

**CRIME PREVENTION AND
SECURITY MANAGEMENT**

Series Editor: M. Gill

palgrave▶pivot

**POLICING
TRANSNATIONAL
ORGANIZED CRIME
AND CORRUPTION**

Exploring the Role of Communication
Interception Technology

**Mitchell Congram, Peter Bell and
Mark Lauchs**



Crime Prevention and Security Management

Series Editor: **Martin Gill**

Titles include:

Paul Almond

CORPORATE MANSLAUGHTER AND REGULATORY REFORM

Rachel Armitage

CRIME PREVENTION THROUGH HOUSING DESIGN

Policy and Practice

Joshua Bamfield

SHOPPING AND CRIME

Mark Button

DOING SECURITY

Critical Reflections and an Agenda for Change

Mitchell Congram, Peter Bell and Mark Lauchs

POLICING TRANSNATIONAL ORGANIZED CRIME AND CORRUPTION

Exploring the Role of Communication Interception Technology

Daniel Donnelly

MUNICIPAL POLICING IN THE EUROPEAN UNION

Comparative Perspectives

Paul Ekblom

CRIME PREVENTION, SECURITY AND COMMUNITY SAFETY USING THE 5IS
FRAMEWORK

Adam Graycar and Tim Prenzler

UNDERSTANDING AND PREVENTING CORRUPTION

Janice Goldstraw-White

WHITE COLLAR CRIME

Accounts of Offending Behaviour

Bob Hoogenboom

THE GOVERNANCE OF POLICING AND SECURITY

Ironies, Myths and Paradoxes

Daniel McCarthy

‘SOFT’ POLICING

The Collaborative Control of Anti-Social Behaviour

Kate Moss

BALANCING LIBERTY AND SECURITY

Human Rights, Human Wrongs

Kate Moss

SECURITY AND LIBERTY

Restriction by Stealth

Tim Prenzler

POLICING AND SECURITY IN PRACTICE

Challenges and Achievements

Emmeline Taylor
SURVEILLANCE SCHOOLS
Security, Discipline and Control in Contemporary Education

Jan van Dijk, Andromachi Tseloni and Graham Farrell (*editors*)
THE INTERNATIONAL CRIME DROP
New Directions in Research

Adam White
THE POLITICS OF PRIVATE SECURITY
Regulation, Reform and Re-Legitimation

Crime Prevention and Security Management

Series Standing Order ISBN 978-0-230-01355-1 **hardback**
978-0-230-01356-8 **paperback**
(*outside North America only*)

You can receive future titles in this series as they are published by placing a standing order. Please contact your bookseller or, in case of difficulty, write to us at the address below with your name and address, the title of the series and one of the ISBNs quoted above.

Customer Services Department, Macmillan Distribution Ltd, Houndmills, Basingstoke, Hampshire RG21 6XS, England

palgrave▶pivot

▶

Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology

Mitchell Congram

Australian Federal Government

Peter Bell

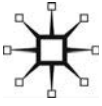
Queensland University of Technology, Australia

and

Mark Lauchs

Queensland University of Technology, Australia

palgrave
macmillan



© Mitchell Congram, Peter Bell and Mark Lauchs 2013
Softcover reprint of the hardcover 1st edition 2013 ISBN 978-1-137-33378-0

All rights reserved. No reproduction, copy or transmission of this publication may be made without written permission.

No portion of this publication may be reproduced, copied or transmitted save with written permission or in accordance with the provisions of the Copyright, Designs and Patents Act 1988, or under the terms of any licence permitting limited copying issued by the Copyright Licensing Agency, Saffron House, 6–10 Kirby Street, London EC1N 8TS.

Any person who does any unauthorized act in relation to this publication may be liable to criminal prosecution and civil claims for damages.

The authors have asserted their rights to be identified as the authors of this work in accordance with the Copyright, Designs and Patents Act 1988.

First published 2013 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan in the US is a division of St Martin's Press LLC, 175 Fifth Avenue, New York, NY 10010.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN: 978-1-137-33379-7 PDF

ISBN: 978-1-349-46237-7

DOI: 10.1057/9781137333797

A catalogue record for this book is available from the British Library.

A catalog record for this book is available from the Library of Congress.

www.palgrave.com/pivot

Contents

List of Figures	vi
Series Editor's Introduction	vii
Notes on Authors	ix
1 Introduction	1
2 Transnational Organized Crime	11
3 Corruption	29
4 Policing Methodologies	47
5 Anti-Corruption Models	56
6 Communication Interception Technology	69
7 Directions in Intelligence and Investigations	96
8 Integrating Communication Interception Technology within Investigations	103
9 Conclusion	112
References	121
Index	136

List of Figures

2.1	Standard hierarchy	14
2.2	Regional hierarchy	15
2.3	Clustered hierarchy	16
2.4	Core group	16
2.5	Criminal network	17
5.1	The second Joke network	66
6.1	UK warrantry authorization process as required under RIPA	76
8.1	Conceptual framework for the integration of CIT into an active TOC/corruption investigation	106



Series Editor's Introduction

This book provides a discussion about an area of policing that has suffered from a lack of research; surprisingly little is known about the characteristics of transnational organized crime (TOC) and corruption and the links between them. Mitchell Congram, Peter Bell and Mark Lauchs provide a scholarly overview of the circumstances and contexts in which these activities flourish, and the different ways offences are planned and conducted, and the different ways offenders organize themselves. It does not shy away from considering definitional issues, nor does it let these get in the way of progressing discussion about how best to respond. Indeed, this aspect, how to tackle TOC and corruption, has, in particular, received far less attention than it merits.

The authors argue that tackling these offences will always require a variety of approaches, not least because they manifest themselves in different ways; different causes and patterns of offending will inevitably call upon the need for different prevention approaches. The skill rests in pinpointing these thereby affording the opportunity for focused responses that have the potential to work.

They argue that a key element of organized crime groups is the need for communication; they need to engage with each other speedily and reliably. This is a key way in which communication interception technology (CIT) comes in, and is the focus of much of the book. Although it has received limited discussion, the authors highlight its potential. Similarly, with regards to corruption, they discuss the merits of accessing 'dark networks' via intelligence


gathering with the help of CIT; that is both to identify offenders and to disrupt networks. CIT is presented as more than just an investigative technique but as an investigative tool in its own right.

The use of technology typically poses a range of challenges. This includes 'human factors' relating to usability issues that receive less coverage to the advantage of a discussion of another main challenge, and perhaps the main one, the balance between providing security and ensuring respect for civil liberty issues. Legal complications and the broader intelligence gathering culture pose further hurdles to the integration of CIT. Yet through case study examples you will read about the opportunities.

This book proposes a theoretical model for integrating CIT into investigations and intelligence operations. The theory has to be tested but is presented in order to generate discussion about how to better tackle both TOC and corruption. For that reason alone we must hope its merits and drawbacks are debated rigorously.

Martin Gill

Notes on Authors



Dr Peter Bell (Ed D, MBA, M Ed, B Bus) is a senior lecturer at the Queensland University of Technology's (QUT) Faculty of Law, and the Director of Postgraduate Studies at the School of Justice. Dr Bell has held senior analytical and operational positions with the Queensland Police Service, the Australian Bureau of Criminal Intelligence, the Australian Federal Police and the Organised Crime Agency of British Columbia-Canada (OCABC). Published internationally on transnational organized crime, intelligence, and counter-terrorism and policing issues, Dr Bell has travelled extensively and has been retained by various state and federal governments, law enforcement agencies, academic institutions, multinational and crown corporations in Canada, the United States, Saudi Arabia, China, Thailand, Singapore, Hong Kong, Indonesia and the United Arab Emirates (UAE). Dr Bell also teaches the 'International Policing' programme which forms the major component of the Bachelor of Justice Degree for the Singapore Police

Mitchell Congram (B Justice – Hons) is an Honours graduate of the Queensland University of Technology's (QUT) School of Justice, with a Bachelor's degree majoring in Policing and Criminology and focus on transnational organized crime.

Dr Mark Lauchs (L LB, Ph D) is a senior lecturer at the Queensland University of Technology's (QUT) Faculty of Law, and the Coordinator of the Policy and Governance Major of the Bachelor of Justice degree at the School of Justice. Dr Lauchs previously worked in the Queensland

state government in policy and project roles associated with accountability and the justice system. He completed his PhD on the history of public sector ethics and accountability in Queensland through Queensland University of Technology. Dr Lauchs also teaches in the 'International Policing' programme which forms the major component of the Bachelor of Justice Degree for the Singapore Police. Dr Lauchs has published internationally on the link between police corruption and organized crime. He is also a member of the Higher Education Research Network (HERN).

1

Introduction

Abstract: *The development of information and communication technology (ICT), in providing opportunities for improved communication for both legitimate and criminal purposes, impedes traditional law enforcement strategies directed towards the disruption of criminal activities. This chapter introduces the research problem to be addressed by the remaining chapters: that the development of ICT and its use for illegitimate purposes presents a key vulnerability that can be exploited by law enforcement agencies (LEAs). Transnational organized crime (TOC) and corruption take advantage of modern information and communication technologies to communicate and in doing so communication interception technology (CIT) has become a crucial weapon in the fight against TOC and corruption. This chapter introduces the elements addressed throughout the book, explaining the underpinning research methodology, scope and limitations.*

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

The consistent development of information and communication technology (ICT) and its subsequent growth in usage and popularity has not been limited to legitimate uses. Indeed, ICT is routinely utilized by criminals to advance their own illicit goals. The ability to communicate is a key requirement for any organized crime and/or corrupt network and, as such, is a key vulnerability. The need for two criminal entities to exchange information regarding a planned crime is the critical point at which law enforcement agencies (LEAs) can disrupt criminal activities. With transnational organized crime (TOC) and corruption much of this communication makes use of ICT and, as such, communication interception technology (CIT) is a crucial weapon that can be utilized. However, without the placement of CIT in the correct policing framework and a viable knowledge management model it is a weapon lacking efficiency or effectiveness (Congram and Bell, 2010).

This book provides academics, researchers and practitioners in the law enforcement and intelligence fields with a comprehensive review and analysis of literature in the fields of CIT, TOC and corruption (particularly official corruption) up to the first decade of the 21st century. In particular, the book has a strong focus on four, English-speaking Commonwealth countries, namely: Australia, New Zealand (NZ), Canada and the United Kingdom (UK). It reviews the notion and threat of TOC and corruption, the modern frameworks of policing methodology, and the issues and concerns relevant to the practice of employing CIT in the fight against TOC and corruption. In doing so the book provides a strong argument for, and evidence of, the growing acceptance of the need to place CIT within the investigation continuum. Based on the review and analysis the authors propose a model of best practice that will support the development of a proactive and intelligence-led framework that will underpin the use of CIT in the fight against TOC and corruption.

Research problem and significance of the research

An assortment of research surrounds CIT (see for example Attorney General's Department, 2008; Bamford, 2009; Brady, 2008; Flood and Gasper, 2009; Heldon, 2009; Leyden, 2009; Rogers, 2009; Waters, Ball and Dudgeon, 2008; Willey, 2009; Jackson et al., 2007) and TOC (see for example Abadinsky, 2009; Andreas and Nadelmann, 2006; Australian

Crime Commission, 2009; Block, 2008; Borger, 2007; Brady, 2008; Davies, 2007; Leong, 2008; Lyman and Potter, 2007; Malkin, 2007; Stelfox, 2008; United Nations Office of Drugs and Crime, 2008; Walters, 2009; Chalk et al., 2009).

However, these bodies of knowledge have rarely intersected in an examination of the effective and practical use that CIT can have against TOC and corruption. Researching TOC, corruption and entrepreneurial criminals is an essential endeavour, as the expansion of ICT, breaking down of borders, and connections across the globe means that all nations have the potential to be negatively impacted by criminal entities. It is, therefore, imperative to understand how these criminals are operating, how they are structured and, more importantly, how they can be stopped. This research addresses an important gap in the modern policing theory.

While there is some literature on CIT it is either outdated and does not address the current issues and legislation of the 21st century or focuses less on its use as a law enforcement tool and primarily on the privacy concerns that arise with an intrusive method of investigation. Others focus on the use and implementation in a foreign country and therefore are limited in their application to Australia and other English-speaking Commonwealth countries.

The globalization and growth of TOC and corrupt networks is a cause for great concern amongst society and it is essential to examine whether CIT is an appropriate law enforcement tool to be used in this context.

This is done by asking:

- 1 How effective is communication interception technology in the fight against TOC and corruption? and;
- 2 How should the issues surrounding CIT be best managed within a practical law enforcement framework by English-speaking Commonwealth countries that share comparable legislative platforms?

The present study therefore builds on the existing literature on organized criminality, official corruption and CIT, and draws them together to provide a clearer overview of CIT's use in an enforcement and intelligence capacity. This research addresses several gaps in the literature by examining how TOC enterprises and networks of corruption are structured, their respective method(s) of communication and how this is a vulnerability that can be exploited by LEAs. The research identifies the most

appropriate policing methodology to underpin the use of CIT and how it can be or is currently being restricted by the policing culture and privacy concerns present in various English-speaking Commonwealth countries.

By examining the way in which CIT can be used, this publication contributes to the knowledge that can provide greater efficacy for law enforcement strategies and the disruption of the serious threat posed by official corruption and TOC to society. The publication findings have further implications for intelligence-led policing (ILP) initiatives and the subsequent use of intelligence as a strategic decision-making tool which can be implemented appropriately into the broader Commonwealth law enforcement community (Coyne and Bell, 2011b).

Limitations in scope

It is important to note that this book is confined to open and available source material up to and including March 2012. As can be expected, there have been major advancements in ICT as well as significant changes to legislation and policy since this data collection period. The release of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013 is a prime example. The Manual was created at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence and is a collection of opinions of independent experts in relation to how 'extant international law norms apply to this "new" form of warfare' (www.ccdcoe.org). As its release occurred outside of the data collection period the Manual is not covered in this publication; it may, however, be of interest to academics, researchers and professionals in the law enforcement and intelligence arenas and can be accessed by visiting The NATO Cooperative Cyber Defence Centre of Excellence website (www.ccdcoe.org). While specific issues such as cyber attack and cyber crime are not the focus of this book, specific legal instruments employed by certain Commonwealth countries in managing cyber crime and the like are touched on in relevant chapters.

Book structure

This book comprises nine chapters. The second and third chapters provide a review of the literature and relevant theory on TOC and

corruption (in particular official corruption) respectively. Both chapters seek to examine the issues surrounding the definition of both TOC and official corruption, their theoretical constructs, as well as predominant organizational structures and vulnerabilities. The literature is also examined with regard to the legislative instruments that are used to address the issues of TOC and official corruption in Australia and other English-speaking Commonwealth countries, namely: NZ, Canada and the UK.

Chapter 4 examines contemporary policing methodologies, theories, systems, processes and practices used to investigate TOC and official corruption in Australia and other English-speaking Commonwealth countries. The chapter analyses specific policing and anti-corruption models such as traditional policing, community-oriented policing, problem-oriented policing, computer statistics and ILP.

Chapter 5 analyses the strategies currently employed by law enforcement organizations within Australia, NZ, Canada and the UK to investigate corrupt systems and 'dark networks' – networks that are covert and illegal. The inclusion of CIT as an investigative/intelligence tool is discussed along with contemporary anti-corruption methods such as integrity testing and advanced integrity testing. The chapter also examines the legislative instruments that support the deployment of CIT strategies in such investigations and various proactive measures designed to reduce the incidence of official corruption.

Chapter 6 discusses CIT in the context of being more than just an individual investigative tool used to gather intelligence and evidence in investigations relating to TOC and official corruption, but rather that CIT is frequently incorporated into the surveillance arena of practical investigative methodologies. The chapter examines the legislative instruments used to support and monitor the lawful use of CIT in Australia, NZ, Canada and the UK and discusses the various forms of CIT, its role and function within an investigation and the challenges posed to both investigators and legislators. It also identifies the major constraints to the advancement of CIT in an investigative capacity: legislative constraints, privacy concerns and intelligence culture.

Chapter 7 discusses several emergent themes within the literature regarding the direction of intelligence doctrine and contemporary investigative strategies in combating TOC and official corruption and the role for CIT in support of the four primary directions of intelligence direction, the ILP model and the practical application and effectiveness of CIT.

Chapter 8 presents a conceptual framework for the effective integration of CIT into investigations of TOC and official corruption. The chapter also examines the impact of legislation, intelligence limitations and organizational culture on the efficacy of the proposed conceptual framework.

Chapter 9 provides a conclusion and includes a summation of the main themes contained in the book, providing some indication of the challenges faced by LEAs in Australia and other English-speaking Commonwealth countries in combating TOC and official corruption. The concluding chapter also makes recommendations for further research.

Research approach

In support of the research outlined in this book a qualitative study employing grounded theory was used to explore the relationship between CIT and its application in practical policing methodologies. Denzin and Lincoln (2005) argue that qualitative research highlights the importance of meanings and processes that are not otherwise measured or examined, where the characteristics of the data relate to numbers, such as quantity, frequency or intensity. Hence qualitative research methods involve analysing interviews and texts in order to uncover meaningful patterns relating to a particular issue (Mason, 2002; Denzin and Lincoln, 2005; Neuman, 2006). The use of the grounded theory methodology provided legitimacy and logic to the study and allowed theory to emerge from the data. Grounded theory is defined by Glaser (1998) as a systematic generation of theory from data acquired through thorough research, providing an integrated set of conceptual hypotheses and probability statements about the relationship between concepts. Grounded theory provides a viable method of induction and deduction of theory without the need to force the data (Glaser, 1978, 1992, 1998; Glaser and Strauss, 1967).

The research questions developed for this study focus on framing two issues. The first relates to the effectiveness of the use of CIT by Australian LEAs in being able to combat TOC. The second relates to the practical framework, or model of best practice, for LEAs to harness the 'crime fighting' capacity of CIT.

As such the study was designed to address the following two questions:

- 1 How effective is CIT in the fight against transnational organized crime?

- 2 How is CIT best managed in a practical law enforcement framework?

Data collection

A data collection plan (DCP) was used to manage the collection process. The DCP allowed the researchers to list the initial data requirements and work in incremental tasks for collection.

When a source of data was found the details were recorded within a spreadsheet, along with any relevant comments and a folio reference number to allow for easy recall. This ensured that the researcher was covering all areas relevant to the research and that unnecessary saturation of a particular topic did not occur. If a new topic of relevance was discovered during the collection and/or analysis phases this was simply added to the DCP as a new data requirement and the process for collection was repeated. Using the data requirements listed in the DCP the researcher was then able to commence actual collection.

Data collection included all available and relevant sources up to and including March 2012. With a range of relevant resources available the researchers utilized various search engines as a systematic research tool for this study. Initially, broad keyword search terms such as 'communication interception', 'communication interception technology', 'stored communication interception', 'email interception', 'SMS interception', 'lawful interception' and 'interception legislation' were utilized. Additionally, the literature review had suggested that communication interception research was grouped into three areas: privacy considerations, legal considerations and practical applications. Subsequently, more specific search terms such as 'privacy', 'legal' and 'applications' and appropriate synonyms such as 'intercepts', 'telecommunications' and 'phone' were employed to target core subjects. The documents retrieved through these searches also guided the decision for the use of further search terms to obtain information that was more specific. For example, key phrases such as 'tapping' or 'taps' and 'bugging' or 'bugs' were discovered which led to the creation of more specific keyword phrases such as 'telecommunication + bugs or bugging', 'telecommunication + taps or tapping', 'communication + bugs or bugging', 'phone + taps or tapping' or 'phone + bugs or bugging'. In doing this the researchers were able to conduct searches that were more refined and retrieve data of

greater relevance. Additionally, the researchers used a variety of phrases developed from 'signals intelligence'. The researchers recognized that, whilst the majority of the results related to military history concepts and national security, the underlying concepts and data that resulted proved relevant to the project. It is important to note, however, that issues that have become increasingly relevant in the literature post-2012 such as cyber warfare-related issues are not specifically covered in this book. As such, related terms such as 'botnets', 'Trojan insertion' and 'ransomware' were not included in the data collection process.

Online databases such as the Attorney General's Information Service Plus Text, CINCH Australian Criminology Database, Criminal Justice Periodicals, Informit, SpringerLink, Informaworld and ScienceDirect, along with the use of various search engines such as Lexis-Nexis, provided a vast array of online peer-reviewed journals. Databases such as the Australia/New Zealand Reference Centre, ProQuest Telecommunications and ProQuest Social Sciences provided the latest accounts relating to interception technology and interception activities within Australia, NZ, Canada and the UK. Annual Reports published by government agencies, such as the Australian Attorney General's Department, the Department of Justice – Canada, the New Zealand Ministry of Justice and The Office of the Commissioner for Communication Interception (UK), provided detailed information as to the statistical figures relating to telecommunication interception including warrants, arrests, prosecutions and costs. Dissertations and Theses via ProQuest and Australasian Digital Theses also provided information on previous research conducted in the field or related areas of CIT. During the examination of texts the reference lists of documents were also consulted as a means of recognizing additional works that were not identified during searches. This information led to the acquisition of several printed publications on related fields of organized crime, criminal intelligence and knowledge management systems. Case studies illustrating clear examples of the effective use of CIT were also used, collated from a variety of government reports and official publications. Overall the data collection procedure ensured that each identified category was given both equal consideration and weight.

Due to the constant comparative and collective nature of grounded theory it was appropriate to conduct further data collection with respect to these specific relationships as a means of identifying whether a relationship exists. With a specific core category it was possible to conduct an immediate collection and saturate the category without the need to

sift through irrelevant material. A principal example of this is the data relating to the practical methods of ILP and CIT. By collecting additional data the researchers were able to identify the relevant characteristics in supporting the use of the ILP model. The process also helped to identify less robust themes as a means of eliminating those that were not substantiated by this phase of data collection.

Document analysis

Document analysis was employed as a secondary analytical method in order to address two critical issues. Firstly, data relating to the use of CIT is not easily available through other methods. Finding criminal enterprises willing to be interviewed or surveyed to determine their communication patterns and structures is highly unlikely due to their obvious illegitimate criminal culture. Interviewing law enforcement personnel also poses its own challenges. They are often unwilling, for obvious reasons, to disclose confidential information that could include current strategies and uses, available technology and targets. This is further amplified by the use of interception technology within the intelligence community, where high levels of secrecy and sanitized publications pose severe limitations on the availability of appropriate information. Secondly, access to this information is well beyond the researchers' capabilities in terms of clearances, 'inside' knowledge and, of most relevance for this study, time. For similar reasons, observation of interception activities and law enforcement investigations are also difficult with the potential for invasion of privacy of investigated parties, along with ethical and legal issues of security clearances, and again the possibility of publishing current strategies or techniques employed against criminals that are yet unknown to them. The problems arise in these research methods due to the paucity of prior research and studies in this area.

Further to this, earlier work on CIT offers little information with respect to the advancement of technology and criminal cultures, the growing transnational nature of organized crime, their communicative patterns and abilities or CIT's specific use within policing methodologies. As such, learning from previous research and utilizing prior methods is challenging. Mason (2002) notes that documents provide a way of gaining access to strategies, events or procedures that cannot be

observed because they are either private or have already occurred. For this research on CIT, document analysis can, to an extent, reveal some concealed elements of interception technology. It is for these reasons that it suits the exploratory nature of the research.

Chapter summary

The development of ICT, in providing opportunities for improved communication for both legitimate and criminal purposes, impedes traditional law enforcement strategies directed towards the disruption of criminal activities. This chapter has presented the research problem, namely that the development of ICT and its use for illegitimate purposes presents a key vulnerability that can be exploited by LEAs. TOC and corruption take advantage of modern information and communication technologies to communicate, and in doing so CIT has become a crucial weapon in the fight against TOC and corruption. However, despite this opportunity there is a gap in our understanding of CIT's role in this context. While bodies of literature exist on TOC, corruption and CIT they have rarely intersected in an examination of the effectiveness and practical use CIT can have in these contexts. As such this book presents research which builds on existing literature on organized criminality, official corruption and CIT in order to provide a clearer view of the use of CIT in an enforcement and intelligence capacity.

In doing so it presents academics, researchers and practitioners and professionals in the law enforcement and intelligence fields with a comprehensive background and analysis of the literature in regards to the nature and extent of TOC and related corruption issues, culminating in a proposed model of best practice which imbeds CIT within an investigation continuum. This model aims to generate discussion on the merits of embedding CIT in an ILP framework to aid in the fight against transnational crime and corruption.

2

Transnational Organized Crime

Abstract: Transnational organized crime (TOC) is a diverse and complicated arena, costing global society in excess of US\$3 trillion annually – a figure that continues to grow (Borger, 2007). This chapter reviews the current literature which demonstrates that globalization has resulted in an increasing growth and sophistication of crime groups as they take advantage of disappearing borders and greater profit markets. It considers the various TOC organizational structures that exist and the legislative responses to this global threat by four English-speaking Commonwealth countries: Australia, the United Kingdom, Canada and New Zealand. It identifies that whilst crime groups are vulnerable to detection and disruption because of their need to communicate, law enforcement agencies need a method and framework that allows them to capitalize on this vulnerability to combat these crimes efficiently and successfully.

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

Understanding transnational organized crime

Transnational organized crime (TOC) is defined by the United Nations (UN) as:

structured groups of three or more persons acting together, over a period of time, with the aim of committing one or more serious crimes committed in more than one State, or has significant effect on another state, or elements of planning, preparation, direction or control occur in another State. (UN, 2000, pp. 25–26)

Whilst TOC can be viewed as a broad spectrum of activity, law enforcement agencies (LEAs) note a range of specific ‘organized’ activities. These include money laundering, drug trafficking, sex/human trafficking, people smuggling, arms trafficking, endangered species trafficking, cybercrime and, most notably over the past decade, terrorism (Abadinsky, 2009; Davies, 2007; Lyman and Potter, 2007; Australian Crime Commission, 2009; Borger, 2007; Grennan and Britz, 2006). Unlike many ‘habitual’ forms of crime, TOC defies ‘tradition’ and exploits the reactive crime control techniques currently utilized by LEAs (Andreas and Nadelmann, 2006). As a result there has been substantial disagreement over the ability to succinctly define such an adaptable assortment of crimes and groups. Grennan and Britz (2006, p. 7) contend that ‘definitions of organised crime are as diverse, as inaccurate, and as numerous as those traditionally associated with criminal groups’. An alternate definition by Conklin (2009) which shares the similar definitional notions of rules and codes and the organizational characteristics put forward by both Abadinsky (1994, 2009) and Grennan and Britz (2006, p. 12) describes organized crime as:

Criminal activity by an enduring structure or organization developed and devoted primarily to the pursuit of profits through illegal means... organized crime has the characteristics of a formal organization: a division of labor, coordination of activities through rules and codes, and an allocation of tasks in order to achieve certain goals. The organization tries to preserve itself in the face of external and internal threats. (Conklin, 2009, p. 73)

Despite this definition others argue that there is no generally accepted definition of TOC in spite of the many authorities and academics who have attempted to describe its attributes (Williams, 2001; Abadinsky, 1994, 2009). Van Duyne (2000) proclaims that the concept of organized

crime itself is too vague and too contradictory to be satisfied with a general scientific definition. He contends that as soon as one engages in drafting an operational definition the subsequent definition has to be adapted to a particular form of organized crime, which can be specified. In doing so, however, it renders the term 'organized crime' redundant in its use (Van Duyne, 2000). Van Duyne (2000) goes so far as to suggest the withdrawal of the term 'organized crime' and the use of the term 'continuous criminal enterprise' as its replacement and 'criminal entrepreneurs' to describe the criminals involved. Whilst disagreements surrounding definitions are viewed by many as simple semantics there is good reason for the concern. This is embedded in the specific terminology of 'transnational' and the subsequent legal and jurisdictional issues that emerge from cross-border criminal activities; for where definitions differ, so too do legislative and operational responses of nations. Shelley (1998) argues that a key to this is recognizing the political, geographic, economic and cultural factors underpinning TOC as a means to understanding the reasons for its growth and development among organized crime groups. For the purpose of this research Conklin's (2009) definition is used to underpin discussions relating to TOC.

Structure of transnational organized crime groups

The structure of organized crime networks, domestic or transnational, have long since been viewed as highly organized hierarchical structures, with groups such as the Sicilian Mafia popularized in novels and film, influencing common perceptions. In line with Conklin's (2009) notion of the criminal's self preservation, crime groups have modified their structures into what Cressey (1997, p. 3) and Williams (2001, p. 70) describe as 'fluid, dynamic and loosely structured networks that are highly flexible and possess the ability to adapt to relevant influences, designed with an intention to confuse authorities and protect their organization.' It is this complexity and sophistication of crime groups that impacts on policing, and further supports the need for specialized operations and international cooperation to address the full dimensions of international criminal organizations (Shelley, 1998). Understanding the structure of criminal groups, however, is integral to the development and recognition of potential weaknesses.

As with defining TOC, the organizational structure of crime groups is also highly debateable. Research by the UN (2002) of 40 organized crime groups in 16 countries led to the development of five organizational structures for TOC groups:

- ▶ standard hierarchy
- ▶ regional hierarchy
- ▶ clustered hierarchy
- ▶ core group
- ▶ criminal network.

It is argued that the first three hierarchical structures are those closest to the more ‘traditional’ notions of organized crime, whereas the final two structures are closest to organizations emerging in the current global climate, and are the ‘fluid, dynamic and loosely structured networks’ described by Cressey (1997, p. 3) and Williams (2001, p. 70).

Standard hierarchy

The standard hierarchy (Figure 2.1) is characterized by its clearly defined hierarchy and chain of command, usually led by a single individual. They possess strong systems of internal discipline and ‘codes of conduct’ and have clearly defined roles. They influence and/or control a particular territory from which they operate within, usually under a particular name by which they are known, and use violence as an integral tool to conduct their business. Finally, they consist of members with similar strong identities, either ethnic or social, which aids in maintaining conduct and authority (UN, 2002; Lyman and Potter, 2007).

