticated insiders') terrorism

Intelligent terrorism (IT) is a purposeful unauthorized interference into the process of designing, building and/or operating an EI aimed at increasing its existing vulnerabilities and creating new ones in the system so that these input vulnerabilities, insider's knowledge of the system and access to its elements can be exploited for future realization of most disastrous scenarios of a terrorist attack.

IT implies:

- A comprehensive vulnerability assessment of a system under design, in construction or in operation with respect to various scenarios of terrorist impacts, and identification of the most effective ways of realizing of the initiating impact upon the system
- Insertion of latent changes into the system at the design, construction or operation stage *in order to create new vulnerabilities in the EI*
- Disconnection or disruption of the EI monitoring and protection systems
- Triggering cascading failures in the system and the environment

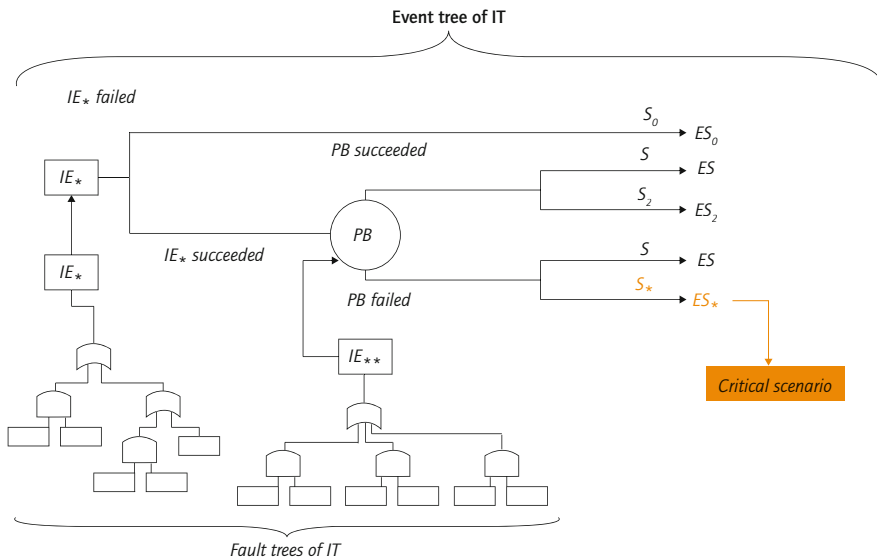
As a rule IT requires a member of a terrorist group to penetrate the staff of the organization that is designing, building or operating the target EI. The terrorist must possess insider information on the EI and be able to perform well-camouflaged actions to weaken protection systems, create latent defects undetectable by the existing monitoring systems.

In sum, intelligent terrorism implies detailed knowledge of the target EI structure and operating principles, awareness of existing and potential vulnerabilities, possible end states, possible scenarios of accident propagation and initial impacts that can trigger them. Additionally, IT can anticipate distortion of the success scenario, formulate false targets and generate new disastrous scenarios.

Intelligent terrorism implies a maximal level of the terrorist competence (comprehensive knowledge of the EI, including its control, operation and protection systems) which will allow the terrorist to select the most disastrous accident scenarios, find the most effective way of initiating these scenarios, and influence the EI monitoring systems to prevent prompt responses to failures. The assessment of the attack scenarios is made through a hybrid scenario tree that, in case of IT, can be somewhat more complicated (Figure 6). It incorporates several fault trees describing the abilities and resources of terrorists and the event tree describing the system vulnerability.

The results of studies in the field of safety and security have been reflected in the fundamental 33 volume series *Safety of Russia* that is being published in accordance with a decision by The Security Council of the Russian Federation.

Figure 6. The hybrid scenario tree for intelligent terrorism



## REFERENCES

### Makhutov 2006 a

Makhutov N.: Methodology for Assessing the Risk of Terrorism. In Countering Urban Terrorism in Russia and the United States (ed. G.Schweitzer and C.Sharber). The National Academies Press. Washington DC. 2006.