Regional hierarchy

The regional hierarchy (Figure 2.2) is similar to the standard hierarchy in that they both possess strong systems of internal discipline, codes of conduct, have clearly defined roles and lines of authority, a single leadership

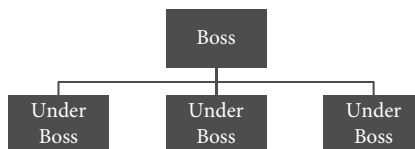


FIGURE 2.1 *Standard hierarchy*

Source: UN, 2002.

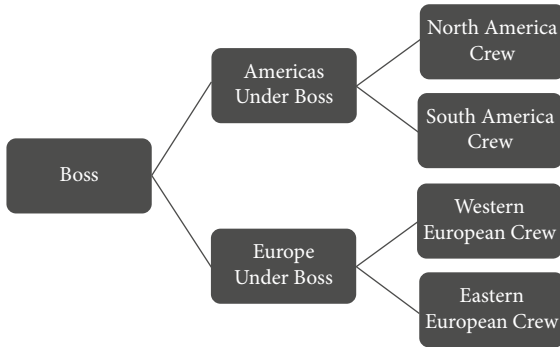


FIGURE 2.2 *Regional hierarchy*
Source: UN, 2002.

structure, and strong ethnic or social identities. The primary difference is that the regional hierarchy provides independence and autonomy to local groups operating under the organization. The individual groups are usually regional in their geographical scope and engage in multiple illicit activities. La Cosa Nostra (the Mafia), the Japanese Yakuza and outlaw motorcycle gangs such as the Hell's Angels or Bandidos are clear examples of a regional hierarchy structure (Lyman and Potter, 2007; UN, 2002).

Clustered hierarchy

The clustered hierarchy (Figure 2.3) is an association of organized crime groups with a single 'oversight' or 'governing' body that coordinates their activities and ventures. The individual crime groups are usually organized in standard structures, though this can vary dependant on the nature of the group, but most maintain a degree of autonomy from the other groups. An essential aspect of the clustered hierarchy is the concept that over time the cluster can develop its own identity. The clustered hierarchy generally results when individual groups agree to work together in a method of increasing profits by combining skill sets or regulating conflict between themselves. The risk of internal competition and exploitation, however, requires a stable balance to maintain the structure (UN, 2002; Lyman and Potter, 2007).

Core group

The core group (Figure 2.4) is a structure that consists of several individuals who form a tight and structured group to conduct business,

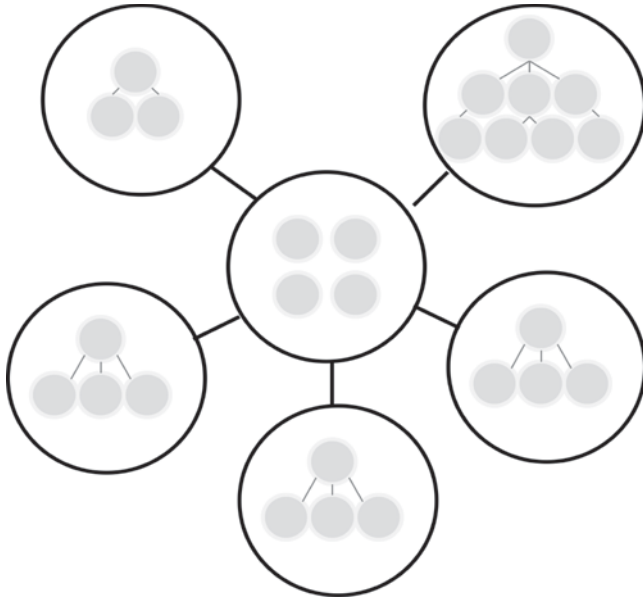


FIGURE 2.3 *Clustered hierarchy*
Source: UN, 2002.

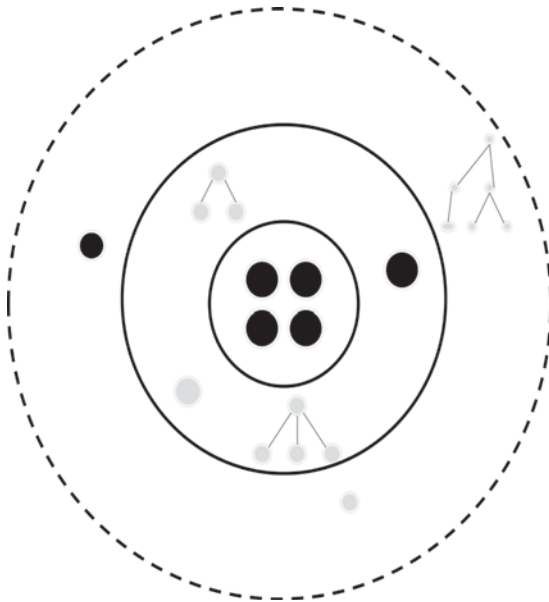


FIGURE 2.4 *Core group*
Source: UN, 2002.

surrounded by a loose structure of associate members or networks who are used to carry out business depending on the core group's intended criminal activities. Core groups generally limit their activities to one or only several ventures, with internal division of responsibilities within the group, acting in a more horizontal structure rather than hierarchical. Violence is not as prominent as the previous hierarchies, although can be used for internal discipline (Lyman and Potter, 2007; UN, 2002). There is usually little social identity and the group exists solely for the profit motivation of each individual, shifting their business activities to whichever venture generates the greatest profit, using their external associates to assist in carrying out their business. The core group is argued to be one of the most readily emerging forms of organized crime structure and, in some cases, is the result of continued law enforcement pressure and as part of the group's adaptation to more sophisticated means (Lyman and Potter, 2007; UN, 2002).

Criminal network

The criminal network (Figure 2.5) is the clearest example of the globalization of TOC and illustrates the measures that individuals and groups have taken to avoid detection and interference by LEAs (Cressey, 1997; Malkin, 2007). Criminal networks are the loosely organized, highly

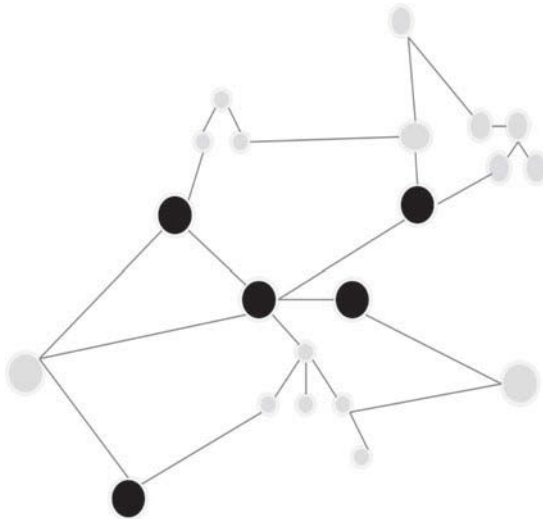


FIGURE 2.5 *Criminal network*
Source: UN, 2002.

adaptable, fluid networks of individuals that engage themselves in illicit activities with regularly shifting alliances (Lyman and Potter, 2007; UN, 2002; Cressey, 1997; Williams, 2001). The shape, organization and membership of the network continually changes dependent upon the participation of an individual and the attributes and skills required for the activities.

The networks are created and reformed in line with continuing criminal projects. The network lacks any social identity and avoids public exposure, with profit motivation and enterprise loyalty as their primary motivation. The lack of predefined identity and maintained structure makes it difficult for LEAs to infiltrate or dismantle the network. Whilst a number of key individuals may still exist, similar to the core group structure, their association with each other is usually distanced with minimal direct association. This again ensures that even if LEAs successfully target and prosecute one key individual the network will still remain connected and, despite possible inconvenience, will continue to operate (UN, 2002; Lyman and Potter, 2007). As noted by the Australian Crime Commission (ACC) in their *Annual Organised Crime Report* (2009), the organized crime groups that pose the most serious threat are those that are fluid and adaptable and resilient to interventions, rebuilding quickly after disruption. It is for these reasons that this form of criminal network is emerging as the new forefront of TOC structures (Lyman and Potter, 2007).

Lyman and Potter (2007) note that not all TOC groups fit specifically within the boundaries of these five structures. It is argued that the basic typologies provide an important understanding of how organizations can vary in structure, highlighting the difficulty that could be encountered in disrupting organizations using core group or criminal network typologies (Malkin, 2007). As identified by the UN (2002) and Lyman and Potter (2007), this is cause for concern with the increasing use of these typologies as the sophistication and complexity of organized crime develops.

Vulnerabilities of transnational organized crime

It is noted that there is minimal research on the weaknesses and vulnerabilities of TOC groups. If there had been a prevalence of research it would be expected that TOC would not be the serious societal threat

that it is. A review of the literature suggests that the focus is less about the vulnerabilities of criminal enterprises and more about the vulnerabilities of victims – be it individuals, groups or nations – and subsequent propositions as how to reduce these vulnerabilities. This reactive nature of law enforcement and government may, however, be hindering the ability to implement crime control strategies effectively. Following a target hardening of victim vulnerabilities, aided by the slow response time as problems are dealt with on a case-by-case basis, crime groups tend to shift their operational focus to new or easier victims or targets, rather than being discouraged from their illicit activities altogether (Abadinsky, 2009; Lyman and Potter, 2007; Cahill and Marshall, 2004). This is exemplified by the recent focus on money laundering and subsequent world reaction following the terrorist attacks of 11 September 2001 (9/11) and new insight into terrorist funding models. The international community has worked tirelessly to implement new anti-money laundering counter-measures and legislation. The issue, however, is that during the years it has taken to introduce these new measures criminal enterprises have developed more sophisticated and effective means to bypass these new counter-measures and continue money laundering undetected (Flood and Gasper, 2009).

Through an understanding of the structure of criminal enterprises it is possible to identify a core vulnerability that will only intensify as groups expand their areas of operation over greater distances and move towards more unstructured networks (Malkin, 2007). The need to communicate quickly, easily and effectively is a basic requirement for any business operating across large distances, either domestically or internationally. As such, for criminal enterprises – a business unto themselves, albeit illegitimate – the need to communicate their activities is just as important (Grabosky and Smith, 1998). It is no longer viable for criminals to conduct clandestine meetings in isolated locations to exchange products or information; they require instantaneous communication that spans the globe amongst their networks of contacts, and the very sophistication and complexity that dictates their business activities also makes them highly susceptible to high quality intelligence attacks.

Criminal enterprises require sources to supply their goods, access to markets and the ability to exploit systems related to their markets. They need proficient communication with their suppliers, conspirators and network members (Flood and Gasper, 2009). They need transport, finance and the services of the ‘middle man’. Whilst building

and sustaining their business they also need to build and sustain their reputation, all the while being able to manage risk – not just from law enforcement but also from criminal competitors and internal threats (Flood and Gasper, 2009).

The ability to understand how these stages work and penetrate the business operation is central to law enforcement's prospects for success (Flood and Gasper, 2009). Grabosky and Smith (1998) argue that the use of telecommunications by criminals is categorized into four basic methods:

- 1 Aids the capacity to coordinate and plan criminal activities.
- 2 Can be used for the marketing and distribution of their illicit services or products.
- 3 Instrumental in sustaining the organizational structure which supports the previous two functions.
- 4 Can be used to obstruct law enforcement investigations.

By identifying these contact and communication points LEAs can acquire vital information and subsequently develop intelligence to facilitate operational response strategies. Grabosky and Smith (1998) note a variety of communication strategies used by various criminal enterprises through the brief review of law enforcement operations and case studies.

For the most part criminals simply exploit existing communication devices for their own use. In 1995 following an operation conducted by the US Drug Enforcement Agency (DEA) on the Cali Cartel, a drug cartel based in the southern Columbian city of Cali, a multitude of communication devices were seized that highlighted methods used by the cartel to communicate. These included voice changers fitted to UHF radios so as to avoid identification during transmissions, video phones that allowed visual authentication of the caller and scrambling devices for internet connections (Grabosky and Smith, 1998). They also note pagers have been frequently used as a means of organizing payment and delivery of illicit products and also as a means of minimizing the amount of communication and voice contact between both seller and buyer (Grabosky and Smith, 1998). Despite this, these studies are of limited use for current research due to the significant advances in technology in the 15 years since Grabosky and Smith's work. The use of products such as pagers has declined significantly and has now been replaced by the prevalence of mobile phones, Smart Phones and Short Message Service

(SMS) text messages, electronic mail (email) and other online mediums such as message forums, instant chat services, Voice Over Internet Protocol (VoIP) telephony services (Jackson et al., 2007), and various social network mediums such as Twitter and Facebook.

Criminals have been identified through enforcement operations to utilize mobile phones that are programmed to send or receive from specific phone numbers only, reducing the identification and thus interception of a phone call by law enforcement. Criminals are also known to exploit the easy availability and poor identity checks of prepaid SIM (Subscriber Identity Module) cards for mobile phones, along with access to cheap handsets. This allows criminals to frequently change both the SIM and handset, again reducing the chances of detection, interception and limiting their links to other criminal counterparts (Waters, Ball and Dudgeon, 2008; Jackson et al., 2007). Through the use of the internet, criminals have access to a growing multitude of free and temporary email accounts that require no identification and can allow messages to be transmitted with relative anonymity (Waters, Ball and Dudgeon, 2008; Newnham and Bell, 2012; Dean, Bell and Newnham, 2012).

The growing availability of encryption devices also allows criminals to either encode whole messages or encode the messages within a particular attachment such as an image, document or link, otherwise known as steganography (Bakier, 2007). This is by design, so while a communication may be intercepted the message content itself can appear otherwise innocent. While 'off-the-shelf' products are readily available for use by criminals, they are also available to LEAs for decryption purposes (Jackson et al., 2007). To combat this criminal enterprises have been known to develop their own software and methods.

This has been particularly evident in Eastern European crime groups who are known for their specialization in cyber crime and recruitment of young computer programmers, whose skills are put to use developing new encryption techniques to disguise the crime group's communications (Abadinsky, 2009). Leyden (2009) and Willey (2009) report that the use of Skype, an encrypted VoIP telephony software, is being exploited by criminals within Italy as a means of counter-surveillance of 'normal' interception technology. Willey (2009) argues the possibility, however, that these claims by European LEAs is indeed 'smoke and mirrors' to provide criminals with a mistaken belief of Skype as a 'secure' communicative method. Despite this, Malkin (2007) notes that the primary issue with the literature available is that there is a distinct lack

of research that examines the social structures of criminal enterprises and the communication, both verbal and non-verbal, that occurs within criminal networks.

Much of the research that does exist focuses solely on the flow or path of the communication, rather than the 'how' and 'what' of the actual communication (Malkin, 2007). This again highlights another large gap in the literature surrounding the concepts of communication interception technology (CIT) and the ability to identify its effectiveness and successful integration into intelligence operations and investigations.

Legal response to transnational organized crime in Australia

Over the past decade Australia and other Commonwealth countries have introduced a variety of reforms to assist in the combat of transnational criminal activities occurring on and off shore (Hughes, 1999). Cornall (2005) and Irwin (2001) identify that policy and operational responses are two key facets required to challenge this societal threat. Consequently, administrative arrangements have strengthened the fight through the expansion of agreed extradition treaties, mutual assistance agreements, memorandums of understanding with neighbouring countries, and the establishment of international cooperation groups responsible for establishing laws, agreements and treaties (Cornall, 2005).

Since the 9/11 terror acts and the Bali Bombings of 12 October 2002, stringent legislation has been introduced to further the prevention of similar attacks occurring within Australia. These legislative measures have not only introduced definitions and offences for transnational criminal activities (based on the UN Convention Against Transnational Organised Crime) but have further assisted in combating these crimes. This has included an expansion of powers, such as the ability to seize and freeze assets identified as proceeds of criminal activities, and an increase of powers and responsibilities to law enforcement and intelligence agencies such as the Australian Federal Police (AFP) and the Australian Security Intelligence Organisation (ASIO) regarding investigations and arrests. Australia has also promoted their involvement with the Organisation for Economic Cooperation and Development (OECD) with attempts to ratify the Financial Action Task Force's (FATF's) 40 Money Laundering recommendations, and nine other special recommendations

against money laundering and terrorism financing (Cahill and Marshall, 2004).

Cornall (2005), Irwin (2001), Wardlaw and Boughton (2006) and Chalk and Rosenau (2004) all note attempts to increase knowledge sharing through the interweaving of law enforcement and intelligence agencies. This has included the creation of the ACC, which is equipped with coercive hearing powers, the National Threat Assessment Centre and the Transnational Crime Coordination Centre, along with the acknowledgement of the importance of including the private sector in intelligence sharing as a means of protecting crucial infrastructure as a major step in the right direction.

In addition to the policy responses, operational responses have been important in the fight against TOC. The extent of international deployment and operations occurring through the AFP has enhanced not only intelligence gathering but also diplomatic ties between nations, namely Indonesia, Papua New Guinea and those in the Pacific Islands. This is achieved through the construction of trust-based relationships through assistance provided by federal agents and diplomats (Cornall, 2005). Irwin (2001), however, goes further than the simple descriptive nature of Cornall's work noting the importance of other responses. Glenn, Gordon and Florescu (2008) argue that whilst Australia has instigated significant changes to recognize the growth of TOC, where 'transnational' underscores organized crime, the need for a comprehensive, integrated, global counter-strategy is required and, consequently, the response of a single nation is less than effective.

Legal responses to transnational organized crime in other commonwealth countries

New Zealand

New Zealand's (NZ's) current response to TOC is both domestic and international in scope (NZ Ministry of Justice, 2011). The NZ Government's response conforms to international obligations and best practices as a signatory to the UN Convention Against Transnational Crime (UNTOC). Further to this, NZ is also party to other multilateral treaties and is actively involved in international forums which continue to establish best practices relevant to combating TOC and official corruption – as is Australia. Evidence of this can be found in NZ's and

Australia's participation in the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, FATF and the Asia Pacific Group on Money Laundering (APGML), all concerned with anti-money laundering and countering financing of terrorism measures (NZ Ministry of Justice, 2011; Wardlaw and Boughton, 2006; Chalk and Rosenau, 2004).

Along with Australia, NZ co-sponsors the UN Transnational Organised Crime Threat Assessment for East Asia and the Pacific and provides legislative drafting assistance in order to address counter-terrorism counter-initiatives within the region. Both Australia and NZ support organized and transnational organized crime initiatives within regional groups such as the Asia Pacific Economic Community (APEC) and the Asia Regional Forum (ARF) and the Bali Process on people smuggling, human trafficking and related transnational crime (NZ Ministry of Justice, 2011).

NZ complies with and is party to two of the three UNTOC protocols which target specific areas of organized and transnational organized crime: Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; and the Protocol against the Smuggling of Migrants by Land, Sea and Air (NZ Ministry of Justice, 2011).

NZ's law enforcement and intelligence agencies share information about threats and approaches with counterparts in other countries through agency arrangements (Cornall, 2005; NZ Ministry of Justice, 2011). For example NZ is involved in arrangements with the United Kingdom (UK), Australia, Canada and the United States (US) in the Strategic Alliance Group comprising law enforcement bodies, and Border 5 comprising customs bodies and, most recently, the Attorney-General Quintet. Under the Quintet a Declaration of Understanding provides for greater dialogue in developing policy, legislative responses and criminal intelligence on organized crime, and closer cooperation on capacity building and training between the countries.

At the regional and domestic levels NZ has developed the Organised and Financial Crime Agency of New Zealand (OFCANZ) in order to respond to criminal groups which operate across police district boundaries, nationally and internationally. Regional-level agency intelligence is shared and regional-level responses to TOC and corruption are coordinated by the long-standing Combined Law Enforcement Group (CLAG) of agencies. The CLAG comprises a regional network for intelligence, enforcement and compliance officials mandated to coordinate, cooperate

and communicate across government to identify and disrupt criminal threats identified by member agencies. The CLAG has 20-member agencies, a national oversight body and a Secretariat (NZ Ministry of Justice, 2011).

In response to the threat posed by TOC through cyberspace, NZ has developed a National Cyber Security strategy that seeks to enhance security awareness, resilience and protection for individual citizens, nationally recognized key assets and critical infrastructure, and government information indices (NZ Ministry of Justice, 2011).

The Council of Europe Convention on Cybercrime (the European Convention) establishes best practice responses to cybercrime and argues in support of greater cooperation between countries that are party to the European Convention in prosecuting cybercrimes. NZ's legal and operational arrangements conform with many of the European Convention's provisions (CECC, 2011; NZ Ministry of Justice, 2011). The new *Search and Surveillance Act (2012)* will additionally provide for production orders for data and extend NZ's communication interception warrant system in line with the terms of the Convention. NZ's legislation pertaining to communication interception is discussed in detail in Chapter 6.

NZ remains proactive in its response to TOC and corruption; however, some issues remain unresolved. These include NZ achieving full compliance with the European Convention, and addressing judicial challenges to the recently enacted *Search and Surveillance Act (2012)*. It is expected that both initiatives will significantly enhance NZ's ability to expeditiously order the preservation of computer data, in particular traffic data, that exists in some stored form at a point in time to enable it to be obtained. Traffic data is defined under the European Convention as:

any data relating to a communication by means of a computer system...indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service. (CECC, 2011)

It should be noted that traffic data is distinct from the content data of the communication (CECC, 2011; NZ Ministry of Justice, 2011).

The terms of the European Convention would also require mutual legal recognition of certain intercept warrants and production and preservation orders issued by other countries for data from NZ. Full compliance with the European Convention would also improve NZ's ability to obtain data created or used to offend within NZ's legal jurisdiction but which is held in another country (CECC, 2011; NZ Ministry of Justice, 2011).

Canada

Home to some of the wealthiest organized crime groups in the world, namely the Canadian chapters of the Hells Angels OMG, Canada has responded by initiating anti-gang legislation to combat the threat posed by this and other elements of TOC (CISC, 2006). Further to the enactment of specific anti-crime legislation, the Canadian governments (both federal and provincial) created specific units to combat the threat posed by TOC.

In 1992 the British Columbia Provincial Government created the Coordinated Law Enforcement Unit (CLEU). CLEU was tasked to combat TOC at the provincial level. However, in developing the charter for the unit, legislators failed to include the investigation of drug trafficking in the unit's mandate. As a result, the effectiveness of the unit was challenged by opposition political parties and thus in 2000 the Organised Crime Agency of British Columbia (OCABC) was formed. Staffed with officers from all municipal police departments within the province, and supported by members from the national police service, the Royal Canadian Mounted Police (RCMP), OCABC was provided with a clearer operational mandate and sufficient funding and resources to target TOC and make a meaningful contribution to the intelligence holdings of the Criminal Intelligence Service of Canada (CISC). In 2005, following another change of government, OCABC was disbanded despite considerable success in disrupting TOC activities within the province of British Columbia, and the Combined Forces Special Enforcement Unit (CFSEU) was created and managed by the senior executives from the RCMP. Like its predecessor the CFSEU is authorized to conduct targeted investigations into TOC and to intercept communications where deemed necessary and appropriate following the issuance of a warrant under a judicial order.

CISC is the national criminal intelligence agency tasked with collecting, analysing and disseminating intelligence pertinent to the activities of transnational and organized crime in Canada. Through its national database, ACIS III, CISC prepares strategic intelligence documents such as the *National TOC Threat Assessment* for dissemination amongst the broader Canadian law enforcement and intelligence community (Coyne and Bell, 2011a, b). CISC is not empowered to conduct investigations but serves as a conduit for sharing intelligence on TOC between member agencies. CISC does not have authority to intercept communications.

This remains the domain of the RCMP and specialist units such as the CFSEU following the issuance of a warrant under judicial order.

The Canadian Security Intelligence Service (CSIS) is responsible for matters pertaining to national security and terrorist-related activities. Limited information is shared between CSIS and the law enforcement community through the RCMP–CSIS liaison function.

As a signatory to the UN Convention Against Transnational Organised Crime, Canada further supports anti-crime initiatives at the regional level. Like Australia, the UK and NZ, Canada is a signatory to two of the three UNTOC protocols which target specific areas of organized and transnational organized crime: Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; and the Protocol against the Smuggling of Migrants by Land, Sea and Air (CISC, 2011).

In 2010 the Canadian Government introduced legislation to broaden the powers of its LEAs. Referred to as the *Investigative Powers for the 21st Century Act*, the legislation places an emphasis on cybercrime and aims to provide police with the ability to collect and seize electronic data, and enable them to respond to an ever-evolving technological environment while protecting the human rights of persons in Canada, including their right to a reasonable expectation of privacy (Canadian Department of Justice, 2010).

The legislation also creates the legislative framework necessary for Canada to ratify the Council of Europe's Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime, and the Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. These are important multilateral treaties, which were signed by Canada in November 2001 and July 2005 respectively, and are the only instruments that provide for broad-based international cooperation for the investigation and prosecution of computer-related crimes (Calderoni, 2010; Department of Justice, 2010). This reflects the recognition that effective and evolving international assistance mechanisms are vital in combating the ever-growing threat of international criminality: transnational crime.

United Kingdom

The UK has been instrumental in the drafting of legislation in response to the threat posed by serious, organized and transnational crime. From

the drafting of legislation authorizing the formation of the Serious and Organised Crime Agency (SOCA UK), to providing support of UNTOC and FATF. As is the case with Australia and NZ, the UK is a signatory to two of the three UNTOC protocols which target specific areas of organized and transnational organized crime: Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; and the Protocol against the Smuggling of Migrants by Land, Sea and Air. The UK is also supportive of the Council of Europe Convention on Cybercrime.

The UK has legislated against organized crime at the local level and has provided significant powers (with equally significant oversight) to police and intelligence agencies to combat transnational crime, terrorism and official corruption. Under the *Regulation of Investigatory Powers Act* (RIPA, 2000) law enforcement intelligence agencies are afforded (amongst other things) the power to acquire communication including interception data.

Chapter summary

TOC is a diverse and complicated arena, costing global society in excess of US\$3 trillion annually – a figure that continues to grow (Borger, 2007). The current literature demonstrates that globalization has resulted in an increasing growth and sophistication of crime groups, as they take advantage of disappearing borders and greater profit markets. Whilst crime groups are vulnerable to detection and disruption because of their communications, LEAs need a method and framework that allows them to combat these crimes efficiently and successfully.

The next chapter examines the modern policing methodologies, their appropriateness in fighting TOC and their ability to effectively utilize technology that can exploit criminal communications.

3

Corruption

Abstract: *Corruption can occur in any environment – the police force and public service being no exception. This chapter looks specifically at police corruption, touching briefly on other forms of corruption such as that involving politicians and government employees. It considers the different forms of corruption, why and how corruption can occur and the theories surrounding it. The chapter introduces the concept of network analysis in the context of corruption investigations, presenting it as a powerful mechanism for understanding corruption networks and examining the notion of ‘dark’ networks – those that operate outside of public scrutiny. Identifying that network members rely on the reputations of others to find useful and reliable connections, and that brokers between groups are key to the network operation, communication interception technology (CIT) in particular is recognized as a valuable tool in identifying, disrupting and ultimately closing down dark networks.*

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

Corruption occurs when a person who is the agent of another person acts in a manner where they place their own interests ahead of those of their principle. Corruption can therefore occur in any circumstance – whether in the public or private sector – where someone acts as the agent of another person or group. However, when we discuss corruption we almost always look at the public sector. In this chapter we concentrate on that sector and, more specifically, corruption by police officers – who have been the most regular targets of corruption inquiries. Some reflections will then be made on the extension of these statements to corruption in other fields.

Like corruption in any environment, police corruption occurs when an officer knowingly acts or omits to fulfil his or her duty in order to obtain an advantage for themselves (Punch, 2009). It takes many forms and can alter depending on the circumstances and role the police officer finds themselves in. Police corruption can be: passive, where a police officer could be bribed by a person to ensure the continuance of their illicit activity; or proactive, through *predatory policing* where police approach criminals to extort money by providing protection (Gerber and Mendelson, 2008). Police corruption is more dangerous when it involves an organized network because the power and income of the group is greater than the sum of the income of individuals acting apart (Morselli and Tremblay, 2004). It is important to understand how corrupt police networks operate to be able to better identify and apprehend the targets of internal police investigations. As Warr has said in relation to the policing of delinquents: ‘it is difficult to imagine how investigators can develop, defend, or test general theories of delinquency without some knowledge of the organization and operation of delinquent groups’ (Warr, 1996, p. 12).

Police can commit corruption because they feel they are ostracized from the community they are protecting. This takes three forms (Lauchs and Merrington, 2012):

- 1 Lack of support to do their job properly due to inadequate laws of evidence.
- 2 Being undermined by the courts system who would reverse their good work.
- 3 Receiving worse treatment through noble cause corruption by the integrity services.

Forms of corruption

Public sector jobs are either ‘wet’, being ideal for corruption because they involve a high degree of discretion, or ‘dry’, that is, jobs which have no discretion (Heidenheimer and Johnston, 2002). Thus a uniformed officer on routine duties may rarely be exposed to opportunities of corruption compared to a plainclothes officer in a drug squad (Barker and Carter, 1991). Having said that, all operational police have the opportunity to exercise their discretion and therefore have wet jobs.

There is still a hierarchy of police corruption. The 1972 Knapp Commission in New York described two types of police corruption:

Corrupt policemen have been described as falling into two basic categories: ‘meat-eaters’ and ‘grass-eaters.’ As the names might suggest, meat-eaters are those policeman who ... aggressively misuse their police powers for personal gain. The grass-eaters simply accept the payoffs that the happenstances of police work throw their way. Although the meat-eaters get the huge payoffs that make the headlines, they represent a small percentage of all corrupt policemen. The truth is the vast majority of policemen on the take don’t deal in huge amounts of graft. (Knapp, 1972, p. 4)

The majority, grass-eaters, make small-scale corruption ‘respectable’ through publicly accepted gifts such as free coffee or fast food discounts. Even those who would refuse such gifts still participate in the ‘code of silence’ that brands anyone who exposes corruption a traitor (Knapp, 1972).