### Makhutov et al. 2006 b

Makhutov N.: "Analysis of Technogenic Risks Under Terrorist Impacts" in Protection of Civilian Infrastructure from Acts of Terrorism. K. Frolov, G.Baecher. Springer. P.O. Box 17, 3300 AA Dordrecht, The Netherlands. 2006. 54-67

### Makhutov, Reznikov 2007

Makhutov N., Reznikov D.: Methods for Quantitative Terrorist Risk Assessment. Problems of Safety in Emergency Situations Vol. 1, 2007 pp.89-104 (in Russian)

### Makhutov 2008

Makhutov N., Reznikov D.: Assessment of risks of Major Catastrophes at Critical Infrastructures Taking into Account the possibility of Extreme Losses. Problems of Safety in Emergency Situations. Vol. 4, 2008 74-89 (in Russian)

**Makhutov et al. 2009**

Makhutov N., Petrov V., Reznikov D.: Characteristics of Technological Terrorism Scenarios and Impact Factors. (ed. G.Schweitzer), The National Academies Press. Washington DC. 2009.

**Reznikov 2007**

Reznikov D.: Models for Assessing Terrorist Risks. Workshop on Open-source Risk Software. California Institute of Technology, Pasadena, USA 2007

**Kaplan 2002**

Kaplan S.: "Applying the General Theory of Quantitative Risk Assessment (QRA) to Terrorism Risk." In Risk-Based Decision-Making in Water Resources X: Proceedings of the Conference, Y.Y. Haimes, D.A. Moser, and Stakhiv E.Z., eds. Reston, VA: ASCE Publications. 2002.

**Garrick et al. 2004**

Garrick B., Hall J., Et al.: Confronting The Risk Of Terrorism: Making The Right Decisions/Reliability Engineering And Safety Systems, 86 (2004) 129-1768.

**Pate-Cornell 2002**

Pate-Cornell E.: Probabilistic Modelling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Counter-measures. Military Operations Research, 2002, v7, N4, pp5- 23



## > CONCLUSION

KLAUS THOMA/DANIEL HILLER/TOBIAS LEISMANN/BIRGIT DREES

Considering the breadth of perspectives in security research among Europeans, as exemplified within this publication, one may certainly note that a tremendous development of this young discipline has occurred in a short period of time. Only three years have passed since the discipline was promoted to an individual theme within the specific programme on 'Cooperation' of the European Commission FP7. Since then, a conceptual framework has been established and the first collaborative projects have been executed on different levels, all at an impressive pace. Although the future of security research will remain closely linked to the political will of EU member states, the established base will serve as a solid foundation for the further development of the discipline on a European scale.

This publication makes it abundantly clear that many European countries have a long-standing security research tradition. In the mean time, numerous European states have even aligned their national civil security research programmes to the European approach within FP7. Security missions and research paths are oriented towards building basic capabilities to master the multiplicity of challenges, more specifically threats and risks, that result from today's security environment. It appears there is an undisputed common denominator among European countries, regardless of whether thinking on a national or European level, when it comes to the imperative of:

*"... research activities that aim at identifying, preventing, deterring, preparing and protecting against unlawful or intentional malicious acts harming European societies, human beings, organizations or structures, material and immaterial goods and infrastructures, including mitigation and operational continuity after such an attack (...) or natural/industrial disaster"*<sup>1</sup>

It goes without saying that Europe, as a union of 27 member states, is in a very unique position. In spite of the fact that today most security issues are deliberated on a global scale, the European Union obviously faces some genuinely European challenges that require immense effort to reduce vulnerabilities while at the same time increasing the overall resilience of European citizens and critical assets.

---

<sup>1</sup> See ESRA B report.

Before concluding with the commonalities and differences extracted from the perspectives of the various national representatives throughout this publication, we will review some characteristics specific to the European security environment.

Today, at unprecedented speed, revolutions in information technology and transportation networks, just to name two, have accelerated the free movement of capital, goods, services, information and people within Europe. The European Union, with its more than 500 million citizens of diverse cultural backgrounds, provides a common economic area with open borders between members of the Schengen agreement. To the degree that this liberalization of regulations and controls has increased the personal mobility and liberty, it has also increased the vulnerability of European societies as a whole<sup>2</sup>. Daniel Hamilton, an American security researcher, has pointedly summarized this shift as follows:

*“Globalization is causing a shift in conceptions of power and vulnerability from those that are state-centric and territorial-based to those that are stateless and network-based. A transformative approach to security would supplement the traditional focus on the security of the territory with a clearer focus on the security of critical functions of society. Terrorists, for instance, wielding weapons of mass destruction or mass disruption are less intent on seizing and holding our territory than they are on destroying or disrupting the ability of our societies to function”<sup>3</sup>*

The crux is that the sensitive structures guaranteeing the overall functionality of our modern societies are based on complex intertwined networks, rather than on clearly defined territorial spaces or assets cordoned off by distinct borders. Consequently, a holistic approach to civil security research must be comprehensive, creating new and possibly unorthodox research paths while bringing together different disciplines of the technical sciences, as well as humanities, law and economics.