There are different types of meat-eating or proactive corruption. At the lowest level of severity is *occupational deviance*, when rules are bent to an employee’s advantage, such as sleeping on the job, pilfering and work avoidance (Punch, 2009). Next are *police crimes* or crimes committed by police officers including *process corruption*: the manipulation of the justice system, usually to ensure a conviction. Most process corruption is ‘noble cause’, which will be discussed in more detail below. Finally, the most serious form of police corruption are corrupt individuals or networks involved in stealing and extorting money from the illicit economy or innocent victims. Networks usually operate through the social networks between underworld organized crime and upper-world actors like politicians and police (Block, 1994; Blok, 1974; McIllwain, 1999). Thus we could characterize corrupt police as upper-world actors selling protection – an extortion racket – to the underworld (Skaperdas, 2001).

Police are a subculture in society (Sewell, 1999); they are socially excluded from the community and make friendships with other police. Their work is dangerous, so they risk their lives for the community, but their reward is unpopularity and stigmatization. The central elements of police culture are having a sense of mission, solidarity, danger and sacrifice, cynicism, the rule of silence, rough justice and just desserts, social isolation and routinization (Chan, 1999; Punch, 2009). Police see the 'brotherhood' as a central part of their life and identity.

Police corruption is often excused as being one or a few 'bad apples' within an organization. But this view is being replaced by a notion of a 'bad barrel' after the record number of large corruption networks discovered over the last few decades. A pattern of corrupt behaviour becomes ingrained in a police pattern of socialization (Barker and Carter, 1991); the corruption may begin with a few individuals but expands as more and more officers become involved as a result of the need to fit in with the brotherhood (Porter and Warrender, 2009). Thus 'police culture fosters corruption' (Punch, 2009, p. 19). Part of this police culture is the *code of silence*: never informing on another police or even lying for another officer (Kleinig, 1996). An officer who breaks this code can suffer threats, ostracism, damage to personal property, malicious rumour and even violence (Reiner, 1992). The code of silence hinders the reporting of misconduct and corruption (Dean, Bell and Lauchs, 2010; Carter 1997). Essentially it must be accepted that the pressure of fitting in can push someone down the self-rationalizing slippery slope (Baumeister and Leary, 1995; Punch, 2009).

Another aspect of this culture is leadership. A police officer's incentives or rewards depend on the incentives provided by the leaders in the organization (Myerson, 2011). Some officers have been more inclined to escalate their career prospects by engaging in corrupt acts in the hope that they will be rewarded by their superiors. Thus there is a *moral hazard* problem at the top leadership as agents must trust that their superiors will judge their performance in a positive manner and will reward them accordingly (Alchian and Demsetz, 1972).

Noble cause corruption occurs when a person tries to produce a just outcome through unjust methods, for example police manipulating evidence to ensure a conviction of a known offender (Punch, 2009). Unlike monetary corruption, such as bribery, it is seen as a positive act by perpetrators (Lauchs and Merrington, 2012). Nonetheless, this type of corruption still leads to injustice through the prejudging of an accused

by the investigators and the inability of this accused to have a fair trial. Noble cause corruption demonstrates the moral hazard of seeking convictions at all costs. Long-term rewards or incentives for not abusing police power must outweigh the benefits gained from engaging in corrupt activities (Myerson, 2011). In the case of noble cause corruption, police are breaking the law to enforce it.

Police may participate in noble cause corruption even if they would refuse to take a bribe (Fitzgerald, 1989; Herbert and Gilling, 2004). Thus the reward they sought was job satisfaction. Police have noted that they have no need for noble cause corruption when they are given the means to obtain conclusive evidence through better powers and equipment. But police have to accept that they may suffer from confirmation bias (Nickerson, 1998); they may convince themselves of someone's guilt, pursue charges and 'load up' a person under an entirely incorrect presumption (Lauchs and Merrington, 2012).

Theories of corruption

As noted above, police culture can drive compliance. According to social identity theory a group member usually takes on the beliefs and values of the group, in part through the natural desire to be liked (Brown and Abrams, 2003) and not cause social friction (Coady, 1996). Group members emulate the ethics of their peers and prefer them, even over those of direct authority figures (Granitz and Ward, 2001). Consequently, a person feels they will 'join in' and act unethically rather than letting their friends down (Beck, 1999; Grossman, 1995; Weber, Kurke, and Pentico, 2003).

Police can have a tendency to see themselves as the 'white hats' or good guys in the community. As such they are susceptible to the two types of 'moral distance': *punishment justification* (showing the person is guilty of a punishable/vengeful act), and the *legal affirmation* of legitimizing acting against the punishable offender (Grossman, 1995). While this is literally true there is a danger that entire groups, rather than offending individuals, are depicted as 'malicious, alien forces intruding on the world of well-meaning, unsuspecting, virtuous people' (Baumeister, 1997, p. 89). These concepts are especially useful in justifying noble cause corruption.

People can also partake in corruption through changes in their lifestyle. According to life-course criminality studies of offenders, a

criminal career begins with offending as a youth and ends with either desistance from crime or the continuation into offending as an adult. Crime reaches a peak between the ages of 15 and 17 and then usually declines (Gottfredson and Hirschi, 1990). According to Moffitt (Moffitt, 1997; Nagin, Farrington, and Moffitt, 1995), offenders are either *adolescence limited offenders* (who confine their offending to adolescence) or *life-course persistent offenders* (who remain active in crime throughout their lives). These studies contain three presumptions:

- ▶ adult offending is a progression from offending as a youth
- ▶ offenders possess *latent traits*, that is, persistent offending occurs because something is wrong with the offender, such as low self-control or weak ties with the community (Caspi et al., 1994; Gottfredson and Hirschi, 1990; Nagin and Farrington, 1992)
- ▶ an offender will reduce or cease offending once they have a job or are married and, thus, are part of the community (Gottfredson and Hirschi, 1990; Laub and Sampson, 2003; Sampson, Laub, and Wimer, 2006).

However, most white-collar criminals do not have prior criminal records as juveniles before they commence offending as adults (Piquero and Benson, 2004, p. 156). They are *adult onset* offenders:

- ▶ they commence offending in their adult years, having never offended as children
- ▶ they generally do not grow up in socially disadvantaged environments, thus they grow up integrated into the community rather than being marginalized (Piquero and Benson, 2004)
- ▶ offending in white-collar crime takes place late in life, when life-course studies say offending should taper off (Piquero and Benson, 2004)
- ▶ many white-collar offenders are married and employed, thus socially integrated – circumstances which life-course criminality suggests should reduce or cease offending.

Like white-collar criminals, police officers fall outside of the standard life-course criminality model. They could not enter the police force with a prior criminal record. They are no more likely than anyone else to grow up in a socially disadvantaged environment. Most are married and all are employed at the core of social control, thus they have strong social ties. At least in Western countries police are reasonably well paid

and there are no indications of financial hardship or trauma to motivate their criminal activity. Under the life-course criminality thesis police offending should not occur.

White-collar crime seems to be driven by life events combined with the opportunity to commit crimes that did not exist earlier in the life of the offender. This is similar to the *social opportunity structure* of organized criminals (Kleemans and de Poot, 2008). According to Dutch studies there are a number of indicators of organized crime activity (Kleemans and de Poot, 2008):

- ▶ organized criminals do not commence offending until they have social ties to give them access to profitable criminal opportunities
- ▶ the complex nature of offending requires that they have suitable co-offenders available to them before they can commit their crimes
- ▶ they commence offending through an opportunity that arises from their legitimate occupation rather than proactively seeking involvement with the illicit community (Kleemans and de Poot, 2008).

Thus adult onset offenders in the Dutch studies have a propensity to commit crime but do not do so until they enter a scenario that makes criminal activity both possible and profitable.

Dutch studies found that offenders shared characteristics in their legitimate jobs:

- ▶ their job role kept them mobile in the community
- ▶ they operated independently
- ▶ they had social jobs that allowed for interaction with potential co-offenders, in other words they had ‘embeddedness of criminal activity in work relations’ (Kleemans and Van de Bunt, 2008, p. 189).

Significantly, they also found that offenders developed a strong culture and maintained a ‘wall of silence’ (Kleemans and Van de Bunt, 2008).

The previous discussion of police culture matches many of the findings of the Dutch studies. Police have many opportunities to participate in illicit activity in the course of their normal work. They tend to be mobile in the community, work fairly independently and work closely with the criminal community. Given that police corruption is an example of adult onset offending we should use this information to help target potential corrupt activity.

Neutralization

Another association with white-collar crime is the reliance on *neutralization*, or rationalizing one's actions to justify illicit behaviour (Sykes and Matza, 1957). Mars (1994) describes neutralization as rituals which allow a person to separate their persona into one which is compliant with social norms as an employee or businessperson and another which allows covert offending. These two personalities can operate independently. This division can be supported by organizational culture; often a person is simply replicating a split personality being operated by, or in collusion with, all their co-workers. These rituals of neutralization include denial that injury was actually caused to anyone else, denial of personal responsibility for the negative outcomes from their actions and/or a higher justification for the action which overrides the otherwise negative social norms that apply.

Corruption networks

Social networks form naturally through social interaction when there are ongoing exchanges from which trust, mutuality and reciprocity are developed. The network members form common norms maintained through peer pressure, social approval and sanction (stigma), which tends to bind individuals to a collective unit or a form of 'social organization' (Kooiman, 1993). Social networks have been studied extensively in business and society (Castells, 1996). However, as a number of theorists have stressed (O'Toole and Meier, 2004; Raab and Milward, 2003; Milward and Raab, 2006), networks do not always function in the public interest and exist in the illicit economy and underground criminal community. Granovetter (1992, p. 45) points out that networks can create their own norms at odds with the outside world to the point where they become a 'law unto themselves', and see illegal activities as justifiable and use the group structure and culture to protect their illicit activity. Thus, Raab and Milward (2003, p. 5) argue that networks can possess either 'bright' or 'dark' properties. They can be 'dark' when they are both covert and illegal as opposed to bright networks which operate legally in public view. Bright networks can also have a dark side, where the network achievements can come at the cost of other individuals or groups (Portes, 1997; Keast and Brown, 2002; O'Toole and Meier, 2004;

Raab and Milward, 2003). However, this chapter focuses on the dark, criminal networks.

Criminal, drug trafficking, terrorist and corrupt police networks are dark. Dark networks exhibit varying degrees of 'darkness.' For example, at the darkest end of the spectrum would be a paedophile network which wishes to operate completely outside the gaze of the public. Slightly less dark is a drug dealing network which operates outside the observation of the general public and law enforcement, yet still needs to be found by customers. A terrorist network thrives on publicity of its cause and actions but its membership and management are cloaked in secrecy. A police corruption network falls to the darker range of the scale. It exists secretly within a public agency, the police force, yet it strives to keep its operations completely hidden from view while disguising the illicit operations of the people who pay bribes for its service.

Studying social networks is particularly useful for understanding corruption networks. There is an increasing amount of research into organized crime networks (Morselli, 2009). Most of this relates to how the network is structured and the relationship types within the structure, such as the role of *brokers*, the entrepreneurs of the illicit economy who bridge the gaps between different networks (Morselli, 2001; Coles, 2001; Kaza, Daning and Hsinchun, 2007).

Police corruption networks are dark networks:

- ▶ They rely on the informal relationships that arise from membership of the police force rather than the official hierarchy of the force or its operational systems. The corrupt network is built on an *ad hoc* basis, based on close and clandestine relationships.
- ▶ Corrupt officers rely on their guise as the force and their relationships to, and positions within, the formal hierarchy and system to provide resources, opportunity and power to exploit those outside the system. For example, a corrupt officer can travel within the criminal world as a police officer and use their police powers as coercive tools and the agency's resources to support their corrupt activities.
- ▶ Police culture is known for rules of silence, solidarity, cynicism and exclusivity (Chan, 1999; Punch, 2009). The survival of the dark network relies in part on its connection to the police subculture of silence that privileges loyalty over integrity.

Networks can build resilience – the capacity to survive environmental change and direct attack – into their processes and structures to protect themselves against change. For example, the resilience of an organized crime group is its ability to continue its operations through a changing market and the attacks of both competitors and police. Usually criminal networks survive by staying out of sight and reduce their visibility either through small size or looser structures (Bouchard, 2007). Visibility to the community may not be a weakness in itself but it increases the likelihood of investigation. Visibility can occur in two ways:

- 1 A large, formal network will be more visible to outsiders than a small, loose network.
- 2 A central person in the network, someone with many connections and power, will be more visible than someone associated with a smaller range of activity.

Dark networks must follow certain steps to establish the network (Milward and Raab, 2003):

- 1 They must find enough people for the network.
- 2 They must train their members.
- 3 There must be an external driver – a demand – for the creation of the network such as the need to provide an illicit service.
- 4 The network then grows as new members are encouraged to join.

According to Williams (2001) some networks defend themselves by developing buffers at the periphery to protect the core from police investigation. The low-ranked members do the high-profile criminal work whilst the core members keep such activity at arm's length to ensure deniability of any criminal action and to reduce their visibility to observers outside the network. Thus the network leadership may not be at the core. Carley, Lee and Krackhardt (2002) demonstrate that the leaders may not have the most contacts in the network; a leader may only communicate with one lieutenant who then interacts with agents and allies. In such a group the leader is protected by the more central decoy should law enforcement make assumptions about targeting group members based on centrality. This is the style of operation which is targeted by the Racketeer Influenced and Corrupt Organizations (RICO) legislation (Williams, 2001). A network may also be compartmentalized, like Al Qaida, so that the loss of one cell does not bring down the entire network.

Networks can also be resilient through a system of redundancy where removing one person may not destroy the network if that person can be replaced by a new person equipped to fill that role (Carley et al., 2002).

There are three indicators of destabilization:

- 1 A reduction in the rate of information flow in the network.
- 2 A failure/destruction or significant slowing down of the decision-making process.
- 3 A reduction in operational effectiveness – the ability to conduct its tasks (Carley et al., 2002).

That disruption can occur through law enforcement and the network must adapt. Milward and Raab identified three alternative criteria of resilience (Carley et al., 2002):

- 1 Members need to have character traits that support the network.
- 2 Members have to be able to trust each other.
- 3 The network is more resilient if it has *connectivity robustness*: the ability to respond to and recover from losses of critical people.

Bouchard (2007) used environmental studies of resilience to develop a list of characteristics which are useful in determining network resilience: *vulnerability* – the likelihood of damage from a specific type of attack; *elasticity* – the system's ability to return to its original state after taking damage; and the network's *adaptive capacity* – its ability to change to reduce its vulnerability. We can therefore conclude that resilient dark networks are not large, so they avoid attention, and have a low centrality (defined by Keast et al. (2011) as the degree to which network activity is centred on a few individuals).

Reputation

Trust is essential for networks to work effectively and can only be measured by reputation. Large networks are made up of a heterogeneous collection of small groups of homogenous members. The small homogenous groups are *closed networks* of people with strong relationships who share the same interest and the same information (Burt, 2005). Members share information about the reputation of other members and group members' expectations of the person's future performance based on his or her past performance within the group. Also, a good reputation is built by emulating behaviour that reflects the group's norms; norms which are built

up over the social history of the group. If a member of the group does not know a potential working partner they can obtain a reliable assessment of the person's trustworthiness, work ethic and commitment to the group's shared values by seeking the opinions of other group members (von Lampe, 2004). Thus gossip within a network allows a person to obtain a sufficient assessment of another group member's reputation to decide whether they are trustworthy.

Trust is reliant on having a good reputation and the network success relies on trust (Burt, 2005). This is especially important to underworld operators as criminals need to avoid conflict with their illicit partners because they do not have recourse to the mainstream legal system to enforce contracts or otherwise seek legal arbitration (Haller, 1990; Morselli, 2001). Reuter and Haaga (1989, p. 36) found that being "a good businessman" was a term of praise, occasionally contrasted with excessively flamboyant and unstable characters, heavy users, and addicts, who would lose track of their accounts, miss appointments, and dip into their inventories.' Thus trust, as communicated by a good reputation, is a desirable component of a successful illicit career.

A police agency is also a trust-based organization in which members build trust by working together in dangerous and even life-threatening circumstances that weed out the untrustworthy. Groups may even develop their own criteria for trust; for example the Australian New South Wales Commonwealth Investigations Branch (CIB) mantra was 'you never trust a man that doesn't drink' (Padraic, 2005, p. 19). The success of a new member of a squad may depend on participation in corruption; they will not be trusted unless they can develop a reputation for participation in graft and reliability to follow the code of silence. An untrusted member of the squad can suffer marginalization (Caccioloa, 2009; Jones and Carlson, 2004). With the prospect of belonging and gaining a highly regarded reputation and therefore trust from the fellow corrupt officers, it must be noted how far this viewpoint could potentially push an individual into attaining and retaining membership.

Brokerage

Activity in networks depends on locations/relations of players within the networks more than the personalities of the members of the network (Burt, 1992). Groups are connected by individuals who communicate and have relationships with members of more than one group. These *brokers* are in a position to pass information, arbitrate disputes and negotiate

cooperation between the groups. For example, a broker in a police corruption network would link illicit operators with police and channel the demand for protection from law enforcement and its supply from a covert group within the police. Very importantly, in dark networks the broker is able to communicate reputations (Burt, 2005). Also, dark network participants need to communicate covertly that they can be trusted to keep the group's secrets and that they have the necessary skills the group needs (Gambetta, 2009). This places the broker in a position of significant power as a controller of knowledge and also a position of leverage in being able to play off his exclusive connections. However, this is also a point of vulnerability for a network as the loss of a broker with exclusive knowledge can mean that the network no longer functions. Also, the broker becomes an important target for policing agencies wishing to both disrupt a network and obtain access to the exclusive knowledge held by the broker.

Police corruption networks

It would be reasonable to assume that the structure of the police organization directly affects the career path of a corrupt police officer. But Lauchs et al. (2011) established that, at least in one network, there was no relationship between agency hierarchy and authority within the corruption network.

According to Reuter and Haaga (1989) capital of a criminal enterprise consists of the inventory in hand (because of the fast turn-over of transactions) and the goodwill of the entrepreneur. In their study of the drug trafficking industry they said that resilience was not necessary. These findings do not apply to police; they have a monopoly over policing powers with no competition other than that provided by other police. This monopoly is permanent even though the individuals involved change over time. Also, the police are geographically bound; that is, they cannot extend their power beyond their operational jurisdiction. Thus, while criminals are flexible, ephemeral and mobile, police are fixed in a hierarchy, resilient and restrained to a locale.

Corruption operates in layers: the illicit operators seeking protection, the vice police who can provide that protection, and the senior police who can protect the corrupt police. Thus there are multiple opportunities for brokerage (Lauchs, 2012).

Corrupt networks are very hard to identify and infiltrate. An example of a closed network is the corruption network known as the *Joke*, which operated in the Queensland Licensing Branch, and which was investigated as part of the Fitzgerald Inquiry into police corruption in Queensland, Australia, in the 1980s. This network operated for at least four decades providing protection to illegal gambling and bookmaking operations. Members came and went from the network over its life, but the network retained an internal culture which ensured its continued operation. The members shared values about the nature of their illegal activity, the manner of distribution of bribes and the need to provide mutual support. New members entered the network through trusted connections and had to build their own reputation within the network (Lauchs and Staines, 2012).

So what can we learn about police culture and corruption which can help us in the investigation of corruption?

- 1 Anti-corruption agencies should extend their gaze beyond uniformed officers to those they socialize with and/or used to serve with who can broker arrangements with illegal operators.
- 2 A person with a reputation for reliable corrupt activity will develop connections to other corrupt actors.
- 3 Criminal brokers are looking for opportunities for monopolies so we should uncover the people who control those monopolies, both within and outside of government agencies.
- 4 Immobility caused by the geographic boundaries of police operations has the potential to make corrupt police more vulnerable to detection.

Corruption in other fields

While police corruption has received the most attention both in public debate and in this chapter, it is not the only type of corruption that takes place. Corruption can also occur in any area of public service and also in the private sector, although the latter is more generally discussed as white-collar crime (Sutherland, 1949). Corruption is a form of white-collar crime but both issues tend to be separately addressed in research. Corruption in the public sector can be broken into two areas: corruption by politicians and corruption by government employees. Both types take slightly different forms in practice.

Corruption by politicians relates to their role as agents of the voting public. They are charged with representing the public in parliamentary bodies and, in the Westminster system, carrying out the executive functions of government as ministers. As such their potential for corruption involves the sale of favours for decisions and patronage. Under a Westminster system the non-ministerial members of parliament have limited power. They may lobby for an idea and vote in parliament but they are not 'decision-makers' per se. In nations like Australia and New Zealand (NZ) the strength of *party discipline* (the necessity to vote in accordance with the party line) further restricts the ability of backbenchers to make decisions. Similarly, they do not have the ability to appoint people to positions in the government (a power limited to the ministerial ranks) so they do not have extensive powers of patronage. They can only obtain these powers in the horse-trading of political manoeuvring within their party ranks. Therefore, backbenchers do not have much that they can sell in the illicit market for corruption.

Conversely, ministers are in the opposite position. They are decision-makers independent of parliament, often with exclusive power to make decisions under pieces of legislation that belong to their portfolio. These decisions can be as mundane as registering an insect as a pest, up to awarding multi-million dollar contracts. They also have the power of patronage, being able to appoint to positions at many levels of government within their portfolio. This can include government employees within a department, to heads of independent agencies and government boards. Thus ministers are quite marketable.

In a presidential system the power of individuals is different. Individual members of Congress are not bound by party discipline, giving them much more marketable status. They also have access to a strong independent committee positions that can provide further opportunities to influence policy outcomes. However, the most power is held by the executive as president or, at a state level, governor. As an example, Huey Long was Governor of Louisiana from 1929 to 1932. In that short period he developed a system of graft through which he had total control over government appointments and decision-making to a totalitarian degree. He also 'milked' the public and private sectors for many millions of dollars. Long acted like an organized crime figure, extorting outcomes rather than simply selling an illicit service (Folsom, 2010).

Government employees can also sell their services. Many public officials have exclusive decision-making or decision-influencing powers,

very similar to those of police officers. The bureaucracy is set up to intervene in public affairs and the 'red tape' is designed to act as a barrier to progress, so that action cannot be taken until government scrutiny has occurred. However, this red tape also provides an opportunity for corruption (Guriev, 2004). Any officer with an inspection role, whether it be health inspection, building approvals or any other form of small-scale approval at a community level is a small target and in an easy position to extort or agree to graft. A person such as a parking inspector generally works independently with limited supervision. There is no record of them failing to make a decision, such as the failure to book an illegally parked vehicle – thus they have a power they can sell. Similar activity can take place at any low-level decision-making position (Bertrand et al., 2007). At higher levels of decision-making there are greater levels of accountability and there is also a link between the scrutiny of a free press and the reduction of corruption (Brunetti and Weder, 2003). But this has not stopped the occurrence of corruption; it just makes the operation of a corrupt practice riskier. However, corruption becomes easier when supervision is lax and when the payoffs are high. Local government areas around the world tend to receive far less media attention than either state/provincial governments or national governments. As such, they have the potential to be able to act in an illicit manner with greater chance of success. They also combine decision-making powers which can enrich members of the private sector, for example approvals for buildings and other construction (ICAC, 2008).

The earlier discussions about networks of corruption still apply to the government sector. The level of networks varies with the circumstances of the decision-making and the necessity for coordination. A single officer working on his own could take routine payments without the need for an intermediary: 'taking the pad' (Punch, 2009). Conversely, it may be necessary to share money with fellow officers and supervisors to ensure the individual is protected. In some cases, independent brokers work between the public and the bureaucrats to arrange graft. They have the connections to known corrupt officials that the public do not, thus they can act as a service provider by selling the services of the officials who protect themselves by not directly dealing with the public. These brokers can also sell their skill in graft by not only ensuring provision of an illicit decision but doing so in a much more timely manner than a member of the public could achieve on their own (Bertrand et al., 2007).

At the level of high-political office, politicians, like Huey Long, can use their power of patronage to build a mutually supporting network of corrupt officials. They can appoint compatriots to key positions to ensure that there is no independent scrutiny and that there is no avenue of redress for those aggrieved by the corruption. Politicians have the added advantage of being able to sell a service to the media. The 4th Estate, as the independent media are known to, relies on politicians for information when preparing stories about politics. Politicians can trade this information for support both licit and illicit. Modern politicians also have media advisors who are paid significantly more than members of the media working for news agencies. The patronage of appointment to these positions can be a great temptation for an ambitious reporter working in political journalism. At a more strategic level, the Fitzgerald Inquiry noted the undue influence the Queensland Government could have over the local press through the decision of which outlet to place government advertising. This very lucrative income source can be used to leverage positive reporting about government activity (Fitzgerald, 1989).

Chapter summary

Corruption can occur in any environment – the police force and public service being no exception. This chapter looked specifically at police corruption, touching on other forms of corruption such as corruption by politicians and government employees, considering the different forms of corruption and why and how corruption can occur and the theories surrounding it. An important aspect of corruption is that it usually occurs within a supportive culture. This culture validates the otherwise illegal activity and provides a rationalization that alleviates the guilt of new members/participants. Police forces are marginalized from society and develop a culture based on their exclusion from the mainstream; an ‘us versus them’ culture. One aspect of this culture can cushion police officers from the normalizing influences of society and allow them to cause harm to the community, through corrupt behaviour, without the social restraints that would apply to other professions. This is exacerbated by the police career path matching the characteristics of adult onset offending: an ability to work relatively unsupervised and mix with negative influences within the community.

Network analysis is a powerful mechanism for understanding corruption networks. As such, this chapter examined the notion of 'dark' networks and police corruption networks specifically. Networks that operate outside of public scrutiny – dark networks – have benefits and disadvantages that shape their structure. Their clandestine operation provides some protection from investigation, but the same secretive behaviour makes it difficult for the group to operate efficiently. Knowledge can only be passed through trusted hands and members rely on the reputations of others to find useful and reliable connections. Brokers between groups are key to the network operation. They have the power of exclusive knowledge, but the retention of that exclusivity makes the network vulnerable should they be removed, and also makes them useful targets for law enforcement who want to disrupt the network.

The following chapter investigates the various policing methodologies used in the context of TOC and corruption.

4

Policing Methodologies

Abstract: *This chapter reviews the current policing systems, processes and practices that underpin both tactical and strategic responses to transnational organized crime (TOC) by contemporary and progressive law enforcement agencies. It shows that whilst the methodologies of traditional, problem-orientated, community and computer statistics policing possess their own unique strengths, they all lack the ability to effectively combat TOC. Reviewing the literature, the chapter illustrates that the proactive nature of intelligence-led policing (ILP) is the most beneficial framework that can fight criminal enterprises and support communication interception technology (CIT).*

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

Models of policing

Integral to the success of any law enforcement agency (LEA) is their grounding within a methodology that guides their operating parameters, capabilities and strategies to effectively combat and reduce criminal activity. In an ever changing world driven by a media-fuelled obsession of demanding best practice in crime reduction, policing methodologies have developed into their own research niche as attempts to develop a 'perfect solution' come and go. Ratcliffe (2008a, b) and Weisburd and Eck (2004) contend that the primary methodologies of LEAs can be broken into five models: *Traditional Policing*, *Community-Orientated Policing*, *Problem-Orientated Policing*, *Computer Statistics* and *Intelligence-led Policing*.

These five models each have their own distinct concepts of strategic goals and possess their own strengths and weaknesses. This chapter examines these approaches and identifies the current development of Intelligence-Led Policing (ILP) as the methodology of choice for the 21st century.

Traditional model

Weisburd and Eck (2004, p. 44) argue that the traditional model of policing can be seen as a 'one size fits all' arsenal of reactive strategies to suppress crime regardless of the nature, level or other variations of crime within the jurisdiction. These strategies include rapid response to callouts, random community patrols, generally applied follow-up investigations and occasional intensive enforcement and arrest policies (Weisburd and Eck, 2004). This notion is supported by Eck and Rosenbaum (1994) and Conser et al. (2005) who argue that traditional policing has four primary functions: to control crime, provide immediate response, arrest and serve justice, and provide 'non-emergency' services. These functions mimic the ideals put forward by Weisburd and Eck (2004) in that the model relies solely on law enforcement powers to prevent crime (Conser et al., 2005; Eck and Rosenbaum, 1994). Subsequently, Goldstein (1987) and Ratcliffe (2008b) both argue that the primary drawback with this methodology is that this 'enforcing the law' attitude results in a distinct ineffectiveness in promoting long-term crime control, arguably because of its use as a reactive tactic rather than a proactive strategy (Ratcliffe, 2008a; Goldstein, 1987).

It should be noted, however, that the literature presenting arguments made against the methodology contain a source of bias, resulting from their primary objective to provide support for an alternate policing methodology, with Ratcliffe (2008b) promoting ILP and Goldstein (Goldstein, 1987) both community-orientated and problem-orientated policing. There is also a distinct lack of empirical evidence or explanation supporting the reasoning for successes of the traditional model. Indeed Weisburd and Eck (2004) through their own research have found there is a significant lack of evidence to support any of the notions of traditional policing effectiveness, and that which does exist is weak at best.

Community-orientated policing

Community-orientated policing, or COP, is grounded in the notion that through community interaction and support, crime and fear of crime can be controlled. Police act in a role as a facilitator within the community as they establish a balance between police duties and community responsibilities. Contact with the community as a means of establishing why crime is occurring, rather than a simple response to calls for service, is promoted as a fundamental purpose of COP (Goldstein, 1987). Through this use of involvement and report, agencies can alter their priorities and direct their responses to issues and problems identified by the community. Ratcliffe (2008b) claims that, whilst rarely articulated, the primary purpose of community policing, however, is to increase police legitimacy in neighbourhoods that have lost confidence with police. Through the increase of police legitimacy and subsequent community satisfaction, theoretically there can be a decrease in crime (Ratcliffe, 2008b). In their own review of COP research, however, Adams, Rohe and Arcury (2002) and Eck and Rosenbaum (1994) argue that there is a clear lack of clarity as to what exactly passes as community policing, and that the benefits and impact COP has on crime (in contrast to traditional policing) have been mixed during research evaluation. To further impair the reputation of COP as a viable policing methodology there is significant disagreement as to what actually constitutes and defines community policing; this makes evaluation difficult but adoption and proclaimed use by an LEA easy (Ratcliffe, 2008b).

Problem-orientated policing

Problem-orientated policing, or POP, is an approach that involves the examination and analysis of clustered incidents to determine an underlying cause of crime and implement a strategy specifically designed to address the problem. POP focuses on the use of new preventative responses that specifically engages the wider community when there is potential for their contribution to result in the reduction of the problem (Goldstein, 1990; Centre for Problem Oriented Policing, 2009). This approach is similar to the strategy of situational crime prevention, as ideally the ultimate goal of policing is not simply to enforce the law but to deal with identified problems effectively by preventing them from occurring or reoccurring in the first place (Goldstein in Scott, 2000). However, as a policing methodology, and unlike situational crime prevention, POP guides the whole doctrine of an LEA in crime prevention, rather than as a singular part of an LEA's policy.

John and Maguire (2003) and Braga and Weisburd (2006) note though that there is a clear structural difficulty in implementing POP and transforming it from rhetoric to a practical approach, with an evaluation of numerous studies indicating a disconnect from POP's articulated aims and the realistic practices of LEAs.

Computer statistics

Computer statistics, or COMPSTAT, is a management philosophy that utilizes geographical information systems for crime mapping to identify problems and approach crime reduction and resource management in line with the relevant problem areas. Accountability of police management is addressed by their requirement to demonstrate a reduction of crime in their relevant area, and appropriately justify any increases. Due to the primary focus on statistics, critics such as Weisburd et al. (2003) and Manning (2005) have claimed that the effectiveness of any COMPSTAT programme is minimal due to the ability to misconstrue data to read in a positive light, and the subsequent ability to greatly under-represent crime. Criticism further extends with Manning (2005) claiming that COMPSTAT goes so far as to regenerate and reinforce the hierarchical and methodological guides of the traditional policing

method, a structure that COMPSTAT along with COP and POP were designed to eradicate.

A common factor, and subsequently a negative consequence, presented in these four methodologies is their specific focus only on the local area. Rapid and significant changes on a global scale have also changed the criminal environment, and whilst these methodologies may be appropriate for addressing localized and 'minor' crimes, they fail to possess the qualities required within a methodology to address the more serious threat of transnational organized crime (TOC). The nature, complexity and volume of criminal challenges now faced by LEAs require a fundamental shift in their methodologies and approaches (Ratcliffe, 2003; Ratcliffe, 2008b, 2008a; Ratcliffe and Sheptycki, 2009). Whilst over the past two decades there has been a noticeable shift in the culture and strategies of policing organizations within most, if not all, Australian LEAs towards using a more proactive policing approach for tackling all forms of criminal activity, the traditional reactive model of policing still exists as the primary methodology (Chan, 1997; Ratcliffe, 2008a). This has been precipitated by the increasing sophistication of criminal enterprises, which has made it imperative to work towards the disruption and demolition of the network structures instead of merely arresting individual criminals within these organized groups (Robertson, 1997; Wardlaw and Boughton, 2006). The attempts to break-up criminal networks will fail to be effective until all available information is developed, analysed and transformed into an intelligence product suitable for use by law enforcement personnel. As such, a truly proactive strategy requires a complete alteration in the manner in which both agencies and governments deal with crime. In order to achieve these results, there needs to be a shift within the law enforcement environment that views intelligence as a *precondition* to effective policing, rather than as a *supplement*. As Wardlaw and Boughton (2006, p. 135) assert, this requires the adoption of wider definitions and understanding of concepts such as 'information', 'intelligence sources', 'partners' and 'clients'.

Intelligence has always been associated with the 'spook' mentality of keeping secrets, reinforced by the limitations on what can be shared, with whom and when, coupled with agency competition and culture. Henceforth, to encourage this proactive change there is a need to break down these intelligence 'obstacles' as LEAs enter the new era of the ILP methodology (Wardlaw and Boughton, 2006, p. 135).

Intelligence-led policing

Whilst the use of intelligence has been common practice within the military arena for centuries its application as a proactive, rather than a reactive, strategy within Australian LEAs is still a relatively new concept. It is no surprise when it is noted that the policing environment has changed significantly over the past two decades, and the traditional methodologies of crime as a solely localized threat has been turned upside down (Robertson, 1997). Where there has been a change and increase in political, economic and social globalization, the face and nature of crime has changed with it. Criminals can now not only move at will and at relative ease and cost, both within and between countries, they can communicate instantaneously across the world. So too, criminal activities can now occur at a location far removed from that of its perpetrator (Robertson, 1997).

ILP has no universally accepted definition; however, it is identified by the core idea that policing, from tactical to strategic levels and beyond to government policy, should be informed by relevant and actionable intelligence analysis. It is developed as a model that uses intelligence to guide and shape policy, strategy and operations, rather than simply solving or supporting singular investigations (Wardlaw and Boughton, 2006). Ratcliffe (2002, 2003, 2008a, b, c), a leading authority in the area of ILP, has developed a range of criteria allowing for an appropriate definition:

Intelligence-Led Policing is a business model and managerial centred philosophy where data analysis and crime intelligence are pivotal to an objective, top-down decision-making framework that facilitates crime and problem reduction. It is proactive and informant and surveillance-focused with heightened attention directed toward recidivists and serious crime offenders, and it provides a central crime intelligence mechanism to facilitate objective decision-making and disrupt and prevent crime. (Ratcliffe, 2002, 2003, 2008a, b, c; Ratcliffe and Guidetti, 2008, p. 112)

During the mid-1990s the United Kingdom (UK) introduced a National Intelligence Model (NIM) following several reports by the Audit Commission. The NIM sought to bring intelligence to the forefront of policing objectives, which would lead the way in subsequent strategic and tactical decisions regarding who and what to target.

The NIM framework provided a means for both policy leaders and law enforcement management to use a methodology that would guide

their approach to a problem and allow them to devise an appropriate and properly prioritized strategy that would produce a successful outcome (Flood and Gasper, 2009, pp. 51–53). Flood and Gasper (2009) argue that the model provides police management with the ability to not only understand but further anticipate the threats and risks across the domain of public safety, as it has provided a model for the whole business of policing.

Of all the policing methodologies ILP is uniquely positioned to effectively combat TOC. The UK's Serious Organised Crime Agency (SOCA) (SOCA, 2006) argues that the majority of current LEAs are structured for bureaucratic efficiency. The operational focus is on individual crime types to satisfy the priorities and objectives of a government led by the media advancing community concern. Conversely, criminal enterprises rarely think or deal in terms of isolated and singular crime areas. Instead, they simply see the opportunities available to them for making money if they possess the relevant criminal capability, and frequently amalgamate crime types into their enterprise as a means of maximizing profits whilst ideally minimizing detection (Serious Organised Crime Agency, 2006, p. 15; Flood and Gasper, 2009, p. 57).

The UK's Audit Commission (1993) noted that the targeting of known and recidivist offenders, criminal leaders and criminal innovators is the cornerstone of any proactive policing model. A central precept of the ILP methodology is to focus on the prolific and persistent offenders who commit a majority of the crime with the requirement to 'tackle and incapacitate' the primary offenders of serious crime (Flood, 2004; Flood and Gasper, 2009, p. 51; Ratcliffe, 2008b, p. 167). Through the development of an ILP grounded system the ability to manage this criminality can be identified. As Flood and Gasper (2009) note, the primary difficulty that LEAs face is simply trying to visualize and understand the criminal environment. They argue that whilst on the surface it is initially confusing, chaotic, complex and ever changing in both its impact and character, there always remains an area that is stable and enduring (Flood and Gasper, 2009). It is the identification of this area by the collection, collation and analysis of data, and subsequent development of intelligence, that allows the development of a clearer understanding of what once appeared complex and haphazard, and reveals a systematic and comprehensible environment. This understanding enables the basis for a 'highly impactful strategy' that can, at the very least, provide a beneficial starting point for dealing with the bigger picture. These requirements are

answered by the ILP philosophy, characterizing it as the most suitable methodology for combating TOC (Flood and Gasper, 2009).

Among the literature there is a clear acknowledgement regarding the current lack of evaluation of ILP, along with a requirement for additional research and development of a model of best practice for the implementation of ILP into new jurisdictions (Ratcliffe, 2002, 2008a). This is in part due to the difficulty of effectively evaluating a business model and, as stated by Keely (2004, p. 11), the impact of intelligence is 'notoriously difficult to measure'. Within Australia the use and slow integration of ILP has been used with limited, and in some cases flawed, evaluation of its effectiveness. Heldon (2009) and Ratcliffe (2008b) discuss the effectiveness and limitations of Operation Anchorage, a short-term ILP operation carried out by the Australian Federal Police (AFP) in response to a spike in property crime in the Australian Capital Territory in 2001. In line with ILP technique, over a four-month period, the operation targeted known and recidivist offenders. Whilst the operation was deemed effective following its closure, resulting in a 21% decrease in burglaries combined with a residual effect lasting 45 weeks, its unsustainability resulted from limited resources and high costs. This illustrates that ILP cannot be implemented as a 'secondary' strategy used when seemingly convenient. Heldon (2009), more importantly, argues that the operation was flawed in its use of the ILP methodology. Whilst offender targeting was present, she (Heldon, 2009) notes that it failed to address the underlying causal factors for increased property crime, and a primary focus on tactical intelligence meant that the strategic and long-term ideals were forgotten. As such it is theorized that had the AFP embraced ILP as a whole and addressed these underlying issues it is likely that a more robust result could have been achieved (Heldon, 2009).

However, there is an apparent gap in the literature regarding ILP relating to specific discussion of intelligence collection. Whilst Ratcliffe (2008a, b) frequently encourages the use of covert means of intelligence collection and briefly discusses the use of informants, he, along with a multitude of existing literature, fails to examine the covert means in depth. There is also an obvious disconnect in the literature between the use of communication interception technology (CIT) and ILP as a whole. This is evident in the work by Flood (2004) and Flood and Gasper (2009), architects of the UK's NIM. Any focus on these areas by Ratcliffe (2008a, b), Flood (2004) and Flood and Gasper (2009) simply reiterates previous bodies of literature that concentrate on the legislative

and/or ethical and privacy constraints and limitations. Whether this is simply due to the lack of literature that concerns the practical use of CIT, however, remains to be seen.

It has well been documented that the key to combating TOC is a comprehensive, integrated global counter-strategy that involves the continual cooperation, support and knowledge sharing of law enforcement and intelligence agencies worldwide (Glenn, Gordon and Florescu, 2008). A point that then resonates as a primary dilemma in this proclaimed 'war on transnational crime' is that without intelligence the required case for cooperation among countries and agencies cannot be made in the first place; the priorities of the LEA cannot be identified and the threats posed cannot be addressed. Flood and Gasper (2009) argue that the most disruptive and effective opportunities cannot be seized and the activities of all the relevant agencies cannot be coordinated to best effect. Above all, there is no way of knowing just how successful LEAs and governments are in combating TOC.

Chapter summary

This chapter reviewed the current policing systems, processes and practices that underpin both tactical and strategic responses to TOC by contemporary and progressive LEAs. It has shown that whilst the methodologies of traditional, problem-orientated, community and computer statistics policing possess their own unique strengths, they all lack the ability to effectively combat TOC. The literature has illustrated that the proactive nature of ILP is the most beneficial framework that can fight criminal enterprises and, as is discussed in the following section, will support CIT appropriately.

5

Anti-Corruption Models

Abstract: *This chapter examines the techniques used to investigate corrupt systems and dark networks, which are, by their nature, hidden from view and must be revealed through the gathering of intelligence. It reviews the considerations to be examined in order to dismantle entire networks including the structure of investigative agencies. Illustrating that communication interception technology (CIT) can be used on its own or in combination with other strategies to gather information on the full network, provide the evidence necessary to build a strategic intelligence picture of the corrupt environment, and supply evidence in criminal trials, the chapter confirms that CIT provides significant opportunities for intelligence and evidence gathering that otherwise are not available when CIT powers are not accessible to investigators.*

Congram, Mitchell, Peter Bell, and Mark Lauchs. *Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology*. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

This chapter analyses the strategies currently employed by law enforcement organizations within Australia, New Zealand (NZ), Canada and the United Kingdom (UK) to investigate corrupt systems and dark networks.

The investigation of corruption depends on the structure of the corruption network. Simply approaching a problem and working it out as you go along does not mean you will not be successful, as can be seen in the famous Knapp Commission, an inquiry in the 1970s into police corruption in New York that arose out of the allegations made by Frank Serpico (Armstrong, 2012). A greater likelihood of success will come from an understanding of the corruption process. Understanding the process will also allow a considered application of communication interception technology (CIT). Throughout this discussion there will be a focus on corruption networks rather than simply corrupt individuals. While not every corrupt official belongs to a network, CIT is more likely to be used more extensively in the investigation of larger networks.

As was discussed in Chapter 3, corruption networks have particular characteristics which can be used to target investigations.

Techniques can be both more difficult and easier when dealing with small networks or individuals. If an individual police officer is corrupt it will take particular forms. If it is a form of predator policing then it is highly likely that, should the jurisdiction have a public complaints system, the actions of the police officer will continually appear in complaints. For example, in the mid-1990s the investigation into police corruption on the Gold Coast (Australia), named 'Operation Tesco', began with this initial targeting strategy:

A review of the complaints information disclosed that the names of persons allegedly involved in corrupt drug activity reappear from time to time from different sources and are said to be allegedly involved, either alone or in combination with others whose names also tend to appear. (Carter, 1997)

An individual operator or small group does not have the necessary numbers to control the movement of information or to incorporate senior officers who can provide protection. Thus a public complaints system is an effective means of collating data on their activities. One rich source of complaints will be drug dealers in competition with the police, or those who have been aggrieved within their normal business relationships with such officers.

Conversely, an individual or small group participating in a form of corruption that is consensual will be very difficult to detect as no complaints will be made. In Operation Tesco (CMC, 2011) investigations took place into three officers who were involved in corrupt activity with friends. For example one officer would share information from sensitive databases. Whilst these cases were detected, the detection only happened after a taskforce carried out blanket operations into corruption on the Gold Coast – their activity had gone undetected for many years prior to this.

In a separate example, the Victorian Office of Police Integrity (OPI) carried out investigations into the Armed Offenders Squad. The squad had a disproportionate number of complaints made against it given the type of branch and the exposure to a particular criminal demographic. Visual electronic surveillance of interrogations carried out by this squad demonstrated they were using violence on suspects; the OPI used its power to compel answers. The squad members' responses and those of other witnesses were correlated with the video evidence and demonstrated cultural issues such as 'a willingness by at least some Squad members to give false evidence on oath' (Office of Police Integrity, 2008, p. 8).

However, integrity systems are not always effective against corruption. Becker and Stigler (1974) identify that the level of enforcement will depend on a variety of factors. First is the degree of honesty of the enforcers; thus the police who investigate the police may share the same corruption. Also, some otherwise honest enforcers will condone 'noble cause' corruption. Second is the structure of incentives to honesty; the practice will continue if the perpetrators obtain greater rewards from the act than the investigators do from successful investigation. Third, it depends on the frequency and visibility of the violation; it is harder to detect if it does not happen most of the time in a regular pattern. Fourthly, crimes that do not produce an aggrieved victim, such as bribery, are harder to detect. Noble cause corruption does produce an aggrieved victim but they may not complain.

There are three considerations that need to be examined with a view to ensuring the destruction of the network rather than simply the arrest of an individual:

- 1 Who knows about the corruption?
- 2 What roles are played in the corruption network?
- 3 Who is the most valuable target of the interception?

As a dark network very few people will be aware of corrupt activity:

The logical sources of information about corruption, not surprisingly, are the people who know about it: Police officers, citizens, police organizations, and investigative agencies. The pivotal question... is what motivation would someone have to publicly reveal such information, be they a participant in a corrupt transaction or an administrator in an agency? (Ivkovic, 2003, p. 596)

Independent Commission Against Corruption (ICAC) New South Wales (NSW) investigated corruption in the Wollongong local government. A review of the material by Martin (2012) revealed some interesting facts about the awareness of the corrupt activity that would be applicable to most corrupt activity: many people in Wollongong knew about the corruption but few could prove it while others had full knowledge but refused to take action. This is what Martin calls a 'layered access to knowledge':

those directly involved were fully aware of their activities, some close at hand knew there were problems but did not have details, some citizens had generalised concerns and many others were blissfully ignorant. A few individuals obtained specific knowledge via leaks from insiders to the media and community members. (Martin, 2012, p. 8)

Martin provides descriptions of the three layers:

- ▶ those closest to the centre of operations are unlikely to take action other than as an informant
- ▶ others in the next layer are receiving snippets of information from the inner circle
- ▶ further out again receive even more smaller snippets from the second layer
- ▶ eventually the general public and the media will become aware (Martin, 2012, p.10).

It is also possible to profile potential targets of corruption. If public officials earn less relative to the private sector they will have an incentive to make up the difference through graft. Raising salaries not only reduces this incentive but adds a further incentive against corruption by increasing the financial loss incurred if the official loses their job through being caught. A similar disincentive comes if unemployment rates are high; if

the official loses their job they will have less chance of finding another (Goel and Rich, 1989).

Effective investigations

It is equally important that an investigation be carried out in a world's best practice manner. ICAC, Hong Kong (HK), have a reputation of being one of the most effective anti-corruption agencies in the world. An effective investigation requires a number of key components: the investigative body must be independent of the body being targeted and from the government; the body must have adequate resources and investigative power to carry out their own investigations; the investigation must be carried out confidentially but to ensure success and to protect the identities of innocent parties; in some cases it may be necessary to obtain international mutual assistance to track down witnesses, suspects and money trails; and above all you need professional, well-trained investigators (Kwok, 2003).

The techniques used in investigation depend on whether or not the corrupt activity has ceased or is ongoing. For example, surveillance and telephone interception as a technology would have little use in investigating past activity. As Kwok (2003) points out, the nature of corruption investigations is slightly different to the normal criminal investigation: the aim of the corruption investigation is to close down the corrupt network, therefore investigators should not be happy with catching one person but should use that person as a tool to close down the entire network. This may involve the use of this person as an informant and/or an operative to collect information on other members.

The necessity for an independent watchdog has recently been reinforced by the Independent Police Complaints Commission (IPCC) findings in the UK, that out of the 8,500 allegations of wrongdoing made against police officers that were investigated internally by police agencies only 13 criminal convictions eventuated (Peachey, 2012).

There are three necessities for effective internal corruption control:

- ▶ strong committed leadership that actively carries out accountability regimes
- ▶ strong frontline supervision of both operations and outcomes
- ▶ providing rewards for integrity, including the reduction of bureaucracy that inhibits good police work (Dombrink, 1988).

Nature of corrupt activity

Corruption investigations can take two forms: investigations of current activity or investigations in response to complaints or evidence of past dealings. Investigation of corruption after the fact is what McCusker (2006, p. 8) calls the ‘interventionist’ approach.

It has to be noted that in the modern environment successful corruption investigations, especially of high-profile individuals or large networks, are carried out by independent corruption watchdogs. These bodies have grown in the past two decades. The original of the modern versions of such bodies is ICAC HK. It was established in 1974 by the British Government to target corruption within the civil service. Like many such bodies it replaced an internal investigation service that had a very poor track record of success when it came to investigating and reducing corruption. In this case the HK Police had had an Anti-Corruption Branch. ICAC HK was taken outside the normal reporting regime and was directly responsible to the governor of the colony.

Similar histories of ineffective investigative bodies being replaced occurred in Australia. In Queensland various incarnations of internal police anti-corruption units had different levels of fruitlessness in attempts to both identify and prevent corruption. In a theme common around the country, it took a major scandal before reform took effect. The Fitzgerald Inquiry in 1988–1989 uncovered systemic corruption in both the Queensland Police Force and amongst politicians (Fitzgerald, 1989). The recommendations of the inquiry included the formation of a Criminal Justice Commission (CJC) which would effectively operate as a permanent royal commission. The CJC reported to parliament and was thus independent from the Executive – a big step forward on the ICAC HK model. Nonetheless, it had powers to investigate politicians and attracted their ire (Lauchs, 2007). As a result it went through a number of incarnations and is now the Crime and Misconduct Commission (CMC) with similar investigative powers. Its greatest inhibition at present is resourcing, which has been a constant issue for most of its existence (Carter, 1997).

The original independent watchdog in Australia was ICAC in NSW. It was established in 1988, once again in response to a number of scandals involving police and politicians. As a demonstration of its independence its first major scalp was the state’s Premier, Nic Greiner, who had set up ICAC NSW after winning an election with a campaign pushing anti-corruption. He resigned after ICAC ruled that an appointment

he had made amounted to corruption. Unlike the CJC in Queensland, ICAC NSW does not investigate police. This is the jurisdiction of the Police Integrity Commission (PIC NSW) which was set up in 1996 yet again after a major corruption scandal uncovered by the Wood Royal Commission (Wood, 1997). However, unlike ICAC NSW, PIC NSW reports within the Executive, in this case to the Minister of Police.

Other similar agencies have been established in Western Australia – the Corruption and Crime Commission (CCC) – and in Victoria under the Ombudsman. Federally there is no independent commission investigating corruption within the public service. There is only the Australian Commission for Law Enforcement Integrity (ACLEI) which was established in 2006. It has the power to investigate corruption within the policing agencies of the Commonwealth Government, including the Australian Crime Commission, Australian Customs and Border Protection Service, the Australian Federal Police and the now defunct National Crime Authority.

Powers of watchdog commissions

There are some basic powers of Commissions of Inquiries that are essential for success:

- 1 The power to compel witnesses to answer has been very successful for many years in Australia.
- 2 The power to seize evidence under warrants.
- 3 The power to conduct surveillance activity.
- 4 The power to use surveillance technology.
- 5 The power to grant indemnities for prosecution.

From an investigative perspective one of the most important powers is the granting of indemnities. The ability to give a well-informed insider the opportunity to ‘roll over’ has led to successful exposure of large networks. In both the Fitzgerald and Wood Inquiries key indemnities allowed detailed exposure of the network. In the Fitzgerald Inquiry, Jack Herbert, the bagman of the Joke corruption network was able to provide not just information on the nature of the network but also:

- ▶ the names of all the participants of which he was aware
- ▶ the amounts of money for all the transactions

- ▶ the operation of the system of payments including times and methods of payment
- ▶ methods of laundering the money obtained through corruption (Fitzgerald, 1989; Herbert and Gilling, 2004; Lauchs and Staines, 2012).

Herbert was not the first police officer to roll over. But the previous officers could not provide the level of detail and also did not have Herbert's knowledge of the network. His information was instrumental in bringing charges against the then Police Commissioner, Terrence Lewis.

In the Wood Inquiry the indemnity system was used more strategically. Detective Sergeant Trevor Haken was targeted by the Commission before the public hearings began. He was a vulnerable target both in his mental state and career. The commission was able to use him as an intelligence source for their investigations as his status with the Commission was not revealed for many months. As such, Haken was able to facilitate the recording of incriminating conversations including video evidence from his car as he made payments to other police officers. In the Fitzgerald Inquiry, Herbert was not 'turned' until after the hearings had begun. He had fled to the UK and was tracked down by officers of that Commission (Padraic, 2005).

In both cases the production by the Commissions of corrupt officers naming names under indemnity allowed the investigators to leverage confessions and cooperation from other police (Lauchs and Merrington, 2012). Once presented with information clearly establishing their guilt, officers saw no choice but to cooperate. However, an inquiry does not need to have every target cooperate; they only need sufficient cooperation to allow the full network to be exposed. On average, approximately only six cooperative witnesses are needed from the group of participants (Fitzgerald, 1989; Wood, 1997). This fact can lead to a rush of participation as corrupt officials try to obtain protection from prosecution before the requisite number of places has been exhausted. Those who hold out longer must risk another officer exposing their participation. Thus we see the classic *prisoners' dilemma*: if all the police maintain the 'wall of silence' then none of them would face prosecution, but each individual has to risk all of them being exposed by another member, in which case participation is better than conviction.

On another level, cooperation can also come from the non-corrupt network members. In the Fitzgerald Inquiry approximately 12 sex workers

cooperated with the Commission to discuss the nature of police participation in extortion of the illegal industry (Fitzgerald, 1988–1989). This cooperation was easier to obtain. The Commission was established to expose corruption within the government; it was not designed to arrest sex workers. The Commission had nothing to lose by providing indemnities to those sex workers who knew about corruption but were not the perpetrators of corrupt acts (beyond being asked to provide free sex to police officers). Recommendations for arrests would be targeted at the police and the brothel owners. However, while the names of the women and men were suppressed, it was easy for their former employers to work out who they were once they gave evidence in an open inquiry – as such this was extremely risky, but still had to be weighed up against arrest and conviction.

Targeting of CIT

CIT can be used either covertly on both parties engaged in conversation or with the cooperation of one of the parties. For example, the electronic surveillance used in cooperation with Trevor Haken was done entirely with his knowledge. However, in both cases there are tactical questions about who should be recorded covertly.

There are some fundamentals that must be considered in an investigation into a large corruption network. First, the goal of the investigation is not to catch individuals but to expose and close down the network. Simply catching a few members, even if they are big fish, will not end corrupt activity in the network. Social network analysis exposes the people in the network who have the greatest power to disrupt the network operations. For example, if you had a network where only one person knew the people who were paying and the people who were being paid (a situation very similar to the role undertaken by Jack Herbert in Queensland) then the elimination of that broker would end the network at least temporarily. Being a dark network, the payers would not have the means to make fresh connections with payees – until they find a new broker the network would be effectively closed down. This is what occurred in Queensland when the first incarnation of the Joke network was closed down following an investigation into Herbert's role in corruption. Herbert left the police force and therefore could not continue his role as bagman. Six years later former members who still knew Herbert were asking him to reprise his role as broker. Even though he was no

longer a police officer he was still able to carry out the collection and disbursement of bribes. He was actually in a safer position as no agency had a role in investigating corruption by civilians (Lauchs and Staines, 2012) (see Figure 5.1).

However, as has been discussed above, many networks build in redundancy so that they are far less vulnerable to the loss of a broker. For example, a broker could apprentice another member to ensure that his/her knowledge and connections could be carried on in their absence. In this situation a decapitation strategy would only be an inconvenience rather than a fatal blow to a network. An investigation could not stop at the brokers or bosses and would have to ensure it had full knowledge of the network. Having said that, the tactics of this exposure can use the network vulnerabilities as a mechanism to dismantle the rest of the membership.

If a covert surveillance targeted a broker then the interactions of the broker should reveal a significant section of the network. If nothing else it should reveal the other key players in the network. Thus a CIT operation on the phone of a broker should be a valuable intelligence tool. However, this tactic has a chicken and egg problem – how do you work out the identity of the broker without first knowing the whole network? And if you know the whole network, why do you need the broker? The answer is to build perspectives on the network from individuals and, once a key figure is identified, target this individual with either surveillance and/or indemnity as a means of exposing the whole network.

The following example could illustrate this strategy. If you want to see the whole network of illegal prostitution and police corruption you would start with the most vulnerable members of the network – the sex workers. Each sex worker may only know a very small section of the network but comparison of each of these networks would gradually expose overlaps. Overlaps are, by definition, the brokers between the smaller networks. The overlaps can then be surveilled to broaden knowledge of the network. One overlapping broker may be a small player in the entire network but his network can expose more connections. Thus, in the same manner as peeling the layers of an onion, the continued exposure of each individual's network (known as *ego networks*) will expose higher levels of brokerage within the network. Finally, it must be reinforced that you do not need every participants' ego network. The revelations of a Jack Herbert make it unnecessary to pursue every member of the network. This is a very efficient intelligence tool.

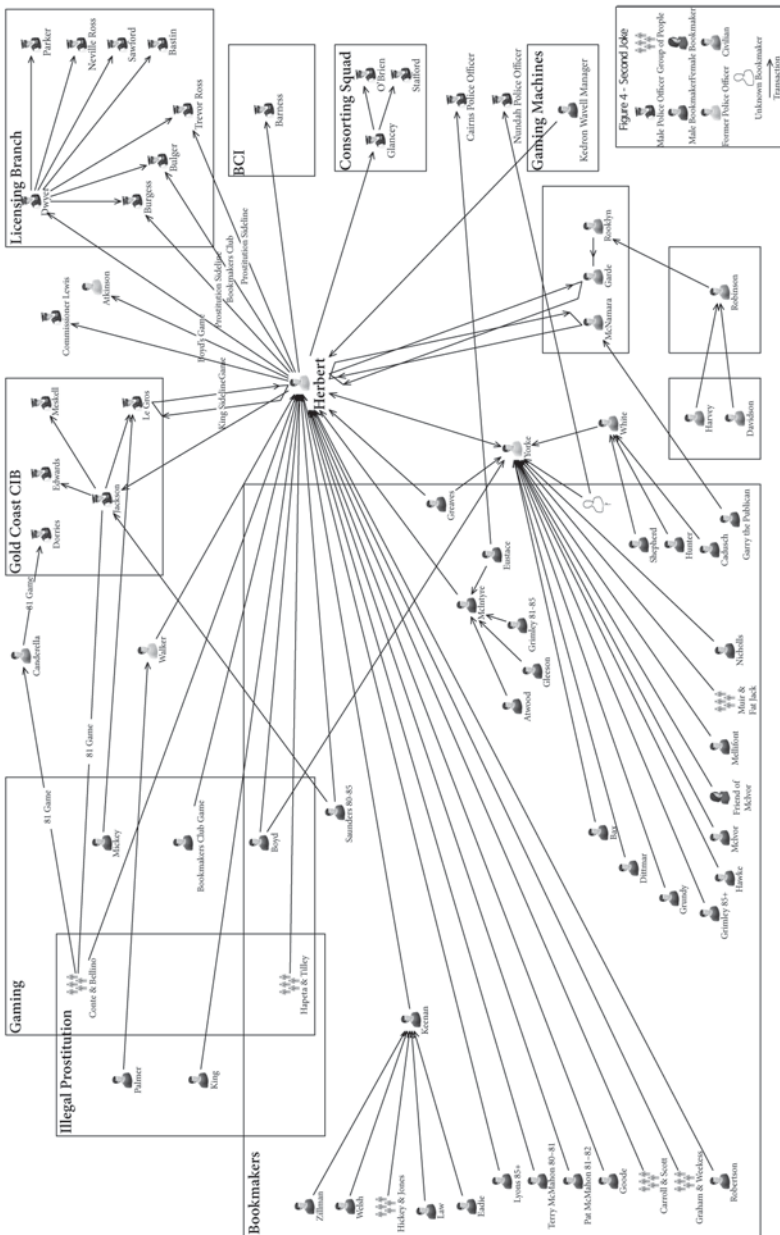


FIGURE 5.1 The second joke network

Figure 5.1 demonstrates this argument. This figure shows Herbert's ego network under the second Joke network. It is an ego network because it is based upon his corrupt activity rather than trying to map the entire corrupt community. For example, Herbert never had dealings with prostitutes and they never paid money for protection. Thus they do not appear in this network which tracks the relationships and movement of money in the second Joke network. Note that even Herbert does not have direct connections with every member of the network. For example, the members of the Licensing Branch are paid by one of Herbert's connections; this person acts as a broker between Herbert and the members of the Branch. None of this reduces the value of sex workers as an entrée into the network. The girls working in the brothels were targeted by the Fitzgerald Inquiry and given indemnity as witnesses. They were able to provide the information concerning the day-to-day operation of the brothels and the payments, in money or by sexual favours, that were made to police. They also knew the identities of all the local officers who policed prostitution and could name those who were corrupt. Corrupt officers could then be targeted as witnesses, both cooperative and hostile. In other inquiries with more extensive intelligence operations, such as the Wood Inquiry into police corruption in Sydney in the 1990s (Wood, 1997), this targeting could take place prior to hearings so that surveillance evidence could be obtained in advance of the public hearings. The evidence thus obtained could be used to improve strategic intelligence and also identify further links in the corrupt network.