In recapitulating the perspectives presented throughout this book, a number of topics common to all contributions will be summarised to give an overview of the broad spectrum of views and concerns raised in the past seven chapters.

First and foremost it is important to note that the terms ‘security’, ‘threat’ and ‘risk’ are perceived and interpreted very differently depending on the historical, cultural and political background of the EU countries represented herein. Switzerland, Russia and the UK, for example, obviously have widely differing experiences and problems with regard to modern security threats. Whereas Russia and the UK may share concerns with regard to domestic terrorism they have experienced throughout long periods of their history, Switzerland, as a non-EU state located in the heart of the Europe, will most likely prioritize other issues, such as energy supply security or ICT security. Many countries

---

<sup>2</sup> Thoma/Drees/Leismann 2006.

<sup>3</sup> Hamilton 2006.

have initiated broad debates in their security research communities as experts increasingly acknowledge the importance of reaching a consensus on basic fundamentals. This certainly includes a common understanding of what these terms and concepts refer to.

It was obvious that the EU, specifically the Commission, would have to address this issue of security perceptions and interpretations when it initiated the process of the security theme. Although both ESRAB and ESRIF have clearly achieved a result supported by its member states, this issue is likely to remain a fervently debated topic as new technology evolutions and future incidents will likely have a radical impact on how we as individuals, researchers and society as a whole will perceive specific security concerns.

The second issue is that many European countries have already designed and implemented *sophisticated national civil security programmes*, often equipped with substantial funding by their respective governments. Whereas in some countries, such as the UK or France, the line between defence and civil security research is not cut and dry, Germany, for the first time in its history, drafted a genuine civil security research programme in 2006 that is closely aligned with the EU's security research programme. Moreover, Germany has chosen to organize security research comprehensively using a multi-disciplinary and cross-institutional approach. Currently, the federal republic is drafting a sequel to its first civil security research programme<sup>4</sup>. The UK, aside from its voluminous national security strategy and unique counter terrorism strategy, has recently drafted the executive document 'Ideas and innovation – how industry and academia can play their part'<sup>5</sup>, which identifies key technologies and concepts to be developed by security researchers to guarantee overall national security. Similar to Germany, Switzerland has also chosen a comprehensive, cross-institutional and multi-disciplinary approach, including all federal agencies and the executive branch, as well as private actors and operators who are involved in security related activities. Slovakia, on the other hand, is still in the process of developing a coherent and systematic approach to developing national capabilities in the field of security research. As a young member of the European Union, it is still in the process of adapting to completely new political structures.

In spite of the successful establishment of security research on a European level within FP7 and beyond, there is a consensus within the European security research community that the Union's unique constellation as a community of many different cultures and national sensitivities necessitates the development of supplemental national capabilities and strategic concepts. In the end, the balance between individual national interests and common European interests must be found in line with a 'not-one-size-fits-all' principle.

The third great concern to most European partners is the *vulnerability* and, consequently, *protection of critical infrastructures*. Here again, definitions of what is considered 'critical' differ to some degree. The lowest common denominator seems to be the

<sup>4</sup> Wissenschaftlicher Programmausschuss zur nationalen Sicherheitsforschung 2010.

<sup>5</sup> Ideas and Innovation 2009.

characterization of critical infrastructure sites and assets, as elaborated by Prof. Kröger. Accordingly, such critical infrastructures vary by their nature (e.g. physically engineered, cybernetic or organizational systems), environment (geographical or natural) and operational context (e.g. political/legal/institutional or economic). In more general terms, however, critical infrastructures often do not have a single operator or regulator. Furthermore, such sites and assets are normally prone to multiple hazards and threats, whether naturally caused or man-made. Ultimately, most critical infrastructures are characterized by a high degree of interconnectivity and mutual interdependence. In this respect, although the pervasive use of ICT in the management of large-scale infrastructures provides great advantages in terms of making complex systems more operable, it also gives rise to new risks, e.g. susceptibility to cyber attacks.