Thus, CIT provides an even greater tool as it obviates the need for indemnities. Good surveillance, of which CIT forms an essential part, can reveal more than a person may willingly discuss as a protected witness. The data obtained can also be used to triangulate against testimony of that person and other witnesses. A combination of both indemnities and CIT is even more effective. In the Wood Inquiry, Trevor Haken, a corrupt detective, was approached by the Commission with evidence of his wrongdoing and agreed to work undercover to gather evidence on other officers. This mechanism allowed the Commission to gather audio and video evidence of transactions and admissions of corrupt behaviour of other members of the corruption network (Padraic, 2005; Wood, 1997). Similarly, the Knapp Commission in New York was able to use the same method to obtain the cooperation of a police officer, Phillips, who was able to facilitate gathering the same type of evidence of extensive corrupt behaviour.

Neither the Fitzgerald, Wood nor Knapp Commissions had the power to tap phones. This power is now used extensively by contemporary watchdog agencies. Telephone intercepts can, to a limited extent, obviate the need for a cooperative network member. The telephone records and conversations of a member can reveal other members in the network and expose the nature of their role. Each newly exposed member can be the target of further CIT which can, in turn, reveal more members and clarify the operation of the network.

Chapter summary

This chapter examined the techniques used to investigate corrupt systems and dark networks. Dark networks are, by their nature, hidden from view and must be revealed through the gathering of intelligence. The chapter reviewed the considerations that need to be examined in order to dismantle an entire network as opposed to simply arresting individuals from the structure of investigative agencies. There has to be delayed gratification to allow for a larger prize. Leaving the bulk of a network in place, and, more particularly, leaving groups within the network with the ability to re-establish their connections after the loss of a few key personnel, simply provides a temporary disruption of corruption rather than a closure of a network. CIT can be used on its own or in combination with the use of informants or indemnified network members to gather information on the full network. It can provide the evidence necessary to build a strategic intelligence picture of the corrupt environment, and also to be used as evidence in criminal trials against the participants. More extensive use of CIT can enhance these abilities by reducing the necessity to rely on cooperation by network members. CIT should not be seen as replacing cooperative indemnified corrupt officers, but it provides significant opportunities for intelligence and evidence gathering that otherwise are not available when CIT powers are not available to the watchdog agency or commission of inquiry.

6

Communication Interception Technology

Abstract: Reviewing the current literature surrounding the specific use of communication interception technology (CIT) and its effectiveness, this chapter shows that, according to the literature, CIT usage is limited in areas such as the fight against transnational organized crime (TOC) and corruption. It identifies that the key issues surrounding the use of CIT are legislation (governing usage), privacy concerns and culture. Despite these constraints, specific case studies cited in this chapter provide a valuable means to examine the effectiveness of CIT as a tool against transnational crime. In particular they demonstrate how intelligence derived from intercept products can provide timely and valuable information, be used to increase understanding of how criminal organizations operate, and lead to significant arrests and seizures.

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

The developments in information and communication technology (ICT), and the greater opportunities this presents for illicit purposes in particular, has resulted in greater demand for interception technologies. However, despite the fact that the greater use of available ICT also creates a point of vulnerability for criminal entities – one that can be exploited by law enforcement agencies (LEAs) – communication interception technology (CIT) remains severely limited in its use. This chapter explores the development and use of CIT using Australia as a case study and other English-speaking Commonwealth countries of the United Kingdom (UK), Canada and New Zealand (NZ) as points of comparison. The chapter examines the legal frameworks surrounding the use of CIT, its current use and effectiveness, and the issues faced by LEAs in their attempt to utilize CIT in the fight against transnational organized crime (TOC) and official corruption.

Defining communication interception technology

In line with the development and growth of ICT there has been an increasing requirement for the use of interception technologies. This ‘popularity’ has resulted in frequent debate regarding the most appropriate definition (Starey, 2005; Branch, 2003; Electronic Frontier Australia, 2006). The decision to develop and use the term ‘communication interception technology’ (CIT) is a result of the preconceived notions attached to the definition of ‘telecommunications’. However, for the purpose of this chapter, perceiving ‘telecommunications’ as solely traditional telecommunication methods such as telephone calls would be a gross error in focus and definition. Rather, the use of the term CIT can be said to imply a broader scope for all forms and methods of communication such as mobile phones, e-mail, text messaging and skype, and subsequently it is this broader interpretation which is used to reference the interception methods and related technology for this chapter.

In adopting this broader interpretation it is relevant to note the gradual shift away from the traditional circuit-switched networks to packet-switched networks. Designed for the telephone, the circuit-switch system uses a dedicated circuit or channel which is kept open during the telephone call and which cannot be used by any other data or calls during this time (Cairncross, 1997; Copeland, 2000). Conversely, packet-switching networks (traditionally used for data) break up the message into

'packets' which travel around a network seeking the most efficient route, with each packet potentially taking a different route. While both networks have pros and cons, traditionally circuit-switching networks are suited to landline telephones (e.g. 'live' communication) while packet-switching is suited for sending data (e.g. 'stored' communication) (Cairncross, 1997). The interception of signals can provide a vast amount of information. While it has been traditionally used to intercept/analyse communications from foreign governments and groups, its broader application to include the collection of intelligence on criminal groups has evolved over time. This in itself presents to be problematic for law enforcement. As can be seen from the next section, current legislation does, however, seek to differentiate between 'live' and 'stored' communication.

Legal frameworks governing communication interception technology

Australia

Access to telephone interception powers has come late in Australia. The power has existed under the *Telecommunications (Interception and Access) Act 1979* (Cwlth) (the TIA Act), as the Commonwealth Government has the power to legislate in relation to telecommunications.

Section 5 of the TIA Act defines 'communication' as being:

conversation and a message whether:

- (a) in the form of
 - (i) speech, music or other sounds
 - (ii) data
 - (iii) text
 - (iv) visual images, whether or not animated; or
 - (v) signals; or
- (b) in any other form or in any combination of forms.

It is evident that the broad nature of the definition clearly encompasses all possibilities associated with communication. It is important to note that concerning CIT, under both the TIA Act and *Telecommunications (Interception) Amendment Act 2006* (Cwlth), communications are divided into two distinct categories: live communications and stored communications. 'Live communications' addresses the category of communication that passes over a telecommunication system, such as voice telephony.

The 'live' aspect concerns the fact that during a telephone call the recipient instantly receives the message being communicated in 'real time' (Starey, 2005; Ahmed, 2007). Starey (2005) argues the key aspect that personifies live communication is that, without interception (listening or recording), there is no record of the conversation once the communication ceases. This is in contrast to stored communication, or communication stored in transit, which covers communication that during the course of its transmission is stored on one or more pieces of equipment belonging to a carrier or service provider before being retrieved and accessed by the recipient. Starey (2005) and Ahmed (2007) both state that the concept of stored communication applies to most forms of electronic communication such as e-mail, SMS text messaging, voice-mail, internet chat or instant messaging software, and Voice over Internet Protocol (VoIP) telephony. During the transmission of all these communication methods the data packets transmitting this information are stored, at the least very momentarily, on various servers and computer equipment belonging to service providers. As a result they argue that this information can be intercepted prior to the intended recipient actually receiving the message (Starey, 2005; Ahmed, 2007). They further argue that this breakdown is especially important with regards to the legislative definitions and subsequent abilities to intercept the communications, where interception consists of the act of listening to a recording, or reading, through any means, a communication without the knowledge of the person making the communication (Ahmed, 2007; TIA Act, 2006; Starey, 2005).

It is interesting to note, however, that in relation to Voice Over Internet Protocol (VOIP), the explanatory memorandum for the *Australian Commonwealth Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* regarded VOIP as 'live' communication – and not 'stored' communication as advocated by Starey (2005) and Ahmed (2007):

Subsection 7(3A) further provides that the definition of stored communication does not include a voice over internet protocol (VOIP) communication... It is necessary to specifically exclude VOIP communications stored in this way from the definition of stored communication because VOIP data packets may be stored for very short periods of time while the communication is in transit... and not giving rise to the creation of a permanent or retrievable copy of the communication... Subsection 7(3A) ensures that a telecommunications interception warrant will be required in order to carry out "live" interception of communications carried by VOIP, and that VOIP communications are protected in the same manner as standard telephony.

Under the TIA Act each state must legislate to nominate a body as a 'declared agency'. The slow progression of access under the state regimes has had a variety of reasons, many resulting from pressure from privacy and civil liberties groups.

Police Integrity Commission (PIC) New South Wales (NSW) and the Independent Commission Against Corruption (ICAC) NSW have the power to use surveillance devices and telephone intercepts under the *Surveillance Devices Act 2007* (NSW) and the TIA Act respectively. Surveillance devices require the approval of a Supreme Court Judge and telephone intercepts need the approval of a Member of the Administrative Appeals Tribunal. The NSW Ombudsman inspects telephone intercepts and controlled operation records. In 2011–2012 ICAC obtained 21 telephone interception warrants (ICAC, 2012). This power was improved by the purchase in 2011 of a specialist telecommunications server and switching system. In the same year PIC issued 62 warrants.

The Crime and Corruption Commission (CCC) in Western Australia has powers for telephone intercepts. It received these powers under the *Telecommunications (Interception and Access) Western Australia Act 1996* (WA) which, in effect, made the CCC a 'declared agency' under the TIA Act. Victoria's Independent Broad-based Anticorruption Commission (IBAC) also has the same power under the *IBAC Act 2011*. In Queensland the Crime and Misconduct Commission (CMC) has the power to use telephone intercepts under the *Telecommunications Interception Act 2009* (Qld) and the TIA Act. In South Australia the Police Ombudsman is responsible for investigating complaints made against police officers. Most of the complaints are actually investigated by the South Australian police with only a small number being handled by the Ombudsman. This office does not appear to have any advanced investigative powers.

At the federal level the Australian Commission for Law Enforcement Integrity (ACLEI) has responsibility for the Australian Crime Commission (ACC), the Australian Customs and Border Protection Service (Customs and Border Protection), the Australian Federal Police (AFP) and the former National Crime Authority (NCA). ACLEI (n.d.) has the following investigative powers:

- ▶ coercive information-gathering hearings and notices
- ▶ telecommunications interception and data access
- ▶ electronic surveillance
- ▶ controlled operations and assumed identities

- ▶ search warrants
- ▶ scrutiny of financial transaction records
- ▶ integrity testing.

Since 1994 there have been five major reviews in relation to laws covering telecommunication interception. Table 6.1 provides an overview of each review.

United Kingdom

The interception of communications is amongst a range of investigative techniques used by UK intelligence and LEAs for the detection and prevention of serious and organized crime, acts of terrorism and to safeguard the economic well-being of the UK where this is directly related to national security (Interception of Communications Commissioner, 2012, p. 12).

The use and oversight of CIT in the UK has been regarded by Hornle, (2010, p. 649) as ‘striking the right balance’ between protecting the rights of individuals and at the same time empowering law enforcement and intelligence agencies to combat TOC, terrorism and official corruption. Under the *Regulation of Investigatory Powers Act (2000)* (RIPA) law enforcement and intelligence agencies (with the exception of the Independent Police Complaints Commission which has power to investigate misconduct and corruption within policing agencies) are granted the power to acquire communication data. Oversight for this activity is provided by a dedicated Commissioner for the Interception of Communications.

Part 1 chapter I of RIPA provides the power to acquire the content of a communication, be it an e-mail, telephone call or SMS message. It requires a warrant to be signed by the Secretary of State or a member of the Scottish Executive. While Part 1 chapter II provides the power to acquire communications data. This represents the who, when and where of a communication event, and requires authorization by a designated person of an appropriate grade within the public authority with the requisite powers under RIPA (2000).

RIPA (2000) outlines quite succinctly which part of the legislation supports specific powers and when these powers can be used, who can use these powers, who authorizes the power to be used (who will sign the respective warrant) and finally who has oversight for the use of these powers.

The Interception of Communications Commissioner is responsible for overseeing the activities of endorsing secretaries and the conduct of an inspection/audit which examines the materials on which decisions

TABLE 6.1 Major reviews regarding telecommunications interception in Australia

Review	Year	Overview
The Barrett Review	1994	Mr Pat Barrett reviewed the cost effectiveness of telecommunications interception. The review resulted in new funding arrangements. Mr Barrett revisited the cost-effectiveness issues following the deregulation of the telecommunications market in Australia in 1997 and proposed minor changes to the 1994 funding model.
The Boucher Review	1999	Mr Dale Boucher also reviewed the cost effectiveness of interception. The review made recommendations regarding the long-term cost effectiveness of interception laws. The review recommended that interception should be available on all telecommunication services. It also recommended that the telecommunications industry should provide and fund the interception, but that LEAs should reimburse costs on a 'user pays' basis.
The Ford Review	1999	Mr Peter Ford reviewed the then <i>Telecommunications (Interception) Act 1979</i> . The main resulting change was the creation of a 'named person warrant regime'. Named person warrants allow a warrant to be issued for many services used by one person.
The Sherman Review	2000	The Senate Legal and Constitutional Legislation Committee reported on the <i>Telecommunications (Interception) Legislation Amendment Bill 2000</i> . The report recommended that the named warrant regime be reviewed within three years. The Sherman Review was conducted in 2003 and concluded that the named person regime should continue, and that it contained adequate safeguards and reporting mechanisms. The review found that the interception regime has a strong compliance culture that is well audited by the inspecting authorities.
The Blunn Review	2005	Mr Anthony Blunn reviewed the 'access to stored communication' element of the legislation. The review found that interception laws were still robust despite major technological change. Recommendations to ensure the longevity of the regime included: <ul style="list-style-type: none"> • making centralized legislation about enforcement and national security access to telecommunication data • keeping the distinction between intercepting live communications and accessing stored ones • allowing interception based on a person that the target is likely to communicate with • developing binding standards for interception where there are no international standards.

were made and how those materials are processed under RIPA (2000). The Commissioner is also responsible for ensuring that compliance is observed by the corresponding law enforcement and intelligence agency utilizing CIT powers/warrants under RIPA (2000).

The 2011 Annual Report of the Interception of Communications Commissioner (2012) noted the important role that lawful interception and communications data acquisition play in the operational successes of LEAs in the UK.

Interception remains a powerful technique in the investigation of many kinds of crime and threats to national security. Many of the largest drug-trafficking, fiscal evasion, people-trafficking, counter-terrorism and wider national security and serious crime investigative successes of the recent past have in some way involved the use of interception and communications data. (Sir Paul Kennedy, Interception of Communications Commissioner 2012, p. 9)

With the potential to be highly intrusive, CIT is an extremely valuable technique that should not be used in isolation but as part of an overall investigative strategy. This position is supported by the Interception of Communications Commissioner who argued that the introduction of the National Intelligence Model (NIM) in the UK in the 1990s provides a suitable platform to embed the CIT technique. Therefore the UK system supports a ‘test of necessity and proportionality’ (Interception of Communications Commissioner, 2012, p. 9).

The UK Warrantry Authorization Process as required under RIPA (2000) is outlined in Figure 6.1.

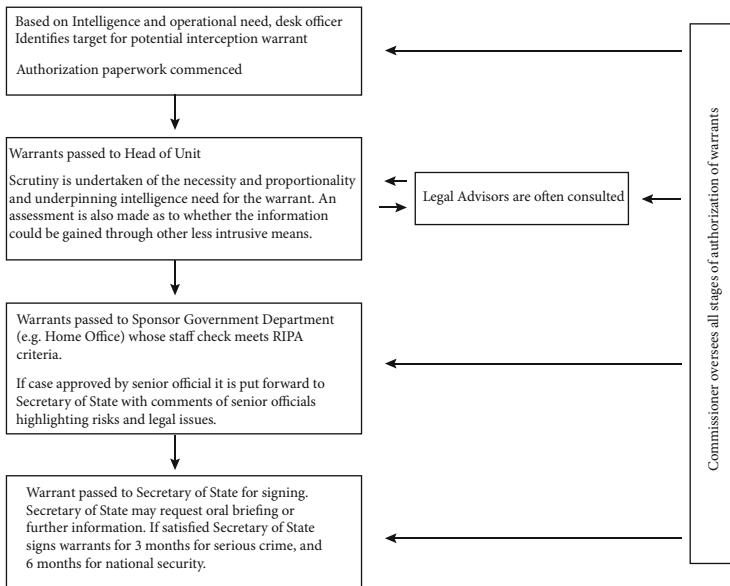


FIGURE 6.1 UK warrantry authorization process as required under RIPA (2000)

Canada

The circumstances surrounding the use of CIT in Canada are quite different to other English-speaking Commonwealth countries. Constantly challenged by a robust Charter of Rights and Freedoms, it could be argued that Canadian law enforcement and intelligence agencies are somewhat behind other Commonwealth countries when it comes to CIT legislation.

With the advent of the *Investigative Powers for the 21st Century Act* in 2010, police became authorized to obtain ‘transmission data.’ Transmission data relates to the underlying means of telecommunication used by a suspect to communicate by telephone or internet. It can provide information on type, date, time, origin, destination and termination of a communication, but would not include content of a private communication. Originally introduced in response to the threat posed by cyber-criminals, this new piece of legislation provides LEAs with new, specialized investigative powers to help them take action against Internet child sexual exploitation, disrupt online organized crime activity and prevent terrorism (Nicholson, 2010).

The Investigative Powers for the 21st Century Act:

- ▶ enable police to identify all the network nodes and jurisdictions involved in the transmission of data and trace communications back to a suspect; judicial authorizations would be required to obtain transmission data, which provides information on the routing but does not include the content of the communication
- ▶ require a telecommunications service provider to temporarily keep data so that it is not lost or deleted in the time it takes LEAs to return with a search warrant or production order to obtain it
- ▶ make it illegal to possess a computer virus for the purposes of committing an offence of mischief
- ▶ enhances international cooperation to help in investigating and prosecuting crimes that extend beyond Canada’s borders.

Requirements to obtain court orders to intercept communications were not changed following the introduction of this new piece of legislation. As is currently the case in Canada, a judicial order is required before police can obtain transmission data. Two different types of orders permit this: a warrant (when the suspect’s data is intercepted in real time) or a production order (to obtain stored transmission data from the service

providers involved). Judicial authorization for this type of data may only be obtained when there are ‘reasonable grounds to suspect’ that the data will assist in the investigation of a crime. The *Investigative Powers for the 21st Century Act* ensures that when warrants are issued telecommunication companies have the technical ability required to intercept communications for the police and the Canadian Security Intelligence Service (CSIS). The Canadian Attorney General Hon Rob Nicholson QC PC MP argues that:

Other countries such as the United Kingdom, the United States, Australia and New Zealand, Germany and Sweden, already have such similar legislation in place.

New Zealand

In 2012 New Zealand’s parliament overhauled its investigative powers under the *Search and Surveillance Act 2012*. The Act’s surveillance device regime (Pt 3 (1)), which came into force on 18 April 2012, replaces the piecemeal provisions that previously governed the use of interception devices (formerly pt 11A of the *Crimes Act 1961* and ss14–29 of the *Misuse of Drugs Amendment Act 1978*).

Beswick and Connell (2012, p. 213) argue that the new legislation aims to strike a balance between law enforcement needs and human rights values by:

- ▶ modernizing the law of search, seizure and surveillance to take into account advances in technologies and to regulate the use of those technologies
- ▶ providing rules that recognize the importance of the rights and entitlements affirmed in other enactments including New Zealand’s *Bill of Rights Act 1990*, the *Privacy Act 1993* and the *Evidence Act 2006*
- ▶ ensuring investigative tools are effective and adequate for law enforcement.

Under the new legislation only a judge can issue an interception warrant and adjudicate that the warrant is based on reasonable grounds, in the belief that evidential material will be obtained. Section 45 of the Act prohibits the interception of any private communication unless it concerns an investigation into an offence that carries a maximum penalty of at least seven years of imprisonment. However, a warrant is only needed if the police do not have the consent of one of the parties being recorded;

that is, they are using a police informant. Interestingly, text messages do not fall under the surveillance data warrant regime and can easily be obtained under the normal search warrant provisions (Beswick and Connell, 2012).

Other jurisdictions

While not studied in detail, it is interesting to note developments in CIT legislation in Hong Kong (HK). Following a court ruling in 2005 new laws were passed in relation to the ICAC HK (an organization with a reputation for being one of the most effective anti-corruption agencies in the world) stating it was unconstitutional to conduct covert surveillance in the absence of relevant legal procedures. These procedures were provided in the *Interception of Communication and Surveillance Ordinance 2006* and are seen as essential to carrying out effective corruption investigations (Kwok, 2003).

Signals intelligence

Signals intelligence, or SIGINT, has had a long history of use by military forces around the world ever since the tactical use of both wired and wireless communication technologies. During both WWI and WWII the use of SIGINT developed into a crucial tactical and strategic decision-making tool by both Allied and Axis forces. The interception and decryption of signals allowed operations to be adapted, and provided a clear advantage to those forces intercepting communications. The growing recognition for the importance of SIGINT following WWII led to the creation of permanent signals amongst intelligence agencies around the world. These include the Defence Signals Directorate (DSD) in Australia, National Security Agency (NSA) in the United States (US), Government Communications Headquarters (GCHQ) in the UK, Communications Security Establishment (CSE) in Canada and the Government Communications Security Bureau (GCSB) in NZ. Richelson (1999) claims that traditionally signals intelligence is considered one of the most important and sensitive forms of intelligence. The interception of signals can provide a vast amount of information and whilst it was traditionally used to intercept/analyse communications from foreign governments and groups, its expansion to include communication collection on

criminal groups has slowly developed over the years. Communication Intelligence (COMINT) and Electronics Intelligence (ELINT), however, form the majority of CIT relevant to law enforcement.

COMINT (the interception of signals between people) broadly corresponds to live communications such as telephone calls, while ELINT (the interception of signals between machines) corresponds to stored communication mediums such as e-mail or SMS.

Whilst the DSD plays a pivotal role in intelligence collection and analysis within the Australian Intelligence Community (AIC), its membership and subsequent framework with the AIC limits its functions to a national security-oriented position, rather than a crime-fighting agency. The *Australian Security Intelligence Organisation Act 1979* (Cth) s4 outlines security as including espionage, sabotage, politically motivated violence, the promotions of communal violence, foreign interference, attacks on Australia's critical infrastructure and defence systems, and also includes carrying out Australia's responsibilities to any other foreign country in relation to threats to security with a particular focus on politically motivated violence. This is further exemplified by DSD's specification as a foreign signals intelligence agency. In particular, restrictions imposed under the *Intelligence Services Act 2001* (Cth) s11 of the Act details that:

- 1 The functions of the agencies [DSD] are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.
- 2 The agencies' functions do not include:
 - (a) the carrying out of police functions; or
 - (b) any other responsibility for the enforcement of the law.

This requirement prohibits DSD from engaging in any interception of signals originating from within Australia and requires a so-called double up of resources as Australian LEAs must purchase, maintain, operate and analyse their own interception technology. This is coupled with the need to go through the rigorous process of requesting appropriate intercept warrants and attempting to maintain a quality level of information sharing between multiple agencies. This separation of not only intelligence and law enforcement but also foreign intelligence and domestic intelligence is a significant obstacle to the overall success of

effective transnational crime fighting (Chalk and Rosenau, 2004; Chalk et al., 2009; Bhaskar and Zhang, 2007; Brady, 2008; Ratcliffe, 2008b). The issues this can cause are best highlighted by the intelligence failure associated with the 11 September 2001 (9/11) terrorist attacks in the US. The restrictions on the US's foreign signals intelligence agency, the NSA, and the organizational culture barriers and restricted knowledge sharing between the NSA, the Central Intelligence Agency (CIA) and the FBI ultimately led to attacks which had the possibility of being prevented (Bamford, 2009).

This is summarized by Staff Director of the 9/11 Congressional Committee, Eleanor Hill, (Bamford, 2009, p. 27) who states 'It's very, very hard to draw a hard and fast line between where foreign intelligence stops and domestic intelligence starts. You have to have very good communication and coordination between the agencies, otherwise things slip between the cracks.' The concern, however, is that these cracks are more akin to canyons, traversed by narrow bridges of communication with a high likelihood of practical intelligence information falling over the side.

Practical application of CIT

CIT in the fight against transnational organized crime

The literature is scant on information relating directly to the specific use of CIT. This research has shown that, rather than being recognized as an individual investigative tool, CIT is more frequently incorporated into the 'surveillance' arena of practical methodologies. Christopher and Cope (2009, pp. 238–239) discuss the importance of the use of surveillance techniques that result from the inability to utilize 'traditional' methods of investigation:

targeted policing ultimately depends upon the capability to infiltrate 'difficult to access' criminal milieu in order to gather information. The capacity to penetrate inimical environments and subcultures is afforded by covert policing, and the Audit Commission accordingly commended to forces the utilisation of informants and surveillance to facilitate and underpin intelligence-led policing. Yet, this recommendation was not only an operational imperative. It was also ostensibly grounded in 'value for money', thereby reinforcing the synthesis of efficiency and 'crime busting' that has tenuously emerged in relation to proactive work.

This statement has application across multiple covert collection methods, such as undercover policing, interception technology, closed circuit television (CCTV), physical surveillance, geographic positioning systems (GPS) and electronic tracking systems and so forth. Its importance to CIT, however, is still relevant. It is recognized in the statement that the pervasive nature of TOC makes intelligence collection an increasingly problematic situation. It has been recognized that more invasive and intrusive measures, such as CIT, are becoming essential to LEAs. These views are additionally supported by Ratcliffe (2003, 2008b, a) who notes that the use of covert information-gathering techniques, such as CIT, is an important aspect of intelligence-led policing (ILP).

What is not highlighted, and thus frequently misunderstood about the ILP framework, is that although it encourages use of these surveillance techniques the purpose of the data, and subsequent intelligence, is for strategic direction (Ratcliffe, 2008b, a). This misconception can be a 'make or break' issue that concerns the acceptance of ILP by law enforcement and the public. Regarding the practical use of CIT and its effectiveness as a law enforcement tool, the Australian Attorney General's Department (2008, p. 15) reports that:

There remains a constant view among agencies that telecommunications interception continues to be an extremely valuable investigative tool. Agencies have again noted that evidence gathered through the execution of a telecommunications interception warrant can lead to the successful conclusion of an investigation in circumstances where alternative evidence is uncorroborated, unavailable or insubstantial.

The understanding of this statement is twofold. The apparent view stemming from this statement is that Australian LEAs who utilize CIT believe that it is an effective tool in the fight against crime. Whilst this is positive for the reinforcement of CIT's use, the statement exposes the flaw in current use by Australian agencies; it is clear that the use of information collected is specifically directed to an individual case or investigation, with CIT working as an evidence-gathering tool rather than an intelligence-gathering tool. Wardlaw and Boughton (2006, p. 139) warn though:

While there is an obvious and real need for sharing, the distinction between criminal intelligence and security intelligence is becoming increasingly blurred. The challenge for the AFP, as for other law enforcement bodies, is to make sure those who need to know do know, and yet still remain focused on its core role as a law enforcement agency.

The important distinction, as highlighted by Ratcliffe (2008b, a), is that when employing CIT under the ILP business model intelligence collection is used for operational targeting as well as strategic decision-making. This combination ensures that the law enforcement role is continually maintained by LEAs. Rather than intelligence simply informing against possible threats (the 'security' role) it provides vital guidance for the deployment of enforcement strategies on either persons or areas of interest.

CIT in Australian corruption investigations

In Australia policing agencies received telephone intercept technology much earlier than their watchdog counterparts. This section discusses the gradual move towards extending telephone intercept technology to Australian commissions of inquiry and later standing commission bodies such as the Independent Commission Against Corruption (ICAC) or the Crime and Misconduct Commission (CMC).

The Fitzgerald Inquiry into police corruption in Queensland, Australia, in the 1980s had the power to use listening devices but not telephone intercepts (Fitzgerald, 1989). Their greatest power was the use of indemnities:

Indemnities to present and former police officers were a vital step in cracking the facade which had previously defeated every attempt at penetration. Some indemnified witnesses acted as catalysts, pushing the Inquiry into areas of crime and misconduct which would not otherwise have been explored, while others provided a fresh insight or corroborated important matters which were already known or suspected... Many of the offences for which indemnity was granted would otherwise never have been discovered, let alone prosecuted. It is fanciful to pretend that those indemnified would otherwise have all been sentenced to lengthy prison terms. (Fitzgerald, 1989, pp. 12–13)

The Wood Royal Commission, carried out in 1995–1997 to determine the extent of police corruption in New South Wales, Australia, had the power to receive but not carry out CIT intercepts.