The fourth dominant topic concerns *making critical infrastructures and society as a whole more resilient* against the multiplicity of threats and risks we are facing today. A major guiding principle of the British counter terrorism strategy is maintaining a resilient society. In the German security research community, increasing attention has been devoted to the idea of resilient infrastructures and societal resilience in general. Switzerland has fostered the concept of resilience in the field of disaster management on a very sophisticated level. The basic idea, as portrayed repeatedly herein, is to increase a society's capacity for absorbing shocks and disturbances and thereby preserving its overall function after a major attack/shock or natural disaster. In its comprehensive understanding of the term resilience, current research considers not only societies' ability to 'bounce back' to a pre-attack status, but also their ability to learn and adapt in the aftermath of major incidents<sup>6</sup>. The underlying premise of this overall concept is that, in light of our current and future security environment, aiming for 'complete security' is not an overly realistic goal. Instead, Europeans must strive to prevent major incidents from incapacitating the critical nodes of our highly complex modern societies.

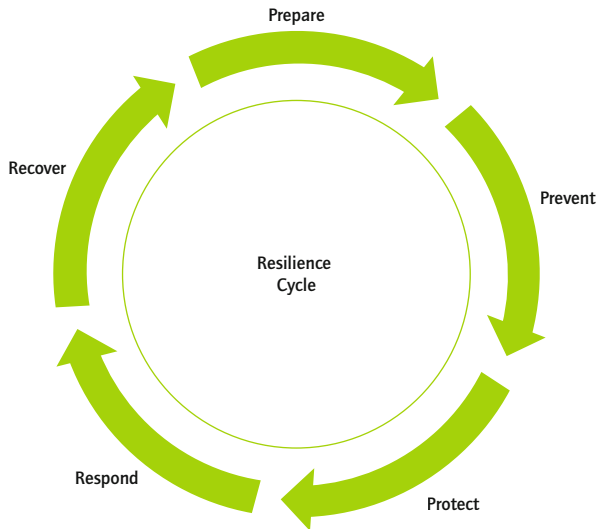
Quintessentially, a promising way to master this enormous endeavour is to ensure well-established and sophisticated concepts and technologies throughout the entire so-called *resilience cycle*.

This cycle has been chosen as a central element in ESRI's final report and many European countries are adapting this concept of *prepare – prevent – protect – respond – recover*.<sup>7</sup> The chapters of this book show there is a clear consensus on the need to approach security research on a much broader scale than in the past. Key terms are 'comprehensive approach', 'holistic approach' or 'system of systems' approach. All of these terms indicate that the discipline has lacked the requisite breadth and depth. The resilience cycle offers a truly comprehensive list of aspects to be considered if we are to think big in security research.

---

<sup>6</sup> Edwards 2009.

<sup>7</sup> See also: Fraunhofer Memorandum der Fraunhofer-Gesellschaft zur Fortführung der nationalen Sicherheitsforschung 2010.



Ultimately, the approach to security research taken by individual member states and Europe as a whole demonstrates diversity in accord. Countries can forge their national programmes individually while sharing common goals and values that will, in the end, hopefully provide a further example of successful European integration – enabling the Union to meet the security challenges of today and tomorrow.

## REFERENCES

### Edwards 2009

Edwards, Charlie: Resilient Nation. Demos. London: 2009.

### Hamilton 2006

Hamilton, Daniel S. Transforming Homeland Security: A Road Map for the Transatlantic Alliance. In: Transforming Homeland Security: U.S. and European Approaches. (ed.) E. Brimmer. Washington, DC: Center for Transatlantic Relations, 2006.

### Ideas and Innovation 2009

Countering the terrorist threat – Ideas and innovation. How industry and academia can play their part. HM Government. Office for Security and Counter-Terrorism, A Directorate of the Home Office, London: August 2009.

**Memorandum der Fraunhofer-Gesellschaft zur Fortführung der Nationalen Sicherheitsforschung. München: 2010.**

**Thoma, Klaus/Drees, Birgit/Leismann, Tobias 2009**

Zukunftstechnologien in der Sicherheitsforschung. In: Winzer, Petra/Schnieder, Eckehard/Bach, Friedrich-Wilhelm (eds.): „Sicherheitsforschung – Chancen und Perspektiven.“ München: 2009

**Wissenschaftlicher Programmausschuss Sicherheitsforschung**

Positionspapier des Wissenschaftlichen Programmausschusses zur nationalen Sicherheitsforschung. Freiburg: 2010.

## INDEX OF AUTHORS

**Christian Bréant** has been appointed by J. Solana in May 2008, EDA Director for Research & Technology. From February 2004, he was deputy director for “technology strategy” and R&T Director for Defence and Security of the DGA in the French MoD. He is a graduate from Ecole Polytechnique (1976) and PhD scientist in Laser Physics from Paris University. He was post-doc at JILA, Boulder, University of COLORADO, USA. Initially in charge of R&T studies in the field of laser sources and systems, he became manager of the optronics and laser department in 1989. In 1994, he became Deputy Head of the Directorate for Research and Technology and Assistant to the NAD’s Chief scientist Adviser. In 1997, he joined the Directorate for Cooperation and Industrial Affairs in Paris as Deputy Director in charge of industrial and economic analyses. In 2000, he was appointed Director of the Defence Analysis Centre (CAD) in charge of operational analysis and simulation for preparation of the future defence systems. In March 2005, Christian Bréant was elected a member of the French Academy of Technologies. In 2006-2007, he was a member of the European Security Research Advisory Board (ESRAB) of the European Commission and presently member of ESRIF.

### **Birgit Drees**

After having finished her studies at the Westfalian-Wilhelms-University of Münster and the University of Joensuu, Finland, Dr. rer. nat. Birgit Drees received her PhD in Biology from the Westfalian-Wilhelms university of Münster. In 2008, Dr. Drees joined the Fraunhofer Ernst-Mach-Institute for High-Speed Dynamics (EMI) in Freiburg. She is part of EMI’s Business Development unit, responsible for supporting and assisting different departments involved in the field of security research. Aside from organizing and managing research proposals and projects on a national and European level, Dr. Drees is also project manager for the Fraunhofer innovation cluster »Future Security BW«.

### **Tobias Feakin**

Dr. Tobias Feakin is Director of the National Security and Resilience department at the Royal United Services Institute for Defence and Security Studies. Within this role he is responsible for the growth of a research team examining issues pertaining to radicalisation, terrorism, counter-terrorist policy and technologies, resilience, critical national



infrastructure, and the security impacts of climate change. He completed his PhD in International Security and Politics from the University of Bradford in 2005 with a thesis entitled "Non-Lethal Weapons: Technology for Lowering Casualties". Since that time he has worked as a Research Fellow for the Landau Network, Centro-Volta in Italy, and the Home Office arriving at Royal United Services Institute in 2006. He has lectured at the University of Cambridge, University of Bradford, Joint Services Command and Staff College, the NATO Defence College in Rome, as well as speaking internationally at numerous conferences and roundtable discussions. Regularly being used by the media he has appeared on the BBC, Channel 4, NBC, Al-Jazeera, Sky News, as well as being quoted in many newspapers around the globe.

### **Daniel Hiller**

Before joining the Business Development unit of the Fraunhofer Ernst-Mach-Institute for High-Speed Dynamics (EMI) in Freiburg, M.A. Daniel Hiller has worked in the field of Market Research for Rheinmetall Defence, Düsseldorf. Mr. Hiller completed his M.A. in Political Science, History and Conflict Studies at Philipps-University of Marburg, Germany and Pennsylvania State University, USA.

### **Ulrich Karock**

Ulrich Karock joined the R&T Directorate of the European Defence Agency in July 2005 where he is currently the Technology Manager of the „Systems of Systems, Space, Simulation & Experiment“ domain. Since autumn 2006 he manages the first ever European defence research programme on „Force Protection“. In this frame twenty nations jointly invest in eighteen projects in the areas of individual and collective protection, counter CBRNE, intelligence and surveillance, command and control, mobile communications and protection technology forecasting. Before joining EDA he worked as a project officer in the Aeronautics, Space, Transport and Security Directorate of the European Commission's Research Directorate General. He moved to Brussels from Berlin where he was the Head of Quality Management of Condat AG. Further positions in his career were the Mechanical Engineering Faculty and the Institute for Quality Management of the University of Hanover and the Naval Shipbuilding at Bremer Vulkan AG. He received his mechanical engineering degree from the University of Hanover where he studied production sciences, project and quality management. Ulrich Karock is married, has three children and lives with his family in Brussels.

### **Wolfgang Kröger**

Professor Dr. Wolfgang Kröger studied at the RWTH in Aix-la-Chapelle where he received his Dr.-Ing. (PhD) in Mechanical Engineering. He continued his studies at the BUGH Wuppertal where he habilitated in 1986. From 1974 until 1990 he works at the



National Research Centre (FZJ) where he eventually became Director of the Institute for Nuclear Safety Research. Since 1990 he is employed at the ETH Zurich. From 1990 until June 2003 he was also Head of Research Department and Member of the Directorate of the PSI. Afterwards he became Founding Rector of IRGC (International Risk Governance Council).