The Kennedy Royal Commission (2002–2004) in Western Australia was able to commence operations with access to CIT. Kennedy described these powers, along with the use of assumed identities, controlled operations and integrity testing programmes, as 'invaluable to its work'. However, the Commission did not have full access to interception

powers. The federal government declared the Royal Commission an eligible authority under the *Telecommunications (Interception) Act 1979* (TIA Act), which enabled the Royal Commission to ‘receive information obtained as a result of the interception of telecommunications’. The Royal Commission was not given the power to carry out telecommunications interceptions. Kennedy got around this through joint operations with agencies that had full access to the powers of the TIA Act. Whilst these arrangements were not ideal they did provide a workable basis for operations by the Royal Commission into investigations of corrupt conduct. These investigatory tools have generated intelligence and evidence that might not otherwise have been obtained. In particular, proactive investigations gathered useful information concerning the behavioural patterns, work histories and associations of targeted officers (Kennedy, 2004).

Effectiveness of communication interception technology

The effectiveness of CIT is clearly an important aspect of any intelligence collection strategy. However, there is limited availability of examples and evidence of effectiveness. In Australia the Attorney General’s *Annual Report on Telecommunication Interception* (Attorney General’s Department, 2008) identifies that:

On a per warrant basis, there were 63 arrests for every 100 warrants issued. This represents an increase from the previous reporting period, in which agencies reported 53 arrests for every 100 warrants issued... On a per warrant basis, there were 120 prosecutions and 78 convictions secured on the basis of intercepted information for every 100 warrants issued. In the previous reporting period, agencies reported 81 prosecutions and 69 convictions based on lawfully intercepted information for every 100 warrants issued. It should be noted that the statistics do not necessarily relate to lawfully intercepted information obtained under telecommunications interception warrants issued in the current reporting period.

Initial review of these figures would suggest that CIT, even in its current state of use as an evidentiary gathering tool, is an effective technology. Approximately 63% of warrants issued resulted in arrests based on lawfully intercepted information, which would indicate effectiveness and compliance with the requirements of the TIA Act. Further, it is noted:

The tables may understate the effectiveness of interception in so far as, in some cases, prosecutions may be initiated, and convictions recorded, without the need to give intercepted information in evidence. In particular, agencies report that telecommunications interception effectively enables investigators to identify persons involved in, and the infrastructure of, organised criminal activities, particularly drug trafficking syndicates. In many cases, the weight of evidence obtained through telecommunications interception results in defendants entering guilty pleas, thereby obviating the need for the information to be introduced into evidence. (Attorney General's Department, 2008, p. 53)

This should again demonstrate that the use of CIT under the TIA Act is effective. This does not, however, illustrate the overall effectiveness of this manner of investigation on crime rates, nor does it provide any measure for the level of disruption caused by arrests, prosecutions and convictions from lawfully intercepted communication on criminal enterprises. The use of case studies does provide a more valuable means of examining the effectiveness as a tool against TOC. There is, however, limited evidence available.

The Public Affairs Unit of the Australian Government Attorney-General's Department produces an annual report detailing the issuance and effectiveness of all warrants requested and issued under the TIA Act. The report breaks down the type of warrant sought, the offence under investigation, the result of the investigation (arrests and seizures), name of the applicant agency and the length of time for the warrant to be active (and if required any renewal request).

A comparative analysis of data provided by the department for the period 2007–2010 saw a slight increase in the number of CIT warrant applications from authorized agencies from 3,254 in 2007 to 3,589 in 2010. It should be noted that of the 3,254 applications in 2007, eight applications were rejected while only five applications were rejected in 2010.

The analysis of data provided by the department for the period 2010–2012 further supported consistency in the number of applications and a

TABLE 6.2 *CIT warrant applications from 2007–2012*

	2007/2008	2008/2009	2009/2010	2010/2011	2011/2012
Applications	3254	3233	3589	3495	3764
Refused/Rejected	8	13	5	7	9
Issued	3246	3220	3584	3488	3755

similar number of rejected applications. In 2010, 3,548 applications were successful and in 2012, 3,755 applications were successful. The number of rejected applications remained constant at between 7–9 applications.

From the number of successful applications it is apparent that the use of CIT in investigations of serious and organized crime, official corruption and matters of national security that law enforcement and intelligence agencies are complying with the requirements of the Act surrounding the issuance of a communication intercept warrant and, further to this, LEAs are embracing the benefit of incorporating intelligence products, derived from telecommunication interception, into their investigations. Kisswani (2010) cited Australia as an example of best practice in relation to the balancing of individuals' right to privacy with the needs of the public interest:

In Australia, telecommunication interception is regulated by the Telecommunications (Interception & Access) Act 1979. The Act distinguishes between national security warrants and law enforcement warrants and sets forth specific procedures and requirements for each. Lawfully intercepted information is admissible as evidence in exempt proceedings or defined circumstances or for permitted purposes. By addressing both types of investigatory uses of telecommunications interception and access within one Act, distinctions can be made clearer and specific procedures and exceptions can be addressed with greater consistency; an approach recommended for development of any new regime.

As a means of illustrating the effectiveness of a systematic interception scheme, a case study of the use of the DSD in the cooperative investigation of the AFP and Indonesian National Police (INP) in the 2002 Bali Bombings was examined.

DSD–AFP case study

Two Telstra technicians flew into Indonesia two weeks after the October 12 bombings at the request of the AFP and with the knowledge of the INP. The technicians returned home from Jakarta after spending several days at the main link to Indonesia's government-owned telecommunications carrier, Telkomsel... they had with them a database of millions of phone numbers they handed over to DSD. Around the clock, the supercomputers of DSD and the US National Security Agency crunched the numbers, establishing call patterns and listening for key words. The data played a key role in the capture of one of the Bali plotters, Mukhlas. He was traced by his mobile phone to a small town in central Java, despite taking precautions such as changing

his SIM card every two days and speaking for only a few seconds at a time. Another Bali ringleader, Imam Samudra, was captured through electronic eavesdropping when he sent an indiscreet e-mail, alerting authorities to his movements. Electronic eavesdropping also played a key role in capturing fugitives after the second Bali bombing in October last year [2005]. The eavesdroppers at DSD and the AFP had never fallen off the hunt, but the second Bali strikes had given them renewed impetus to nail (bomb-maker) Azahari bin Husin once and for all. After the bombings, authorities homed in on three suspicious numbers, which they believe might have been used by Azahari and his bomb-making accomplice Noordin Top. They narrowed it down to one number, and traced it to a bus moving through east Java. When the bus pulled up, authorities discovered the man with the phone was Yahya Antoni, a courier for Azahari and Top. Within hours, Yahya had revealed Azahari's location, and authorities swarmed to the town of Batu, where they killed him in a shootout. (Stewart, 2006)

In the United Kingdom the Interception of Communications Commissioner (2012) reported the issuance of 2,911 lawful intercept warrants under Part 1 chapter 1 of RIPA (2000). This is the first time that the Commissioner has declared in open source material how many intercept warrants were authorized in a calendar year. Further to this the Commissioner reports that for the reporting year that his audit identified 42 errors representing 1.4% of the total number of intercept warrants signed in 2011. While this represented an increase in the number of reported errors the Commissioner was satisfied that none of the reported errors or breaches were deliberate. The audit identified two categories for errors: human and technical (Interception of Communications Commissioner, 2012, p. 17).

The Commissioner's ongoing support for the deployment of CIT as part of a broader investigative strategy in combating serious and organized crime, official corruption and matters pertaining to national security is evidenced by the citing of a specific case, the Serious and Organised Crime Agency (SOCA) case, in the 2011 Annual Report in which CIT proved to be invaluable.

SOCA Case Study

Background

This report concerns a SOCA investigation undertaken in 2009 and 2012. The details have been sanitised. Originating from a SOCA operation into the money laundering activities of a UK-based organised crime group

(OCG), two senior members of the OCG were identified as controlling its activities. The operational team had encountered significant difficulties in using conventional investigation techniques. As a result, SOCA considered it necessary and proportionate for these OCG members to be subject to interception. Interception commenced early 2009, and soon confirmed that the OCG was well established, and involved not only in money laundering but also in the importation of significant amounts of Class A drugs.

Operational Activity

Intercept intelligence made it possible to identify individuals involved in the transportation and storage of drugs on behalf of the OCG. The intelligence enabled SOCA officers to seize the drugs as they were being delivered to the OCG members. This resulted in a number of arrests and the seizure of more than 100 kilograms of Class A drugs, 1,400 kilograms of Class B drugs and the dismantling of this section of the OCG.

Intelligence later established that a linked OCG was importing Class A drugs using an alternative method. Interception enabled these individuals to be identified and disclosed the location of the consignment of drugs. This intelligence resulted in the seizure of over 150 kilograms of Class A drugs and more than £300,000 in cash.

Throughout 2010, interception identified other OCG members who were involved in money laundering on behalf of this OCG. This intelligence enabled the operational team to gather evidence of OCG members conducting this laundering activity, before arresting them and recovering in excess of £600,000 in cash.

Interception in 2011 revealed that the primary members of the OCG had resumed importations of Class A drugs into the UK and were arranging customers to collect drug consignments. This resulted in further arrests and the seizure of a further 150 kilograms of Class A drugs, a further seizure of 75 kilograms of Class B drugs, firearms and cash.

Conclusion

As a direct result of intelligence provided through CIT, in excess of 300 kg of Class A drugs, 1,780 kg of Class B drugs, three (3) firearms and more than £1,000,000 in cash were seized. More than 75 people were arrested.

(Source: Interception of Communications Commissioner, 2012, pp. 9–10)

It is evident from the above case studies that the interception of criminal communication can provide valuable and timely information. It can be seen that the DSD–AFP case illustrates a combination of processes at work that are important to transnational crime fighting. The cooperation

of the AFP and INP is an aspect that is consistent with the direction of international cooperation, indicated by Glenn, Gordon and Florescu (2008), that is required for TOC. The relationship between the AFP and DSD also illustrates the importance in combining agency skill sets to instigate the most effective response, rather than contribute wasted resources through overlapping purposes. While this particular case study examines the use in a reactive manner, similar use in a proactive manner can yield equal results, albeit ideally in a preventative manner. This is an essential aspect of effective communication interception use for TOC. This proactive approach was demonstrated in the lead-up to the 9/11 terrorist attacks in the US, in which the NSA and CIA had vast data and intelligence pertaining to the activities and movements of the involved terrorists resultant from intercepted communications with an Al Qaeda operations headquarters.

In addition, intelligence derived from intercept products such as those found in the SOCA case study can increase the understanding of how organized crime and terrorist groups operate, including furthering knowledge on importation methods, money laundering and their use of technology. Kisswani (2011) noted that interception activities in the UK and the US have led to significant arrests and seizures making it one of the most valuable tools in the crime-fighting arsenal. It could be argued that the advantages associated with the use of CIT are not just limited to arrests, seizures and forfeitures but also to many suspects pleading guilty, thus saving the state the time and expense of a lengthy court trial (Kisswani, 2011).

Issues surrounding communication interception technology

Whilst SIGINT has been used extensively and effectively in military environments for over a century it is difficult to comprehend why CIT continues to remain so severely limited in its use. In much of the literature there are three primary issues limiting the practical use of CIT within TOC and corruption investigations: legislation (governing usage), privacy and culture.

Legislative constraints

Whilst legislative constraints and privacy are seemingly separate they are directly correlated. The concerns regarding the infringement of

privacy rights have subsequently influenced the controls and limitations placed on the use of CIT within the legislation. The work of Starey (2005) analyses the legal framework that CIT operates under in Australia and makes comparisons to the applicable legislation in the US. Starey (2005) argues that, whilst Australia cannot directly adopt the same legislation applied in the US, we should be able to learn from their errors and debates to improve our own laws and increase their clarity (Starey, 2005). A common feature evident in both countries is the narrow restrictions on, and subsequent difficulty in, being issued a warrant for lawful interception. For live communication interception, warrants may only be issued for serious offences (matters of national security or offences punishable by a maximum period of at least seven years imprisonment), must be accompanied by strong evidence to support reasonable grounds for the suspects involvement, must take into regard the level of privacy to be interfered with, how useful the intercept will be, and what other investigative methods have been used (Starey, 2005; EFA, 2006). This issue of employing alternative investigative methods was also raised in NZ in the matter of *Hamed and Others v the Queen* in which surveillance evidence illegally obtained was excluded by the judiciary (Wall, 2012, pp. 199–201). Further, interception warrants can only be authorized by select Federal Judges or Administrative Appeals Tribunal members to authorized LEAs (Starey, 2005; EFA, 2006). Starey (2005) demonstrates that the current legislation caters for CIT only as a last resort option and serves a primary purpose as an evidence-gathering tool, rather than a forefront intelligence collection method. Stored communications, however, are significantly easier to access under the Amendment Act in which: requirements are for either serious offences or serious contraventions (penalty of at least maximum three years imprisonment); may be issued to all enforcement agencies, including criminal law, civil penalty and public revenue agencies; and can be issued by any federal, state or territory judge or magistrate.

As argued by privacy advocate Electronic Frontier Australia (2006), these responses seemingly position stored communications as a 'less important' communicative method, despite the increasing adoption and preference of these methods over live communication by individuals and business. Their position, however, is degraded due to the failure to recognize the advantages attached to CIT in law enforcement and the sole focus on rights to privacy.

In addition to the restrictions previously discussed, an important restriction on the use of the TIA Act is that the agency must be investigating crimes. As a result CIT could not be used in a corruption investigation that would only result in disciplinary action (nor do agencies have the power to share metadata obtained during a warranted investigation with other agencies which could use this data to enforce actions of official misconduct). This raises an interesting point being considered in Australia, where investigative agencies would like to share information with other agencies that were not a part of the investigation. For example, the CMC would like to be able to do this in cases where there is a time-sensitive emergency or sharing of information would be in the public interest (CMC, 2011). It is unlikely that a time-sensitive emergency would apply to a disciplinary matter, but it may well be very relevant under a public interest test. The case example they provide is one where an individual is being investigated in relation to child pornography but the CMC cannot share the information with the government agency that provides approval for the person to work with children; the agency is therefore prevented from taking industrial action which would remove that person's blue card, the ID necessary for all people working directly with children in Queensland (CMC, 2011).

Privacy constraints

It is not surprising that the process of focusing policing tactics and the implementation of a proactive approach in which a majority of policing work is not observable by the public is seen as a threat to perceived civil liberties by some, irrespective of the accuracy of their perceptions (Ratcliffe, 2008b). As noted by Innes (2004), these changes in policing methodology have been seen to increase the gap between those who are policing and those who are being policed. Subsequently, this apprehension of society and advocates alike regarding the issue of privacy must be addressed. Bronitt and Stellios (2005, 2006) raise concerns regarding the legislative framework that governs CIT within Australia, arguing that the model of 'balancing' law enforcement and privacy is fatally flawed. Similar views are held by privacy advocate groups such as Electronic Frontier Australia (2006), who argue that greater restrictions should be imposed on the use of CIT, and privacy should be placed at the forefront of all decision-making. Even though Australia's legal protection for privacy rights is limited, courtesy of the lack of a Constitutional Bill of Rights, protection is still afforded under article 17 of the International

Covenant on Civil and Political Rights and article 12 of the Universal Declaration of Human Rights. Irrespective, it would be illogical to make recommendations that ignore privacy on the whole. Porter (in Ratcliffe, 2008b, p. 223) highlights this concept by noting:

But intelligence-led policing also brings with it special challenges. While the police analytical function may be an effective tool for protecting the public from serious crime, information-gathering activities associated with intelligence-led policing may also infringe on the privacy and civil liberties of individuals. This type of information gathering requires the police to use more intrusive procedures, such as informants, undercover operations, electronic surveillance, and sophisticated intelligence analysis. Such intrusive procedures pose threats to civil liberties, privacy, and other rights... The potential threat to civil liberties, privacy, and other rights, therefore, is one of the special challenges facing intelligence-led policing and the development of any development of police information networks... It is therefore important for police organisations to put the protection of privacy and civil liberties 'up front' when implementing an ILP [intelligence-led policing] approach. The gathering of information for the police intelligence function is among the critical decision points in policing. Intelligence activity is also an area where law enforcement officers exercise considerable discretion that has seldom been subject to review from outside the police agency.

Viewing the intelligence process as a series of discretionary decisions and using policy and training to institute appropriate safeguards, therefore, can help protect privacy and civil liberties.

However, whilst it is undeniable that privacy is an important aspect of life it does still provide additional protection to criminals and criminal enterprises. Grabosky and Smith (1998) argue that the respect for an individual's privacy is not an absolute interest and is conversely subject to other competing interests of importance within society. The use of interception technology is justified when the social benefits of its use outweigh the cost of individual privacy. It is here that Electronic Frontier Australia (2006) lacks the ability to recognize the careful balance of proportionality between privacy and enforcement. As power shifts in favour of increased privacy it greatly limits vital enforcement technique and technology. Sir Robert Megarry VC explains in the case of *Malone v Metropolitan Police Commissioner* [1979] Ch 344 at 377D:

I think that one has to approach these matters with some measure of balance and common sense. The rights and liberties of a telephone subscriber are indeed important; but so also are the desires of the great bulk of the

population not to be the victims of assault, theft or other crimes. The detection and prosecution of criminals, and the discovery of project crimes, are important weapons in protecting the public... The question is not whether there is certainty that the conversation tapped will be iniquitous, but whether there is just cause or excuse for the tapping and for the use made of the material obtained by tapping.

The sentiments of Electronic Frontier Australia (2006) are also shared by Bronitt and Stellios (2005, p. 887), whose evaluation of the regulatory framework for CIT in Australia results in the rejection of the 'balancing' model and proposes the development of a regulatory model advocating human rights and due process as a 'paramount consideration'. Despite these claims, however, they fail to detail the proposed model aside from noting that it would be a 'radical departure from existing approaches'. A consistent theme in the works by Bronitt and Stellios (2005, 2006) relates to their concerns regarding the increasing use of interception technology by states and territories, rather than sole use by federal agencies. What Bronitt and Stellios (2005, 2006) fail to acknowledge is that the growth of organized and transnational criminals do not limit themselves to breaching only federal or state laws; indeed, they are well known to exploit proposed restrictions (Irwin, 2001). Providing all agencies with access to these methods is an integral part of the unification of Australian LEAs – a factor which is stressed as an essential requirement throughout the literature (Glenn, Gordon and Florescu, 2008; Irwin, 2001; Flood and Gasper, 2009; Ratcliffe, 2008b).

The concept of placing privacy 'up front' is clearly an important aspect to note. Whilst it is understandable for apparent reasons of operational security that transparent intelligence collection is unrealistic, options for building public trust and acceptance exist. Limiting unnecessary discretion and guiding necessary discretion within the decision-making process, introducing tests of proportionality and/or the use of an independent oversight role, such as Queensland's Public Interest Monitor, reinforce the notion of civil liberties as the highest priority, whilst still ensuring that the intelligence-led methodology can continue.

Intelligence and culture

As demonstrated throughout the chapters of this book, for the most effective law enforcement practice intelligence must be placed at the

centre of the organization's ethos. Intelligence must be recognized by LEAs as substantially more than just data or information collected using the stereotypical means of 'intelligence collection' relating to covert information gathering. There is an identified need to ensure that it is evident throughout an organization that intelligence is analysed information. This recognition needs to be supported by a cultural shift promoting the importance of support staff, such as crime intelligence officers and analysts, to centre stage. As noted by the work by Heldon (2009), Dean and Gottschalk (2007b), Ratcliffe (2008b, a; 2002 c; 2008), Oakensen, Mockford and Pascoe (2002) and Osborne (2006), for true intelligence-led policing (ILP) to be implemented – a methodology that relies on high-quality analysis – there would be a need to introduce education and training for all personnel so that a greater understanding of intelligence reports provides an appropriate decision-making regime. Ratcliffe and Sheptycki (2009) note that, currently, intelligence officers and analysts often see few results from their work and that 'intelligence reports collated centrally were said to disappear into an intelligence "black-hole" – a space where all information is swallowed-up but from where no light emerges' (Ratcliffe and Sheptycki, 2009, p. 249). Ratcliffe (2003, 2008b) goes further, noting that whilst seemingly melodramatic, it would be impossible to identify the number of intelligence failures that have occurred across the world as a result of decision-makers failing to identify the importance of an intelligence product, or an agency or analyst failing to convince their clients of its importance. The support of analysts, along with education and training of all personnel, is clearly an essential component of a successful and effective law enforcement methodology.

Intelligence sharing is also a key aspect of not just ILP but of the combat of organized crime on a transnational scale. Agencies both domestically and internationally need to shift from the model of informal networks to a more defined arena that promotes effective intelligence sharing (Dean and Gottschalk, 2007a; Bhaskar and Zhang, 2007; Ratcliffe, 2008b).

This extends through both law enforcement and security agencies. With TOC shifting and consorting in manners that pose threats to both crime control and national security it is no surprise that intelligence overlaps occur. With dissemination forming the final stage of the intelligence cycle (dependent on the model used, here referring to direction, collection, collation, analysis and dissemination) it is vital that there is a shift away from the reinforced cultural stigma that underpins hoarding of

information and refusal to volunteer intelligence for fear of losing their status of ‘importance’, which can be considered to be integral to continued funding (Bamford, 2009). The efficacy of a new intelligence-led model is greatly reduced without the transformation out of a competitive mindset. In line with the continued privacy concerns, it is also essential to ensure that appropriate privacy policies are in place for intelligence sharing systems – for only the slightest hint of a violation of rights and privacy of individuals will quickly see intelligence sharing and, in part, effective transnational policing succumb to a significant setback (Department of Justice, 2005; Ratcliffe, 2008b).

Chapter summary

The use of CIT in Australia and in other English-speaking Commonwealth countries is governed by legislation that aims to balance the right to privacy with the needs of public interest. A study of the literature has shown that, despite the military’s long history of using SIGNIT, CIT continues to remain severely limited in areas such as the fight against TOC and corruption. There is a dearth of literature surrounding the specific use of CIT, and its effectiveness remains difficult to measure. What is apparent from the literature, however, is that the key issues surrounding the use of CIT are legislation (governing usage), privacy concerns and culture. Also noted is that the most effective use of CIT is grounded within a proactive ILP framework. Despite these constraints, specific case studies cited in this chapter do provide a valuable means to examine the effectiveness of CIT as a tool against transnational crime. In particular they demonstrate how intelligence derived from intercept products can provide timely and valuable information, to be used to increase understanding of how criminal organizations operate, and lead to significant arrests and seizures.

7

Directions in Intelligence and Investigations

Abstract: *This chapter concerns the directions in intelligence and investigations relating to transnational organized crime (TOC) and official corruption. It identifies that the need for an intelligence-led approach to policing is apparent throughout the literature. Intelligence – which can be garnered through the use of communication interception technology (CIT) – needs to underpin both investigations of TOC and official corruption. However, as this chapter establishes, current policing strategies do not place intelligence at the centre of law enforcement doctrine. While investigators (both of TOC and corruption) have access to CIT powers, access to certain types of metadata which has the potential to support vital avenues of TOC and corruption investigations remain elusive as a result of societal concerns and current legislation.*

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

This chapter outlines the findings of a content and comparative analysis of documents surrounding the use of communication interception technology (CIT), in particular its use in the fight against transnational organized crime (TOC) and official corruption. The collated documents revealed a number of themes that illustrate the required direction of CIT and its use as a tool in combating TOC and official corruption. The chapter examines the findings of the document analysis, noting the four primary categories identified: intelligence direction, the intelligence-led policing model, the practical application of CIT, and its effectiveness.

Intelligence direction

A theme consistent throughout the literature of communication interception relates to the concept revealing the requirement for policing agencies to move forward from the traditional role of reactive policing, or 'local' policing, to a more proactive manner that utilizes intelligence as their foremost weapon in addressing the growth of TOC. Heldon (2009, p. 125) highlights this concept by stating:

Unfortunately, in the current law enforcement environment where policing agencies are at the forefront of combating terrorism, transnational crime as well as more 'traditional' community-level offences, understanding and information are critical. Intelligence must be able to support decision-makers to negotiate this environment.

The first section of this statement can be seen to identify that currently policing agencies lack a clear understanding of the nature of the criminal enterprises in TOC, corruption and terrorism that they are fighting. This is taken further to imply that this standard of understanding goes so far as to apply to the more 'minor' of crimes found within a specific locality, which one can assume includes vandalism, property crimes such as burglary, robbery and car theft, assaults and the like.

The second section of the statement requires little explanation: the use of intelligence, which can be derived from CIT, is an integral aspect for combating and identifying transnational crime. As such its use must be strategic. It is important here to reiterate that intelligence is not information. Intelligence is a form of data which has an attached relevance and purpose, and has been subject to an organized analysis by an intelligence officer or analyst (Dean and Gottschalk, 2007b).

This statement is further supported by Williams (1980, p. 35) following the Australian Royal Commission of Inquiry into Drugs, who also promotes intelligence-use by stating:

Intelligence is the most important single weapon in the armoury of law enforcement generally and of drug law enforcement in particular. Evidence received by this commission left no doubt that good intelligence is an essential prerequisite to effective law enforcement.

This reveals that, even during the raft of Royal Commissions that occurred during the 1970s and 1980s into the Australian law enforcement and intelligence community, the concept of underpinning intelligence-use as a primary resource in law enforcement methodologies was integral to the growing sphere of organized crime. The specific use of terminology is also important in this statement. The terms ‘good’ and ‘effective’ intelligence carry a similar ideology to that of Heldon (2009). It emphasizes that only information – data with clear relevance and purpose – subjected to analysis, not simply raw data misinterpreted as ‘intelligence’ (Ratcliffe 2008b; Oakensen, Mockford and Pascoe, 2002), will ensure the efficacy of law enforcement activity. It could be recognized that law enforcement can continue to be carried out without the use of good intelligence; it will simply remain reactive (and not proactive) with limited impact on crime control and prevention.

Resultant from the demonstrated need to utilize intelligence in a manner that provides ultimate direction to policing objectives and targets, it is further recognized that the use of a methodological framework, which correctly controls and harnesses the use of intelligence, is imperative. This is reinforced by Wardlaw and Boughton (2006, p. 142) who assert:

If intelligence is going to drive proactive policing, then it too must evolve – as must its organisational context. Intelligence needs to be seen as critical to decision-making within law enforcement. This means going beyond merely seeing intelligence as certain pieces of information that are critical to preventing specific criminal acts or solving specific crimes. Information has always been critical to successful policing. But clearly intelligence – if what is meant by intelligence is value-added analysis for decision-making – has not been... To a certain extent then, what is needed is a degree of internal marketing to turn around organisational cultures and place intelligence squarely where it belongs: at the heart of all strategic organisational decisions.

This statement effectively both summarizes and confirms the importance of intelligence, and CIT, as a vital component. As illustrated in the

statement, intelligence must be placed at the centre of the law enforcement doctrine rather than simply used as a support tool for investigations. This is an important aspect as it identifies the current flaws in the system of many policing agencies.

It goes further, recognizing that where there is a need for intelligence to be placed 'at the heart' of decision-making then there is a requirement to introduce a policing framework or methodology that doesn't simply encourage this change to happen but forces it to occur in recognition of the obstinate nature of law enforcement agencies (LEAs). Intelligence activity is therefore recognized as an essential part of policing practice, and it is this theme that reinforces the purpose of CIT. For without an established means and flow of data collection there can be no analysis and thus no intelligence product.

Corruption investigations

Corruption investigations have a different character to TOC. The intelligence issues for TOC must focus on the flexible nature of how criminals conduct their business. They can change merchandise, innovate new methods of transportation, change customers and come up with entirely new forms of crime. By comparison, corruption is far less flexible. Corrupt officials are fixed in their ability to sell their corrupt services; the basic structure of providing unfair advantage to others or pursuing one's own self-interest stay the same. The nature of government services is reasonably constant; police still police and other government agents still make decisions. The politicians are also participating in inflexible political structures and processes.

From the perspective of strategic and tactical corruption prevention, it is very useful to conduct risk analysis on the government environment. According to Transparency International (2011a, p. 1):

Corruption risk assessment is a (diagnostic) tool which seeks to identify weaknesses within a system which may present opportunities for corruption to occur. It differs from many other corruption assessment tools in that it focuses on the potential for – rather than the perception, existence or extent of – corruption. At its core a risk assessment tends to involve some degree of evaluation of the likelihood of corruption occurring and/or the impact it would have should it occur.

Corruption follows money and discretion. Whilst the act of corruption will remain similar for any public official, the direction in which money is

allocated and the individuals who hold discretionary power will change with time. For example, the whole world is moving towards a green energy future as a result of policies designed to mitigate climate change. Billions of dollars are now being spent on issues that received little attention in past decades. Much of this money is being spent in nations that have very poor records of corruption. The combination of money with opportunity can lead to increased corruption. As Transparency International (2011b, p. xxvi) points out:

Where huge amounts of money flow through new and untested financial markets and mechanisms, there is always a risk of corruption. Some estimate total climate change investments in mitigation efforts alone at almost US\$700 billion by 2020. Public investments of no less than US\$250 billion per annum will eventually flow through new, relatively uncoordinated and untested channels. In addition, pressure already exists to ‘fast-track’ solutions, further enhancing the risk of corruption.

Similar issues will arise in large investment areas in nations with otherwise good track records of low corruption. For example, the expansion of the coal seam gas industry in the United States, Canada and Australia has seen billions of dollars invested into these nations. The competition between companies has been tight and there will inevitably be a temptation to gain an advantage over competitors by reducing red tape or ensuring an outcome from a government decision-maker. While we are not making allegations that corruption has occurred, this new industry is an example of one that must be identified as an area that deserves special attention from anti-corruption agencies.

Intelligence – such as that provided by CIT – could prove invaluable in allowing investigations to proactively identify corruption networks or indeed the potential for acts of corruption to take place. If anything, time has provided an advantage to the investigator.

Data mining and data retention

One of the problems identified in earlier chapters for corruption investigators has been the lack of access to CIT powers. Almost universally these powers are now in the hands of most corruption watchdogs. In addition, the powers of surveillance have improved through advances in technology.

There is one privacy issue that stands in the way of both TOC and corruption investigations: access to metadata. Metadata includes that

information such as who created a message, when it was sent, who it was sent to and the location it was sent from.

Put simply, communications data is information about an electronic communication – a footprint left after accessing the Internet, sending an email, or making a phone call. It might, for example, include customer registration details, the date, time and duration of a communication, the phone number or email address of the sender and recipient, the amount of data up/downloaded, or the location of a mobile device from which a communication was made.

This information is useful to obtain a chronology of events for a transaction or series of transactions and build information on membership and links in a dark network. It can be extremely useful for a corruption investigation. If the agency knew that an individual was involved in corrupt activity their phone records could provide a full profile of their network. This would not be evidence of guilt on the part of others as the metadata does not provide the content of the communication, but it would provide the means to work out who the person was talking to. Some or most of this information would be innocuous; however, the metadata can inform investigation strategies. It would be highly suspicious if a police officer had been making phone calls to a known criminal. Also, politicians making decisions about a major project would have to explain why they were making personal phone calls to individuals who had submitted tenders for the project. Thus the metadata can support avenues of investigation in either TOC or corruption investigations.

Most metadata is easy to obtain because it often falls outside the category of information that requires a warrant. Surveillance powers have had difficulty keeping up with technology as communication methods move from standard fixed-line telephones to email, chat rooms, mobile phones, SMS and Skype. This has prompted many agencies to try to extend their powers to cover metadata from these non-traditional methods. The difficulty is that the data is no longer 'telecommunications data' but is held on IP networks; that is, it travels via the internet. Most suites of intelligence gathering legislation do not cover this data. Also the data is held by private corporations who are not under an obligation to retain the metadata (Brew, 2012). The Australian government is trying to address this gap by extending the powers of the intelligence agencies. The United Kingdom (UK) government (at the time of writing) is likely to pass the *Draft Communications Data Bill* which would amend the *Regulation of Investigatory Powers Act 2000*, to provide similar powers

in that nation. Other legislation also exists in the European Union's *Data Retention Directive* (2006) which has been made law in many member states. The United States (US) does not have such a law and recent attempts to implement one have failed. They instead rely on data mining powers under the *Patriot Act*, which has protections through Congressional oversight (Cohen, 2013).

In addition, the solution to this problem will not be easily negotiated. There are serious privacy issues relating to how this data will be used to produce profiles of individuals in the community (Lee, 2013). There are also public concerns about what the government does with the metadata it collects. Key amongst these is the misunderstanding that the content of communication is not being examined. This issue has recently been given publicity in the US in relation to its government's data mining powers (Feldmann, 2013). A further issue is the cost that will be passed on to small operators to equip themselves to retain the data (Colley, 2013).

Despite the unknowns as to how the collection of metadata and privacy concerns will be addressed what is apparent is that, if the legislative issues can be resolved, the addition of these powers would significantly improve investigations in both corruption and TOC.

Chapter summary

The need for an intelligence-led approach to policing is apparent throughout the literature. Intelligence – which can be garnered through the use of CIT – needs to underpin both investigations of TOC and official corruption. However, as this chapter has established, current policing strategies do not place intelligence at the centre of law enforcement doctrine. While investigators (both of TOC and corruption) have access to CIT powers, access to certain types of metadata remains elusive – information which has the potential to support vital avenues of TOC and corruption investigations.

With this in mind, the next chapter sets out a way forward, presenting a conceptual model for the integration of CIT into an intelligence-led framework.

8

Integrating Communication Interception Technology within Investigations

Abstract: This chapter presents a way forward for placing communication interception technology (CIT) within the investigative framework. It proposes a conceptual model demonstrating how CIT in general can be integrated into investigations and intelligence operations. Ensuring intelligence is central, the model places CIT within an intelligence-led policing (ILP) framework, supporting the integration of tacit knowledge by way of an overarching knowledge-managed policing philosophy. The model outlines five key elements: Intelligence Probe, Preliminary Investigation, Warrantless Inquiries, Warranted Inquiries and Post-operational Intelligence Analysis. While conceptual, the model seeks to generate discussion on the merits of integrating CIT within an ILP framework, while endeavouring to balance privacy concerns by ensuring that legal thresholds are met and all other avenues of investigation are exhausted.

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

This chapter presents a developmental model for the integration of communication interception technology (CIT) into investigations of transnational organized crime (TOC) and corruption. The model proposed is conceptual in nature and as such serves to demonstrate the theoretical integration of CIT strategies into such investigations and intelligence operations. The chapter addresses the impact of privacy, intelligence, knowledge-managed policing and organizational culture on the efficacy of the proposed conceptual model. The proposed model has a broad application with the jurisdictions discussed in this book, with Australia, the United Kingdom (UK), Canada and New Zealand (NZ) operating on a similar platform for TOC and corruption investigations and balancing the privacy rights of individuals against the public interest. In addition, similar standards in so far as the legal threshold governing the issuance of a CIT warrant apply across all four countries.

Crime intelligence in the intelligence-led policing model

The centrality of crime intelligence and data analysis in the intelligence-led policing (ILP) model has been identified as a crucial link to developing a model of best practice for the use of CIT. Currently CIT tends to be used as a resource for developing case-specific evidence, arguably due to the legislative restrictions. As Ratcliffe (2008b) states, the use of intelligence derived from covert information and techniques is essential for strategic planning, and strategic planning has a greater proactive and preventative nature than its traditional reactive counterparts do. It can be seen though, with CIT forming a critical part of ILP and the use of strategic planning and assessment, that a complete picture of the criminal environment can be developed and actions instigated to disrupt these activities (Ratcliffe, 2008b, a).

The primary issue underpinning the effectiveness of CIT is the lack of evidence available to support its use. As established in previous chapters, the figures supplied annually by LEAs in Australia in the *Annual Telecommunications (Interception and Access) Act 1979 (Cth) Report* only substantiates the grounds of impact of warrants on individuals. It does not ascertain the overall effectiveness of CIT's use on overall crime rates, nor does it provide any measure for the level of disruption caused by arrests, prosecutions and convictions from lawfully intercepted communication

on criminal enterprises. It cannot be denied that there is a clear lack of empirical research that provides solid evidence for this cause.

Whilst Grabosky and Smith (1998, 1999) provide examination of case studies utilizing CIT they are neither recent nor in-depth. It can be theorized that this is in part due to the classified nature of law enforcement and restrictive nature of disclosure provisions that exist in the legislation controlling the use of CIT. It is illogical to expect that LEAs and security agencies alike will be willing to detail recent operative successes and/or failures in the threat of exposing sensitive operational strategies, techniques and sources not known to criminal enterprises.

However, when placed in a knowledge-managed policing framework such as ILP, the effectiveness can be interpreted by the level of relevant and reliable information collected from interception sources and, with communication technologies increasing in their availability and adoption by general society, it is an area that requires continued monitoring and use.

Figure 8.1 provides a graphic depiction of how CIT can be integrated into an investigation, while at the same time maintaining the delicate balance between an individual's right to privacy and the public interest. Nesting CIT within an ILP framework supports the integration of tacit knowledge by way of an overarching knowledge-managed policing (KMP) philosophy. This tacit knowledge is described by Dean and Gottschalk (2007a) as 'know-how knowledge'. In an investigation of TOC or corruption an investigator's tacit 'know how' is critical to the outcome of the investigation. As discussed, Figure 8.1 incorporates several elements key to any investigation of TOC and corruption.

The intelligence probe

This component can best be described as an exploratory analysis of what is currently known about the criminal enterprise engaged in TOC or corruption. The Intelligence Probe analyses data from an array of existing sources, such as information repositories (various databases) and informants, and provides insight into the strengths, weakness, opportunities and threats posed by the criminal group. The Intelligence Probe provides investigative options for investigators to consider with respect to effectively targeting the criminal group.

Equally importantly, the Intelligence Probe identifies 'intelligence gaps' within a law enforcement agency's (LEAs) current holdings with

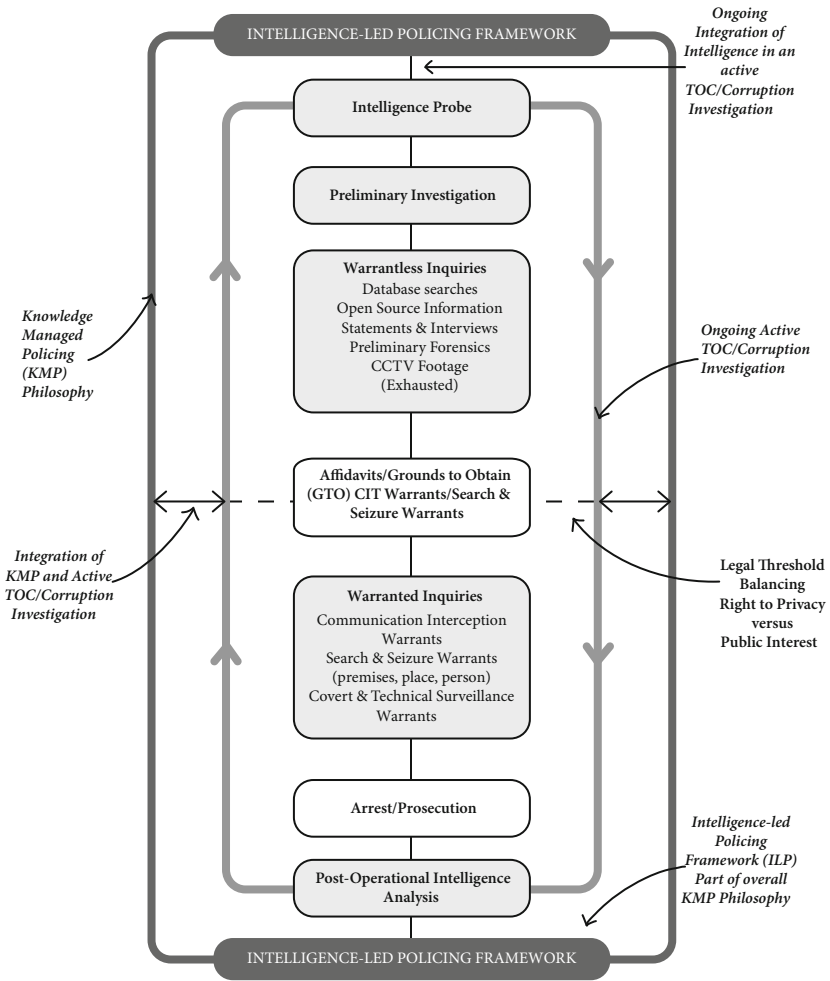


FIGURE 8.1 Conceptual framework for the integration of CIT into an active TOC/ corruption investigation

Source: Dr Peter Bell, Dr Mark Lauchs, Professor Geoff Dean and Mr Mitchell Congram, 2013

respect to the criminal group. Intelligence gaps are, as the name suggests, gaps in an LEA's knowledge of a criminal group. This may extend to include all of the members within the group, the full extent of the group's criminal activities and their respective *modus operandi*. These intelligence gaps could also include the primary source of finance for the

group's criminal activities and its preferred method of communication by group members.

Preliminary investigation

Based on the quality of the analysis contained in the Intelligence Probe, law enforcement executives may decide to escalate the matter to a preliminary investigation. This will result in assigning the probe to a team of experienced investigators who will initially seek to address the existing intelligence gaps in order to develop a greater understanding of the criminal group. During this phase of the investigative process, investigators and intelligence personnel will work closely together to develop information sources (HUMINT) and to gather evidence in support of a charge. The preliminary investigation endeavours to establish a *prima facie* case that can be brought before a court. In order to do this, investigators and intelligence personnel conduct what is collectively known as warrantless inquiries.

Warrantless inquiries

Warrantless Inquiries are elements of an investigation that do not require a warrant in order to secure information, intelligence or evidence of a criminal offence. Such inquiries may include the interviewing of a witness, debriefing of an informant, some forms of surveillance, preliminary forensic examinations and assessments, the interrogation of open source databases, a review of closed circuit television (CCTV) footage. At this point investigators will be able to determine if they have enough evidence to prove each and every element of a criminal offence or if further inquiries are needed. This is a key stage in an investigation and will determine which direction the investigation will take. Again, the analysis contained in the Intelligence Probe together with this new information, which seeks to satisfy the identified intelligence gaps, will be instrumental in directing the investigation. This is a critical element of the ILP framework as it may lead investigators and intelligence personnel towards the preparation and submission of affidavits or grounds to obtain a warrant (GTO).

Referred to as a GTO or Information to Obtain (ITO) in Canada, and an affidavit in Australia, the UK and NZ, these instruments are vital to securing a warrant. The Canadian Criminal Procedure and Practice/Search and Seizure/Warrant Searches (2012) (to be read in conjunction

with the Criminal Code of Canada) provides a succinct and universally applied definition of such an instrument:

An application for a search warrant consists of an 'Information to Obtain' (ITO) and usually a draft warrant that is presented to a justice of the peace or judge. An ITO consists of a statement under oath or an affidavit of an informant detailing the facts known (both first hand or second hand) that would provide basis to issue a warrant. An application for a warrant is an ex parte motion and as such must 'make full, fair and frank disclosure of all material facts'. (Cited cases: R. v. Debot (1986) 30 CCC 207 (Ont.CA) R. v. Richard (1996) 150 NSR 232 (NSCA) R. v. Araujo, 2000 SCC 65 (CanLII), 2000 SCC 65, [2000] 2 S.C.R. 992, at para. 46)

In this instance investigators must demonstrate that there is 'reasonable ground to believe' that the issuance of a warrant will enable the collection of evidence in support of a criminal offence. This standard is higher than 'reasonable grounds to suspect' and as such the information in the GTO/ITO/Affidavit needs to be compelling to an issuing authority. Successful GTO/ITO/Affidavits will result in the issue of a warrant for search, seizure, arrest and the use of specific forms of surveillance and permission to employ CIT. These subsequent avenues of investigation are referred to as *Warranted Inquiries*. At this stage of the investigation two key issues emerge: the need to ensure that the legal threshold is met, and the ongoing integration of tacit knowledge by investigators as part of the KMP philosophy.

Warranted inquiries

Warranted inquiries are elements of an investigation in which a warrant must be obtained from an approved issuing authority granting investigators permission to secure information, intelligence and or evidence in support of a criminal offence. They include search and seizure warrants, entry warrants, covert entry warrants, warrants to enter and re-enter a premises or place. Apart from warrants granting the release of confidential information such as financial records, a warrant is also required to grant the use of CIT and specific types of surveillance. In granting warrants authoring the use of CIT the authoring authority carefully considers the privacy rights of the individual and the public interest. By imbedding this application for CIT to be authorized within the ILP framework, investigators can demonstrate with confidence to the issuing authority that every possible alternative avenue of inquiry has been

exhausted before requesting a CIT warrant. It is anticipated that this will enable the issuing authority to issue the warrant (or refuse the application) on the basis that this standard has been met by the investigators and that the legal threshold has been met.

Following the successful application of a warrant authorizing the use of CIT, it is imperative that investigators adhere to the guidelines and policy set down that govern the use of CIT. Any subsequent breach may result in the warrant being revoked and any evidence obtained by investigators in breach of the guidelines rendered non-admissible in a court of law. A misconduct investigation hosted by the organizations professional standard units, or external organizations charged with investigating matters of misconduct may ensue, resultant from this breach of practice.

In the event that the use of CIT provides investigators with the evidence they need to prefer criminal charges, the suspect or suspects are arrested and charged and a brief of evidence is prepared and the offender(s) prosecuted in a competent court of law. It is important to ensure that another key intelligence product is prepared at this stage: the *Post-Operational Intelligence Analysis*.

Post-Operational Intelligence Analysis

The Post-Operational Intelligence Analysis assessment collects all of the intelligence obtained throughout the course of the investigation and examines the reliability and validity of information sources, analyses the investigative strategy (what was done well, areas for improvement, etc.) and if relevant, it may identify secondary and tertiary targets within the criminal group (or corrupt network). The assessment may also make recommendations to policymakers on what can be done to reduce the incidence of similar criminal (and corrupt) activity from occurring again in the future. The assessment makes a meaningful contribution to the organization's body of knowledge and as such completes the KMP and investigative loop as shown in Figure 8.1.

The Assessment is extremely useful in supporting subsequent investigations in which associates of those convicted may emerge as part of another criminal group or network of corruption. As shown in the proposed model, following the completion of the Post-Operational Intelligence Assessment, intelligence contained in this document may be used to support a subsequent Intelligence Probe and, as such, the ongoing fight against TOC and corruption continues.

From concept to practice

The proposed conceptual model for the integration of CIT into investigations of TOC and corruption seeks to generate discussion on the merits of integrating CIT within an ILP framework while supporting the underlying philosophy of KMP. The model proposed in this chapter takes a common sense approach to balancing the privacy rights of the individual and the public interest. Each phase in this conceptual model is coupled by timely, accurate and actionable intelligence. Progression through each phase of the investigation is contingent upon investigators receiving quality intelligence. This fundamental element underpins the ILP approach proffered by Radcliffe (2004) and supports the broader KMP philosophy advocated by Dean and Gottschalk (2007b). As such, the model is predicated on the assumption that individual LEAs within the selected jurisdictions support an ILP approach to TOC and corruption investigations and utilize intelligence in the manner in which it is intended; that is, proactively as opposed to reactively.

While conceptual in nature, the model forms the basis for the way forward in ensuring LEAs and corruption watchdogs are able to fully utilize CIT and are placing intelligence squarely at the centre of their investigations. Without such a model, investigations will not be able to match the 'fluid, dynamic and loosely structured networks' (Cressey, 1997; William, 2001) that are emerging in the global climate.

Chapter summary

Building on the findings of previous chapters, this chapter presents a way forward for the use of CIT in investigations into TOC and official corruption. It proposes a conceptual model demonstrating how CIT strategies can theoretically be integrated into investigations and intelligence operations. Recognizing the need to address privacy rights as well as place intelligence at the centre of policing methodologies, the model places CIT within an ILP framework, supporting the integration of tacit knowledge by way of an overarching KMP philosophy. The model outlines five key elements within the model: intelligence probe, preliminary investigation, warrantless inquiries, warranted inquiries and Post-Operational Intelligence Analysis. In doing so the model, while conceptual, seeks to generate discussion on the merits of integrating CIT

within an ILP framework, while endeavouring to balance privacy concerns by ensuring that legal thresholds are met and that all other avenues of investigation have been exhausted.

The next chapter discusses the issues that may potentially limit CIT's application in the fight against TOC and official corruption and hinder the development of the conceptual model proposed in this chapter.

9

Conclusion

Abstract: *Concluding the book, Chapter 9 provides an overview of the main findings from each chapter covering the topics of transnational organized crime (TOC), official corruption, policing methodologies, anti-corruption models, communication interception technology (CIT) and directions in intelligence and investigations. Touching on the conceptual model presented in Chapter 8 it discusses the way forward for ensuring CIT is integrated into an intelligence-led policing framework for use in Commonwealth countries with comparable legislation, taking into consideration the current and possible issues impacting the use of CIT in TOC and corruption investigations.*

Congram, Mitchell, Peter Bell, and Mark Lauchs.
Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology. Basingstoke: Palgrave Macmillan, 2013.
DOI: 10.1057/9781137333797.

The globalization and growth of transnational organized crime (TOC) and corrupt networks is a cause for great concern amongst society. While advancements in communication technologies have changed the communication landscape, they have also created opportunities for organized criminals to use the available technology for their own illegal gains. Organized crime can no longer be considered in relation to strict geographic boundaries – it now extends globally across a spectrum of activities including money laundering, drug trafficking, sex/human trafficking, people smuggling, arms trafficking, endangered species trafficking, cybercrime and, most notably over the last decade, terrorism (Abadinsky, 2009; Davies, 2007; Lyman and Potter, 2007; Australian Crime Commission, 2009; Borger, 2007; Grennan and Britz, 2006). Like TOC groups, corruption networks also make use of new and available technologies to advance their own illicit goals, and their structures pose great difficulties to those attempting to infiltrate and disrupt them.

However, while the increased availability of communication technologies and their usage presents opportunities for criminals and corrupt networks, it also presents opportunities for the law enforcement agencies (LEAs) tasked with fighting such crime and corruption. The need for two or more criminal or corrupt entities to exchange information regarding their planned activities is a critical point at which LEAs can disrupt those activities. As such, communication interception technology (CIT) presents itself as a crucial weapon to be harnessed by LEAs. However, despite its possibilities CIT remains drastically underutilized as an investigative tool and, while literature exists on TOC, official corruption and CIT, very few if any studies intersect to examine the theoretical or practical use of CIT as a tool to fight crime.

Recognizing the need to better understand how CIT is currently used, and could be used, to fight organized crime and official corruption, this book builds on existing literature on organized criminality, official corruption and CIT, drawing them together to provide a clearer overview of CIT's use in an enforcement and intelligence capacity. This is achieved by asking the following questions:

- 1 How effective is CIT in the fight against TOC and corruption? and;
- 2 How should the issues surrounding CIT be best managed within a practical law enforcement framework by English-speaking Commonwealth countries that share comparable legislative platforms?

In addition to addressing several gaps in the current literature, the research identifies the most appropriate policing methodology – intelligence-led policing (ILP) – to underpin the use of CIT and how it can be, or is currently being, restricted by the policing culture and privacy concerns present in various English-speaking Commonwealth countries. In doing so this publication contributes to the knowledge that can provide greater efficacy for law enforcement strategies and the disruption of the serious threat posed by official corruption and TOC to society.

Major findings

Using a qualitative design employing grounded theory the chapters in this book explore the relationship between CIT and its application in practical policing methodologies. Each chapter considers various elements of the research questions: transnational organized crime (Chapter 2), official corruption (Chapter 3), policing methodologies (Chapter 4), anti-corruption models (Chapter 5), CIT (Chapter 6), directions in intelligence and investigations (Chapter 7) and, finally, integrating CIT into investigations (Chapter 8). Each of these chapters provide a greater understanding of the issues and nature of the subject, working towards developing a framework (presented in Chapter 8) to embed the practical use of CIT as an investigative tool for use in the Commonwealth law enforcement community.

In reviewing the literature on TOC, Chapter 2 examined the specific structures of TOC groups and the impact these have on an LEA's ability to investigate their activities. The chapter identified that of the five main typologies (standard, hierarchy, regional hierarchy, clustered hierarchy, core group and criminal network) the 'core group' and 'criminal network' are the forms emerging in the current global climate and posing the greatest threat to LEAs and society. As noted by the Australian Crime Commission (2009), the organized crime groups that pose the most serious threat are those that are fluid, adaptable and resilient to LEA interventions, rebuilding quickly after disruptions.

Despite the lack of research to date on the vulnerabilities of criminal enterprises, by gaining a greater understanding of the structures of TOC groups it is possible to identify a core vulnerability that will only intensify as TOC continues to expand globally – the need to communicate quickly, easily and effectively. This presents a unique opportunity

for LEAs – the use of CIT to uncover, disrupt and investigate criminal activities. However, despite this opportunity and the numerous legal responses to TOC by Commonwealth countries including Australia, the United Kingdom (UK), Canada and New Zealand (NZ) – including the power to acquire communication including inception data – CIT’s use in fighting transnational crime remains limited. Chapter 2 highlights the need for a method and framework that will allow LEAs to combat TOC efficiently and effectively – one that requires the use of CIT as an investigative tool.

Similar to TOC, in order to combat and disrupt official corruption it is first necessary to understand the types of corruption, corruption networks and the current LEA responses. Chapter 3 addresses this by first considering the various forms of corruption and, in particular, corruption networks in relation to the police force and the public sector. Examining the notion of ‘dark networks’ (those networks that are both covert and illegal), the chapter identifies that while corrupt networks are extremely difficult to identify, infiltrate and destabilize, employing social network analysis and understanding the networks of corruption LEAs can target key network members, such as brokers, effectively using CIT to both identify other network members and eventually disrupt and destroy the network.

Having unpacked the current state and various issues surrounding TOC and official corruption and LEA and legal responses to these crime types, Chapter 4 considers the various policing methodologies employed by Australia, the UK, Canada and NZ and the role they have to play in the use of CIT as more than just a surveillance technique but rather as an investigative tool in its own right.

Chapter 4 identified the dearth of research focusing on ILP in relation to intelligence collection and the obvious disconnect in the literature between the use of CIT and ILP as a whole, although whether this is a result of the lack of literature concerning the practical use of CIT remains to be seen. What is apparent in the literature and the real-life examples illustrating the effective use of the ILP methodology in practice, however, is that of all the policing methodologies ILP is the only methodology that meets the requirements to combat TOC, namely: the ability to reveal a systematic and comprehensible environment from one that appears complex and haphazard through the collection, collation and analysis of data and the subsequent development of intelligence. ILP, therefore, can form the basis of an effective methodology into which

CIT can be integrated in order to give LEAs the ability to fully harness the capacity of CIT in the fight against TOC and official corruption.

The need to utilize intelligence to fight TOC is echoed in the techniques used to dismantle large corrupt networks – dark networks. As Chapter 5 illustrates, dark networks must be revealed through the gathering of intelligence with CIT being a particularly useful tool. By examining the structure and successes of independent corruption watchdogs, this chapter identifies basic powers essential to successful investigations, of which conducting surveillance, using surveillance technology (such as CIT) and granting indemnity are particularly important. With the primary aim of closing down the entire network, as opposed to simply catching individuals, social network analysis is a powerful tool to help expose people who have the greatest power to disrupt the network.

By selectively targeting people in a network CIT can be used covertly or with the cooperation of one party. In particular, CIT can be used to uncover sections of the network. By targeting a range of players from civilians (such as sex workers) to corrupt officials (such as police officers and politicians) the entire network may be uncovered or intelligence may be gathered to aid in decision-making, helping to identify those to offer indemnity to or those to target with surveillance. In some cases CIT can also be used to obviate the need for indemnities or cooperative network members by providing evidence of corrupt activities. Ultimately, Chapter 5 highlights that CIT is a crucial tool that enables corruption watchdogs to garner the intelligence and gather evidence necessary to disrupt and close down dark networks – intelligence without which the networks would most likely continue to thrive, hidden from public view.

However, despite its obvious benefits in both the fight against TOC and in current anti-corruption models, as Chapter 6 uncovers, CIT remains a largely untapped resource. Reviewing the literature currently available on CIT, this chapter explores the development and use of CIT in Australia and other English-speaking Commonwealth countries – the UK, Canada and NZ. Concerned with both ‘live’ communication (instant, real-time messages such as those conveyed over the phone) and ‘stored’ communication (those that are stored for a period of time on a piece of equipment before being accessed) in each of the countries studied, the use of CIT is governed by legislation that aims to balance the rights to privacy with the needs of public interest. Each country has provided its LEAs with investigative powers authorizing them to utilize

CIT; however, the legislation also presents a quagmire of legal requirements that hinder the effective use of CIT as an investigative tool.

In addition to covering the development of CIT and the various legislative responses from the Commonwealth countries studied, the chapter also importantly identifies the limitations surrounding the advancement of CIT in investigations of TOC and corruption. In providing a greater understanding of the use of CIT and presenting a policing model of theoretical best practice for CIT, the book uncovers issues and constraints that will limit the practical use of CIT: legislative constraints, privacy concerns and intelligence culture. It is unsurprising that privacy presents a severe limitation to the advancement of CIT – the very nature of CIT strategies, in which the majority of the investigative work is not observable by the public, means that it is seen as a threat to perceived civil liberties; the need to balance individual rights to privacy with public interest is paramount. However, as this chapter highlights, while transparent intelligence collection is unrealistic, opportunities exist to build public trust and acceptance – without this privacy concerns will continue to hinder the use of CIT in the fight against TOC and corruption. Likewise, a cultural shift is needed within the law enforcement community in order for true ILP methodologies to be implemented. Greater support and recognition for the work of intelligence analysts and a greater propensity for intelligence sharing – extending to both law enforcement and security agencies – are vital for effective transnational policing and the identification and closure of dark networks.

Despite the dearth of literature surrounding the practical use of CIT as an investigative tool, (as opposed to as a ‘surveillance’ technique) the chapter uncovers evidence regarding the effective use of CIT in two particular cases: the 2002 Bali Bombings involving Australia’s Defence Signals Directorate, and the investigation of a UK-based organized crime group by the UK’s Serious and Organised Crime Agency (SOCA). In particular, the cases illustrate how CIT can be used to provide valuable and timely information and garner intelligence leading to a better understanding of how organized crime and terrorist groups operate, including knowledge on their importation methods, money laundering and use of technology.

However, despite these illustrated successes and its long history of use in military contexts, it is clear from the literature that CIT remains underutilized as an investigative tool by LEAs, largely as a result of legislative constraints and privacy concerns.

Chapter 7 builds on these findings and considers the future directions in intelligence and investigations – in particular those that would aid the development of a proactive and intelligence-led framework that could underpin the use of CIT in the fight against TOC and official corruption. From current literature it is evident that there is a need for policing agencies to move towards a more proactive manner that utilizes intelligence as their foremost weapon against TOC and corruption. However, what is also evident is that LEAs currently lack a clear understanding of the nature of criminal enterprises in TOC, corruption and terrorism. Intelligence – which can be derived by CIT – must therefore be an integral aspect of combating and identifying TOC and dark networks; without an established flow of data collection there can be no analysis and therefore no intelligence product – it is this that CIT can provide.

However, despite the recognized need for intelligence and the access to CIT powers that currently exist, investigators remain on the back foot in relation to accessing certain metadata – information that can support avenues of investigation in either TOC or corruption investigations. For example, by knowing who created a message, when it was created, when it was sent, who it was sent to and where it was sent from investigators can create a chronology of events and build information on a network's membership and links.

In addition, it is clear that surveillance powers often lag behind technology and the communication methods that continue to evolve. As the chapter identifies, governments in Australia, the UK and Europe are attempting to bridge this gap while others such as the United States (US) have failed in their attempts. Indeed there is no simple solution to this problem, with an increase in powers attracting a myriad of privacy and cost concerns. However, what is clear is that if these issues can be resolved these powers would significantly improve investigations into both corruption and TOC.