Professor Wolfgang Kröger is member of various organizations, such as the Swiss Academy of Engineering Sciences, the European Nuclear Forum and Member of Scientific Directorate, Deutsche Gesellschaft für Auswärtige Politik (DGAP). He published numerous books and articles, mainly about risks, opportunities and safety of nuclear power. Furthermore, he received OECD/NEA News prize in 2001 and is Honorary member of the SGK (Swiss Society of Experts on Nuclear Energy) since 2004.

### **Tobias Leismann**


Dr. rer. nat. Tobias Leismann studied physics at Heidelberg, Cambridge (UK) and the Technical University of Munich where he received his PhD working as a research associate for the Max-Planck Institute for Astrophysics. Before joining the Fraunhofer Ernst-Mach-Institute for High-Speed Dynamics (EMI) in Freiburg, Dr. Leismann has been working as a technology consultant for four years. Dr. Leismann is the head of EMI's Business Development unit and responsible for the institute's security research activities. In addition, Dr. Leismann is executive secretary of the Fraunhofer Group for Defence and Security as well as project manager of the Fraunhofer innovation cluster »Future Security BW«.

### **Tjien-Khoen Liem**

Tjien-Khoen Liem, European Commission, holds a Masters degree in Electronics Engineering from the University of Kent at Canterbury. He worked for 14 years for Honeywell in Germany on Military Aircraft Avionics, Infrared Systems and other Defence programmes. For over 17 years he has been with the European Commission. He was part of the team that built up Aeronautics / Air Transport research at DG RTD. He was among the first people in the team setting-up European Security Research, now with DG Enterprise and Industry.

### **Nikolay A. Makhutov**

Since 2009, Prof. Nikolay A. Makhutov is chief researcher at the Institute for Machine Sciences of the Russian Academy of Sciences and since 1995 Vice-president of the International Institute of Engineering Safety. He graduated in Mechanical Engineering from Moscow State Aviation Technology University (1959) and received his PhD degree (1964) and a Doctor of Science in Mechanical Engineering at the Institute for Machine Sciences (1975). In 1978, he became full professor and since 1987, Nikolay Makhutov



is member correspondent of the Russian Academy of Sciences and since 1994 member of the American Society of Mechanical Engineers. In 2003, he was awarded with the Russian Federation State Prize. He has long standing research experiences in the field of development of integrated risk mitigation programs. His current research interest focuses on emergency response management and comprehensive risk assessment.

### **Eckehard Schnieder**

Eckehard Schnieder was born in 1949 in the seaport Wilhelmshaven, Germany. He received his diploma (equivalent with master degree) in electrical engineering with specialisation in control and computer engineering in 1972 from the Technische Universität Braunschweig. Until 1979 he worked as a research scientist at the same university concerning advanced electrical drive control systems simulation resulting in the world's first fully micro computer controlled electrical drive. He received his Dr.-Ing. (PhD in engineering) in 1978. From 1979 until 1989 Dr. Schnieder joined Siemens Division Eisenbahnsignaltechnik (now: Transportation Systems), where he directed the German maglev TRANSRAPID operation control system's design and development as well as the automatic control of Siemens people mover. Since 1989, Dr. Schnieder is a full professor and head of the Institute of Traffic Safety and Automation Engineering, formerly Institute of Control and Automation Engineering. From 2000 – 2002 he represented the Technical University Braunschweig as a vice president. He directed the first formal modelling of the European Railway Control System (ETCS), the basic research on satellite assisted railway location systems, and other German and European projects for advanced railway operation control systems in cooperation with operators, suppliers, and safety authorities especially on level crossing in the EU-project SELCAT. Professor Schnieder was offered several professorships; in 1998 he received the Carl-Adam-Petri-Award of the Society of Design and Process Science. In 2005 he received the Doctor honoris causa from Todor Kableshkov University of Transportation, Sofia followed by the Dr. h.c. of the Slovakian University Zilina and Otto von Guericke University Magdeburg Germany both in 2010, honouring his achievements both in the educational and the scientific sector within the cooperation between the universities. Presently he is spokesman of the acatech group safety.

### **Juray Sinay**

Prof. Juray Sinay holds the chair for Safety Engineering and Quality Management at the department for Mechanical Engineering at the Technical University of Košice, Slovakia. In 1973, he graduated at this department and received his PhD degree in 1976. In 1990, Juray Sinay habilitated at the Bergische Universität Wuppertal, Germany and has been appointed to a professorship for Materials Handling/ Safety Engineering at the

Technical University of Košice in 1991. Juray Sinay is author and co-author of numerous monographs and scientific publications and participated in more than 90 scientific conferences and congresses in Slovakia and abroad.


### **Klaus Thoma**

Prof. Dr. rer. nat. Klaus Thoma is the director of the Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut (EMI), since 1996. EMI is mainly dealing with shock wave phenomena, impact and penetration procedures and the associated simulation and measurement technologies; applications being in the fields of defense, security, Space and car safety. Prof. Thoma has graduated in physics from the Technical University Munich where he also received his PhD. After that he worked as scientist at Messerschmitt-Bölkow-Blohm (today's EADS) for eight years, last in the position as department head. Following that he was co-founder and executive director of an engineering company. In 1994 he was offered a chair at the University of the German Armed Forces in Munich. Two years later Prof. Thoma was appointed director of the Ernst-Mach-Institute of the Fraunhofer-Gesellschaft. 1999 followed the appointment as honorary professor for short time events (structural dynamics) in the department of civil engineering at the University of the German Armed Forces, Munich. In 2003 he became honorary professor at the Nanjing University of Science and Technology, China. Since 2002 Prof. Thoma chairs the Fraunhofer Group for Defense and Security Research. He is a member of the editorial advisory boards of the International Journal of Impact Engineering since 2007. As chairman of a government advisory board he counsels the German Ministry of Education and Research (BMBF) concerning security research. In 2010 he was elected into the German Academy of Technical Sciences. His main research topics are:

- Security research
- Materials research
- Shock, impact and penetration physics
- Numerical simulation
- Crash-analysis
- Ballistics

### **Petra Winzer**

Prof. Dr.-Ing. habil. Petra Winzer obtained her degree in electrical engineering and her magna cum laude doctoral degree from the Technical University of Dresden, and her habilitation from the Technical University in Berlin in 1996. Until her appointment as chair for Quality and Product Safety at the University of Wuppertal in 1999, she held various positions at the Brandenburg Technical University of Cottbus where she worked



on many projects in the areas of quality management and the integration of quality, environment and work safety managements. Her current research fields are systems engineering, management systems, quality sustainable development. Petra Winzer is a member of the academic board of the European Network of Total Quality Management of the European Master Program in Total Quality Management (EMPTQM) as well as a member of the convent of technique sciences of the German Academic Scientific Association (acatech). She is also member of the board of the GQW (Association of Quality Sciences). Since September 2008 she is prorector for international affairs and transfer.

## > acatech – DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

acatech vertritt die Interessen der deutschen Technikwissenschaften im In- und Ausland in selbstbestimmter, unabhängiger und gemeinwohlorientierter Weise. Als Arbeitsakademie berät acatech Politik und Gesellschaft in technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Darüber hinaus hat es sich acatech zum Ziel gesetzt, den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu erleichtern und den technikwissenschaftlichen Nachwuchs zu fördern. Zu den Mitgliedern der Akademie zählen herausragende Wissenschaftler aus Hochschulen, Forschungseinrichtungen und Unternehmen. acatech finanziert sich durch eine institutionelle Förderung von Bund und Ländern sowie durch Spenden und projektbezogene Drittmittel. Um die Akzeptanz des technischen Fortschritts in Deutschland zu fördern und das Potenzial zukunftsweisender Technologien für Wirtschaft und Gesellschaft deutlich zu machen, veranstaltet acatech Symposien, Foren, Podiumsdiskussionen und Workshops. Mit Studien, Empfehlungen und Stellungnahmen wendet sich acatech an die Öffentlichkeit. acatech besteht aus drei Organen: Die Mitglieder der Akademie sind in der Mitgliederversammlung organisiert; ein Senat mit namhaften Persönlichkeiten aus Industrie, Wissenschaft und Politik berät acatech in Fragen der strategischen Ausrichtung und sorgt für den Austausch mit der Wirtschaft und anderen Wissenschaftsorganisationen in Deutschland; das Präsidium, das von den Akademiemitgliedern und vom Senat bestimmt wird, lenkt die Arbeit. Die Geschäftsstelle von acatech befindet sich in München; zudem ist acatech mit einem Hauptstadtbüro in Berlin vertreten.

Weitere Informationen unter [www.acatech.de](http://www.acatech.de)

## > acatech diskutiert

Die Reihe „acatech diskutiert“ dient der Dokumentation von Symposien, Workshops und weiteren Veranstaltungen der Deutschen Akademie der Technikwissenschaften. Darüber hinaus werden in der Reihe auch Ergebnisse aus Projektarbeiten bei acatech veröffentlicht. Die Bände dieser Reihe liegen generell in der inhaltlichen Verantwortung der jeweiligen Herausgeber und Autoren.

## BISHER SIND IN DER REIHE „ACATECH DISKUTIERT“ FOLGENDE BÄNDE ERSCHIENEN:

Reinhard F. Hüttl/Bernd Pischetsrieder/Dieter Spath (Hrsg.): *Elektromobilität. Potenziale und wissenschaftlich-technische Herausforderungen* (acatech diskutiert), Heidelberg u.a.: Springer Verlag 2010.

Manfred Broy (Hrsg.): *Cyber-Physical-Systems. Innovation durch softwareintensive eingebettete Systeme* (acatech diskutiert), Heidelberg u.a.: Springer Verlag 2010.

Klaus Kornwachs (Hrsg.): *Technologisches Wissen. Entstehung, Methoden, Strukturen* (acatech diskutiert), Heidelberg u.a.: Springer Verlag 2010.

Martina Ziefle/Eva-Maria Jakobs (Hrsg.): *Wege zur Technikfaszination* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009

Petra Winzer/Eckehard Schnieder/Friedrich-Wilhelm Bach (Hrsg.): *Sicherheitsforschung – Chancen und Perspektiven* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009

Thomas Schmitz-Rode (Hrsg.): *Runder Tisch Medizintechnik. Wege zur beschleunigten Zulassung und Erstattung innovativer Medizinprodukte* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Otthein Herzog/Thomas Schildhauer (Hrsg.): *Intelligente Objekte. Technische Gestaltung – Wirtschaftliche Verwertung – Gesellschaftliche Wirkung* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Thomas Bley (Hrsg.): *Biotechnologische Energieumwandlung. Gegenwärtige Situation, Chancen und Künftiger Forschungsbedarf* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Joachim Milberg (Hrsg.): *Förderung des Nachwuchses in Technik und Naturwissenschaft. Beiträge zu den zentralen Handlungsfeldern* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2009.

Norbert Gronau/Walter Eversheim (Hrsg.): *Umgang mit Wissen im interkulturellen Vergleich. Beiträge aus Forschung und Unternehmenspraxis* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.

Martin Grötschel/Klaus Lucas/Volker Mehrmann (Hrsg.): *Produktionsfaktor Mathematik. Wie Mathematik Technik und Wirtschaft bewegt* (acatech diskutiert), Heidelberg u. a.: Springer Verlag 2008.

Thomas Schmitz-Rode (Hrsg.): *Hot Topics der Medizintechnik. acatech Empfehlungen in der Diskussion* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.

Hartwig Höcker (Hrsg.): *Werkstoffe als Motor für Innovationen* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.

Friedemann Mattern (Hrsg.): *Wie arbeiten die Suchmaschinen von morgen? Informationstechnische, politische und ökonomische Perspektiven* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2008.

Klaus Kornwachs (Hrsg.): *Bedingungen und Triebkräfte technologischer Innovationen* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2007.

Hans Kurt Tönshoff/Jürgen Gausemeier (Hrsg.): *Migration von Wertschöpfung. Zur Zukunft von Produktion und Entwicklung in Deutschland* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2007.

Andreas Pfingsten/Franz Rammig (Hrsg.): *Informatik bewegt! Informationstechnik in Verkehr und Logistik* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2007.

Bernd Hillemeier (Hrsg.): *Die Zukunft der Energieversorgung in Deutschland. Herausforderungen und Perspektiven für eine neue deutsche Energiepolitik* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2006.

Günter Spur (Hrsg.): *Wachstum durch technologische Innovationen. Beiträge aus Wissenschaft und Wirtschaft* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2006.

Günter Spur (Hrsg.): *Auf dem Weg in die Gesundheitsgesellschaft. Ansätze für innovative Gesundheitstechnologien* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2005.

Günter Pritschow (Hrsg.): *Projektarbeiten in der Ingenieurausbildung. Sammlung beispielgebender Projektarbeiten an Technischen Universitäten in Deutschland* (acatech diskutiert), Stuttgart: Fraunhofer IRB Verlag 2005.