Moving towards an integrated framework

Having investigated how effective CIT is in the fight against TOC and official corruption, Chapter 8 moves towards the second question of 'how is CIT best managed in a practical law enforcement framework?' In doing so it proposes a conceptual model that has a broad application for the jurisdictions discussed within this book. Based on the presumption

that LEAs in Australia, the UK, Canada and NZ support an ILP approach to TOC and corruption investigations, using intelligence in a proactive rather than a reactive manner, the proposed model seeks to integrate CIT within an ILP framework. The five phases outlined in the model – Intelligence Probe, Preliminary Investigation, Warrantless Inquiries, Warranted Inquiries and Post-operational Intelligence Analysis – aim to ensure that standards and legal thresholds are met for warranted inquiries, thus balancing privacy rights with public interest, as well as ensuring the ongoing integration of tacit knowledge by investigators as part of the knowledge-managed policing (KMP) philosophy.

While conceptual in nature the model serves to illustrate how intelligence can be placed at the centre of investigations into TOC and official corruption, allowing CIT to play a greater role in garnering the intelligence which is so often necessary to better understand the criminal or corruption networks under investigation.

Where to from here?

TOC is a diverse and complex area costing global society in excess of US\$3 trillion annually – a figure which is set to grow (Borger, 2007). Although having a different character to TOC, official corruption is no less damaging to society; billions of dollars are spent on issues of public concern – much of which is spent in nations that have very poor records of corruption. As highlighted in Chapter 5, police corruption itself has been endemic in countries with otherwise good track records of low corruption such as Australia and the US. The need to equip LEAs and corruption watchdogs with the necessary tools to uncover and fight these crimes is paramount.

This book has highlighted that while new communication technologies provide new opportunities for criminal and corrupt networks to expand their operations, they also provide a unique opportunity for LEAs and corruption investigators to disrupt these activities. By using CIT, investigators can garner timely and valuable information, better understand the structure and nature of the criminal entities they are targeting and uncover larger networks of criminal or corrupt operations. While the effectiveness of CIT is still difficult to determine based on current literature, what is apparent is that it presents a powerful tool to combat the new and evolving criminal structures and dark networks of

today's global environment. Its limited use in an investigative capacity is largely due to the legal complexities and privacy concerns surrounding its use, as well as the cultural issues which mean that intelligence often fails to truly take centre stage in an investigation. However, there is a way forward. While there are barriers to the effective use of CIT in investigations this book provides a conceptual model illustrating how CIT can be embedded in an ILP framework while still supporting the underlying philosophy of KMP. Taking a common sense approach the model seeks to balance the privacy rights of individuals – by ensuring legal thresholds are met – with the public interest, enabling investigators to access the necessary powers to utilize CIT in the effective investigation of TOC and corruption.

As stated by Williams (1980, p. 35), 'Intelligence is the most important single weapon in the armoury of law enforcement generally'; as this book attests, if embedded in a proactive ILP framework, CIT has the power to secure that intelligence, presenting as a powerful weapon in the fight against TOC and official corruption.

References

- Abadinsky, H. 1994. *Organized Crime*. 3rd ed. Chicago: Nelson Hall.
- Abadinsky, H. 2009. *Organized Crime*. 9th ed. Belmont, CA: Wadsworth Publishing.
- Adams, R. E., W. M. Rohe and T. A. Arcury. 2002. 'Implementing Community-Oriented Policing: Organizational Change and Street Officer Attitudes.' *Crime Delinquency*, 48 (3), 399–430.
- Ahmed, S. 2007. 'B-Party Intercepts and the Telecommunications (Interception) Amendment Act 2006 (Cth).' *Internet Law Bulletin*, 10 (1).
- Alchian, A. and H. Demsetz. 1972. 'Production, Information Costs, and Economic Organisation.' *The American Economic Review*, 62 (5), 777–795.
- Andreas, P. and E. Nadelmann. 2006. *Policing the Globe: Criminalization and Crime Control in International Relations*. New York: Oxford University Press.
- Armstrong, M. 2012. *They Wished They Were Honest: The Knapp Commission and New York City Police Corruption*. New York: Columbia University Press.
- Attorney General's Department. 2008. *Telecommunications (Interception and Access) Act 1979: Reporting for the year ending 30 June 2008*. Canberra: Public Affairs Unit, Attorney General's Department.
- Audit Commission. 1993. *Audit Commission Helping with Enquiries: Tackling Crime Effectively*. London: HMSO.
- Australian Crime Commission. 2009. *Organised Crime in Australia*. Canberra: Australian Crime Commission.

- Bakier, A. H. 2007. 'The New Issue of Technical Mujahid: A Training Manual for Jihadis.' *Terrorism Monitor*, 5 (6).
- Bamford, J. 2009. *The Spy Factory*. SBS (Broadcast 19 May 2009). Television Program.
- Baumeister, R. 1997. *Evil: Inside Human Violence and Cruelty*, Owl Books: New York
- Baumeister, R and M. Leary. 1995. 'The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation.' *Psychological Bulletin*, 117 (3), 497–529.
- Beck, A. 1999. *Prisoners of Hate: The Cognitive Basis of Anger, Hostility and Violence*. New York: Perennial.
- Becker, G. and G. Stigler. 1974. 'Law Enforcement, Malfeasance, and Compensation of Enforcers.' *The Journal of Legal Studies*, 3, 1–17.
- Beswick, S. and Connell, M. 2012. 'For your (government's) Eyes only, Review of the Search & Surveillance Act 2012.' *New Zealand Law Journal*, July 2012, 213–216.
- Bertrand, M, Djankov, S, Hanna, R. and S. Mullainathan. 2007. 'Obtaining a Driver's License in India: An Experimental Approach to Studying Corruption.' *Quarterly Journal of Economics*, 122 (4), 1639–1676.
- Bhaskar, R. and Y. Zhang. 2007. 'Knowledge Sharing in Law Enforcement: A Case Study.' *Journal of Information Privacy & Security*, 3 (3), 45–68.
- Block, A. 1994. *East Side-West Side: Organizing crime in New York City 1930–1950*. New Jersey: Transaction.
- Block, L. 2008. 'Combating Organised Crime in Europe: Practicalities of Police Cooperation.' *Policing*, 2 (1), 74–81.
- Blok, A. 1974. *The Mafia of a Sicilian Village 1860–1960: A Study of Violent Peasant Entrepreneurs*. New York: Harper & Row.
- Borger, J. 2007. 'Organised Crime: The \$2 Trillion Threat to the World's Security.' *The Guardian*. 12 September. <http://www.guardian.co.uk/world/2007/sep/12/topstories3.mainsection>
- Bouchard, M. 2007. 'On the Resilience of Illegal Drug Markets.' *Global Crime*, 8 (4), 325–344.
- Brady, H. 2008. 'Europol and the European Criminal Intelligence Model: A Non-State Response to Organised Crime.' *Policing*, 2 (1), 103–109.
- Braga, A. A. and D. Weisburd. 2006. 'Problem-Oriented Policing: The Disconnect between Principles and Practice.' In *Police Innovation*:

- Contrasting Perspectives*, Ed. A. A. Braga and D. Weisburd, 133–152. New York: Cambridge University Press.
- Branch, P. A. 2003. 'Lawful Interception of the Internet.' *The Australian Journal of Emerging Technologies and Society*, 1 (1), 1–7.
- Bronitt, S. and J. Stellios. 2005. 'Telecommunications Interception in Australia: Recent trends and regulatory prospects.' *Telecommunications Policy*, 29 (11), 875–888.
- Bronitt, S. and J. Stellios. 2006. 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?' *Prometheus*, 24 (4), 413–428.
- Brown, N. and D. Abrams. 2003. 'Despicability in the Workplace: Effects of Behavioral Deviance and Unlikeability on the Evaluation of In-Group and Out-Group Members.' *Journal of Applied Social Psychology*, 33 (11), 2413–2426.
- Brunetti, A. and B. Weder. 2003. 'A Free Press is Bad News for Corruption.' *Journal of Public Economics*, 87, 1801–1824.
- Burt, R. S. 1992. *Structural Holes: The Social Structure of Competition*. Cambridge, Mass.: Harvard University Press.
- Burt, R. S. 2005. *Brokerage and Closure: An Introduction to Social Capital*. New York: Oxford University Press.
- Caccioloa, D. 2009. *The Second Father: An Insider's Story of Cops, Crime and Corruption*. Brisbane: University of Queensland Press.
- Cahill, L. and P. Marshall. 2004. *The Worldwide Fight Against Transnational Organised Crime: Australia*. Canberra: Australian Institute of Criminology.
- Cairncross F. 1997. 'From Circuits to Packets.' *The Economist*, September 13, pp. 25–27.
- Calderoni, F. 2010. 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation, Crime, Law and Social Change.' *Springer Science and Business*, 54, 339–357.
- Canadian Department of Justice. 2010. *Consultation Document to the New Investigative Powers for the 21st Century Act 2012*, Office of the Minister of Justice, Ottawa, pp. 1–15.
- Carley, K. M., Lee, J. S. and D. Krackhardt. 2002. 'Destabilizing Networks.' *Connections*, 24 (3), 31–34.
- Carter, W. 1997. *Police and Drugs: A Report of an Investigation of Cases Involving Queensland Police Officers*. Brisbane: Crime and Misconduct Commission.

- Carter, D. and Barker, T. 1991. *Police Deviance*. Ohio USA: Anderson Publishing pp. 153–167.
- Caspi, A., Moffitt, T. E., Silva, P. A., Stouthamer-Loeber, M., Krueger, R. F. and P. S. Schmutte. 1994. 'Are Some People Crime-prone? Replications of the Personality-Crime Relationship Across Countries, Genders, Races, and Methods.' *Criminology*, 32 (2), 163–196.
- Castells, M. 1996. *The Rise of the Network Society: The Information Age: Economy, Society and Culture Vol1*. Oxford: Blackwell.
- Centre for Problem Oriented Policing. 2009. Centre for Problem Oriented Policing. <http://www.popcenter.org> (accessed 27 August 2009).
- Chalk, P. and W. Rosenau. 2004. *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*. Santa Monica: RAND Corporation.
- Chalk, P., R. Warnes, L. Clutterbuck and A. Kirby. 2009. *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom*. Santa Monica: RAND Corporation.
- Chan, J. B. L. 1997. *Changing Police Culture*. Melbourne: Cambridge University Press.
- Chan, J. 1999. 'Governing Police Practice: Limits of the New Accountability.' *The British Journal of Sociology*, 50 (2), 251–270.
- Christopher, S. and N. Cope. 2009. 'A Practitioner's Perspective of UK Strategic Intelligence.' In *Strategic Thinking in Criminal Intelligence*, Ed. J. H. Ratcliffe. 2nd ed, 235–247. Sydney: The Federation Press.
- Coady, C. 1996. 'On Regulating Ethics,' in M. Coady and S. Bloch (Eds) *Codes of Ethics and the Professions*. Melbourne University Press: Melbourne.
- Cohen, T. 2013. 'Data mining revelation opens political Pandora's box.' CNN. 9 June 2013. (accessed 27 June 2013) <http://edition.cnn.com/2013/06/07/politics/data-mining-after-9-11>
- Coles, N. 2001. 'It's Not What You Know – It's Who You Know that Counts.' *The British Journal of Criminology*, 41 (4), 580–594.
- Colley, A. 2013. 'Data laws would hit smaller providers.' *The Australian*. 2 April 2013. (accessed 27 June 2013) <http://www.theaustralian.com.au/australian-it/government/data-laws-would-hit-smaller-providers/story-fn4htb90-1226610437600>
- Congram, M. and P. Bell. 2010. 'Laying the Groundwork for the Successful Deployment of Communication Interception Technology

- (CIT) in Modern Policing.' *International Journal for Policing, Intelligence and Counter Terrorism*, 5 (1), 9–27.
- Conklin, J. E. 2009. *Criminology*. 10th ed. Boston: Pearson.
- Conser, J. A., G. D. Russell, R. Paynich and T. E. Gingerich. 2005. *Law Enforcement in the United States*. 2nd ed. Sudbury, MA: Jones and Bartlett Publishers.
- Cornall, R. 2005. 'Australia's Responses to Transnational Crime in the Region.' *Public Administration Today*, 4 (1), 61–65.
- Council of Europe. 2011. Convention on Cybercrime (CECC), Strasbourg, France. Date accessed, 21 July 2013, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
- Coyne, J. and Bell, P. 2011a. 'The Rise and Role of Strategic Intelligence in Law Enforcement: A Literary Review.' *Journal of Policing, Intelligence and Counter Terrorism*, 6 (7).
- Coyne, J. and Bell, P. 2011b. 'The Role of Strategic Intelligence in Anticipating Transnational Organised Crime: A Literary Review.' Submitted to the *International Journal of Criminal Law and Justice*, 39 (1).
- Cressey, D. R. 1997. 'The Functions and Structure of Criminal Syndicates.' In *Understanding Organized Crime in Global Perspective*, Ed. P. J. Ryan and G. E. Rush, 3–15. London: Sage Publications.
- Crime and Misconduct Commission (CMC). 2011. *Operation Tesco: Report of an Investigation into Allegations of Police Misconduct on the Gold Coast*. Brisbane: Crime and Misconduct Commission.
- Criminal Intelligence Service of Canada (CISC). 2006. Annual Report, Canadian Government, Ottawa Canada.
- Davies, Cole S. 2007. JSB982 *Transnational Organised Crime: Statistics/ Typologies of Transnational Organised Crime*. Queensland University of Technology.
- Dean, G., Bell, P. and M. Lauchs. 2010. 'Conceptual Framework for Managing Knowledge of Police Deviance.' *Policing and Society*, 20 (2), 204–221.
- Dean, G., Bell, P. and Newnham, J. 2012. 'Social Network Media and Political Activism: A Review of the Literature.' *Pakistan Journal of Criminology*, 3 (3).
- Dean, G. and P. Gottschalk. 2007a. *Knowledge Management in Policing and Law Enforcement*. Oxford: Oxford University Press.
- Dean, G. and P. Gottschalk. 2007b. *Knowledge Management in Policing and Law Enforcement: Foundations, Structures, Applications*. Oxford: Oxford University Press.

- Denzin, N. and Y. Lincoln. 2005. *The Sage Handbook of Qualitative Research*. 3rd ed. Thousand Oaks, CA: Sage Publications.
- Department of Justice. 2005. *Fusion Centre Guidelines*. Washington DC: Department of Justice.
- Dombrink, J. 1988. 'The Touchables: Vice and Police Corruption in the 1980's.' *Law and Contemporary Problems*, 51 (1), 201–232.
- Eck, J. E. and D. Rosenbaum. 1994. 'The New Police Order: Effectiveness, Equity and Efficiency in Community Policing.' In *The Challenge of Community Policing: Testing the Promises*, Ed. D. Rosenbaum, 3–26. Thousand Oaks, CA: Sage Publishing.
- Electronic Frontier Australia (EFA). 2006. Telecommunications Interception & Access Laws. <http://www.efa.org.au/Issues/Privacy/tia.html> (accessed 14 April 2009).
- Feldmann, L. 2013. 'Obama on NSA Data-mining: "Nobody is Listening to your Telephone Calls"'. *The Christian Science Monitor*, 7 June, 2013 (accessed 27 June 2013). <http://www.csmonitor.com/USA/DC-Decoder/2013/0607/Obama-on-NSA-data-mining-Nobody-is-listening-to-your-telephone-calls-video>
- Fitzgerald, G. E. 1989. *Report of a Commission of Inquiry Pursuant to Orders in Council*. Brisbane: Queensland Parliament.
- Flood, B. 2004. 'Strategic Aspects of the UK National Intelligence Model.' In *Strategic Thinking in Criminal Intelligence*, Ed. J. H. Ratcliffe, 37–52. Sydney: The Federation Press.
- Flood, B. and R. Gasper. 2009. 'Strategic Aspects of the UK National Intelligence Model.' In *Strategic Thinking in Criminal Intelligence*, Ed. J. H. Ratcliffe. 2nd ed, 47–65. Sydney: The Federation Press.
- Folsom, R. 2010. *The Money Trail: How Elmer Irey and His T-Men Brought Down America's Criminal Elite*. Washington, DC: Potomac Books.
- Gambetta, D. 2009. *Codes of the Underworld: How Criminals Communicate*. USA: Princeton University Press.
- Gerber, T. and S. Mendelson. 2008. 'Public Experiences of Police Violence and Corruption in Contemporary Russia: A Case of Predatory Policing?' *Law & Society Review*, 42, 1–44.
- Glaser, B. G. 1978. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*. Mill Valley, CA: Sociology Press.
- Glaser, B. G. 1992. *Basics of Grounded Theory Analysis*. Mill Valley, CA: Sociology Press.

- Glaser, B. G. 1998. *Doing Grounded Theory: Issues and Discussions*. Mill Valley, CA: Sociology Press.
- Glaser, B. G. and A. L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company.
- Glenn, J. C., T. J. Gordon and E. Florescu. 2008. *2008 State of Future*. Washington DC: World Federation of UN Associations.
- Goel, R. and D. Rich. 1989. 'On the Economic Incentives for Taking Bribes.' *Public Choice*, 61 (3), 269–275.
- Goldstein, H. 1987. 'Toward Community-Oriented Policing: Potential, Basic Requirements and Threshold Questions.' *Crime and Delinquency*, 33 (1), 6–30.
- Goldstein, H. 1990. *Problem Oriented Policing*. Ohio: McGraw-Hill.
- Gottfredson, M. and T. Hirschi. 1990. *A General Theory of Crime*. Stanford: Stanford University Press.
- Grabosky, P. and R. Smith. 1998. *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. Sydney: The Federation Press.
- Grabosky, P. and R. Smith. 1999. 'Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities.' *The FBI Law Enforcement Bulletin*, July.
- Granitz, N. and J. Ward. 2001. 'Actual and Perceived Sharing of Ethical Reasoning and Moral Intent Among In-Group and Out-Group Members.' *Journal of Business Ethics*, 33, 299–322.
- Granovetter, M. 1992. 'Problems of Explanation in Economic Sociology.' In N. Nohria and R. Eccles (Eds), *Networks and Organizations: Structure, Form and Action*. Boston: Harvard Business School Press.
- Grennan, S. and M. T. Britz. 2006. *Organized Crime: A Worldwide Perspective*. Upper Saddle River, NJ: Pearson Prentice Hall.
- Grossman, D. 1995. *On Killing*. Back Bay Books, Boston.
- Guriev, S. 2004. 'Red Tape and Corruption.' *Journal of Development Economics*, 73, 489–504.
- Haller, M. 1990. 'Illegal Enterprise: A Theoretical and Historical Interpretation.' *Criminology*, 28, 207–236.
- Heidenheimer, A. and M. Johnston. 2002. *Political Corruption*. New York: Transaction Books.
- Heldon, C. 2009. 'Exploratory Analysis Tools.' In *Strategic Thinking in Criminal Intelligence*, Ed. J. H. Ratcliffe. 2nd ed. 124–146. Sydney: The Federation Press.

- Herbert, J. and T. Gilling. 2004. *The Bagman*. Sydney: ABC Books.
- Hornle, J. 2010. 'How to Control Interception – Does the UK Strike the Right Balance?' *Computer Law & Security Review*, 26, 649–654.
- Hughes, A. 1999. 'Liaison Officers Play a Major Role in Australia's Fight Against Transnational Crime.' *AFP News*, 86 (1), 10–12.
- Independent Commission Against Corruption (ICAC). 2012. *Anti-Corruption Safeguards and the NSW Planning System*. Sydney: Independent Commission Against Corruption.
- Independent Commission Against Corruption (ICAC), NSW. 2008. *Report on an Investigation into Corruption Allegations Affecting Wollongong City Council, Pt 2*. Sydney: Independent Commission Against Corruption.
- Innes, M. 2004. 'Reinvesting Tradition? Reassurance, Neighbourhood Security and Policing.' *Criminal Justice*, 4 (2), 151–171.
- Interception of Communications Commissioner. 2012. *2011 Annual Report*. The Stationary Office Ltd, on behalf of Her Majesty's Stationary Office, pp. 1–64.
- Irwin, M. P. 2001. 'Policing Organised Crime.' In *4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses*. Canberra: Australian Institute of Criminology.
- Ivkovic, S. 2003. 'To Serve and Collect: Measuring Police Corruption.' *Journal of Criminal Law & Criminology*, 93 (2/3), 593–650.
- Jackson, B. A., P. Chalk, R. K. Cragin, B. Newsome, J. V. Parachini, W. Rosenau, E. M. Simpson, M. Sisson and D. Temple. 2007. *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*. Santa Monica: RAND Corporation.
- John, T. and M. Maguire. 2003. 'Rolling Out the National Intelligence Model: Key Challenges.' In *Crime Reduction and Problem-Oriented Policing*, Ed. T. Newburn, T. Williamson and A. Wright, 38–68. Cullompton: Willan Publishing.
- Jones, J. and D. Carlson. 2004. *Reputable Conduct: Ethical Issues in Policing and Corrections*. Upper Saddle River: Pearson Prentice Hall.
- Kaza, S., Daning, H. and C. Hsinchun. 2007. *Dynamic Social Network Analysis of a Dark Network: Identifying Significant Facilitators*. Intelligence and Security Informatics, 2007 IEEE.
- Keast, R. and K. Brown. 2002. 'The Government Service Delivery Network: A Case Study of the Push and Pull of Central Government.' *Public Management Review*, 4 (4), 439–459.

- Keast, R., Waterhouse, J., Murphy G. and K. Brown. 2011. *Pulling it All Together: Design Considerations for an Integrated Homelessness Service System – Place-based Network Analysis*. A report for the Department of Families, Housing, Community Services and Indigenous Affairs' (FaHCSIA).
- Keelty, M. 2004. 'Can Intelligence Always be Right?' In *13th Annual Conference of the Australian Institute of Professional Intelligence Officers*. Melbourne: AIPIO.
- Kennedy, G. A. 2004. *Royal Commission in Whether There has been Corrupt or Criminal Conduct by any Western Australian Police Officer*. Perth: West Australian Government Printer.
- Kisswani, N. M. 2011. 'The Reasonable Necessary for the Implement of Telecommunication Interception and Access Laws.' *International lawyer*, 45, 3(Fall), 857–885.
- Kisswani, N. M. and Anas A. Al-Bakri. 2010. 'Regulating the Use of Electronic Signatures Given the Changing Face of Contracts.' *Macquarie Journal of Business Law*, Vol. 7 in Hein Online, date accessed 20 July 2013, <http://heinonline.org/HOL/LandingPage?handle=hein.journals/macqjbul7&div=9&id=&page>
- Kleemans, E. and H. Van de Bunt. 2008. 'Organised Crime, Occupations and Opportunity.' *Global Crime*, 9 (3), 185–197.
- Kleemans, E. R. and C.J. de Poot. 2008. 'Criminal Careers in Organized Crime and Social Opportunity Structure.' *European Journal of Criminology*, 5 (1), 69–98.
- Kleinig, J. 1996. *The Ethics of Policing*. Cambridge: Cambridge University Press.
- Knapp, W. 1972. *Commission to Investigate Allegations of Police Corruption and the City's Anti-Corruption Procedures*. New York: Knapp Commission.
- Kooiman, H. 1993. *Modern Governance: New Government-society Interactions*. Sage: London.
- Kwok, T. 2003. 'Activities of the Hong Kong Independent Commission Against Corruption (ICAC): Its Investigative Technique.' *LAWASIA A Dynamic Asia Pacific: Legal Issues in 2003 and Beyond*, Tokyo, 1–5 September, 2003.
- Laub, J. H. and R.J. Sampson. 2003. *Shared Beginnings, Divergent Lives: Delinquent Boys to Age 70*. Cambridge, Mass.: Harvard University Press.

- Lauchs, M. 2007. 'Rational Avoidance of Accountability.' *QUT Law and Justice Journal*, 7 (2), 10.
- Lauchs, M., Keast, R. and D. Chamberlain. 2011. Resilience of a Corrupt Police Network: The First and Second Jokes in Queensland. *Crime, Law and Social Change*, 57 (2), 1–13.
- Lauchs, M. and S. Merrington. 2012. 'Noble Cause Corruption: The Wood Inquiry.' In *19th Annual Conference of the Australian Association for Professional and Applied Ethics*, 28 June–1 July 2012, University of Queensland, Brisbane, QLD.
- Lauchs, M. and Z. Staines. 2012. 'Career Path of a Corruption Entrepreneur.' *Global Crime*, 13 (2), 109–129.
- Lee, M. 2013. 'Coalition wants Money for ASIO, but Greens want Privacy.' 28 May 2013, ZDNet. (accessed 27 June 2013) <http://www.zdnet.com/au/coalition-wants-money-for-asio-but-greens-want-privacy-7000015941/>
- Leong, A. 2008. *The Disruption of International Organised Crime: An Analysis of Legal and Non-Legal Strategies*. Hampshire: Ashgate Publishing.
- Leyden, J. 2009. 'Italian Crooks use Skype to Frustrate Wiretaps.' *The Register*. 16 February. http://www.theregister.co.uk/2009/02/16/italian_crooks_skype/
- Lyman, M. D. and G. W. Potter. 2007. *Organized Crime*. 4th ed. New Jersey: Pearson Prentice Hall.
- Malkin, S. 2007. 'Social Networks of Organized Crime: Towards a Communication Approach.' *Proceedings of the National Communication Association 93rd Annual Convention*, 15 November, Chicago.
- Manning, P. K. 2005. 'Problem Solving?' *Criminology and Public Policy*, 4 (2), 149–154.
- Mars, G. 1994. *Cheats at Work: An Anthropology of Workplace Crime*. Aldershot, Hants: Dartmouth.
- Martin, B. 2012. 'Corruption Tactics: Outrage Management in a Government Scandal.' *Resistance Studies Magazine* (February), 1–40.
- Mason, J. 2002. *Qualitative Researching*. 2nd ed. Thousand Oaks: Sage Publications.
- McCusker, R. 2006. 'Review of Anti-corruption Strategies.' Technical and Background Paper No. 23. Canberra: Australian Institute of Criminology.

- McIllwain, J. 1999. 'Organized Crime: A Social Network Approach.' *Crime, Law and Social Change*, 32 (4), 301–323.
- Milward, H. B. and Raab, J. 2003. 'Dark Networks as Problems.' *Journal of Public Administration Research and Theory*, 13 (4), 413–439.
- Milward, H. B. and J. Raab. 2006. 'Dark Networks as Organizational Problems: Elements of a Theory.' *International Public Management Journal*, 9 (3), 333–360.
- Moffitt, T. E. 1997. 'Adolescence-Limited and Life-Course-Persistent Offending: A Complementary Pair of Developmental Theories.' In T. P. Thornberry (Ed.), *Developmental Theories of Crime and Delinquency*. 11–54. New Brunswick: Transaction Publishers.
- Morselli, C. 2001. 'Structuring Mr Nice: Entrepreneurial Opportunities and Brokerage Positioning in the Cannabis Trade.' *Crime, Law and Social Change*, 35, 203–204.
- Morselli, C. 2009. *Inside Criminal Networks*. New York: Springer New York.
- Morselli, C. and P. Tremblay. 2004. 'Criminal Achievement, Offender Networks and the Benefits of Low Self-Control.' *Criminology*, 42 (3), 773–804.
- Myerson, R. 2011. *Towards a Theory of Leadership and State-building*. Chicago: University of Chicago.
- Nagin, D. S. and D. Farrington. 1992. 'The Stability of Criminal Potential from Childhood to Adulthood.' *Criminology*, 30 (2), 235–260.
- Nagin, D. S., Farrington, D. P. and T. Moffitt. 1995. 'Life-course Trajectories of Different Types of Offenders.' *Criminology*, 33 (1), 111–139.
- Neuman, L. W. 2006. *Social Research Methods: Qualitative and Quantitative Approaches*. 6th ed. Massachusetts: Allyn and Bacon.
- Newnham, J. and P. Bell. 2012. 'Social Network Media and Political Activism – A Growing Challenge for Law Enforcement.' *Journal for Policing, Intelligence & Counter Terrorism*, 7 (1).
- New Zealand Ministry of Justice. 2011. *Strengthening New Zealand's resistance to Organised Crime*. August. New Zealand Government, Wellington, pp. 6–20.
- Nicholson, R. 2010. *Government of Canada Introduces Legislation to Fight Crime in Today's High-tech World*. Office of the Minister for Justice, Ottawa, 1–2.

- Nickerson, R. 1998. 'Confirmation Bias: A Ubiquitous Phenomenon in Many Guises.' *Review of General Psychology*, 2 (2), 175–220.
- Oakensen, D., R. Mockford and C. Pascoe. 2002. 'Does There Have to be Blood on the Carpet? Integrating Partnership, Problem-Solving and the National Intelligence Model in Strategic and Tactical Police Decision-Making Processes.' *Police Research and Management*, 5 (4), 51–62.
- Office of Police Integrity. 2008. *The Victorian Armed Offenders Squad – A Case Study*. Melbourne: Office of Police Integrity.
- Osborne, D. 2006. *Out of Bounds: Innovation and Change in Law Enforcement Intelligence Analysis*. Washington DC: Joint Military Intelligence College.
- O'Toole, L. and K. Meir. 2004. 'Desperately Seeking Selznick: Cooptation and the Dark Side of Public Management in Networks.' *Public Administration Review*, 64 (6), 681–693.
- Padraic, S. 2005. *Confessions of a Crooked Cop*. Sydney: ABC Books.
- Peachey, P. 2012. 'Thousands of Police Accused of Corruption – Just 13 Convicted.' *The Independent Online* (accessed 14 May 2013). <http://www.independent.co.uk/news/uk/crime/thousands-of-police-accused-of-corruption-just-13-convicted-7786257.html>
- Piquero, N. and M. Benson. 2004. 'White-Collar Crime and Criminal Careers: Specifying a Trajectory of Punctuated Situations.' *Journal of Contemporary Criminal Justice*, 20 (2), 148–165.
- Portes, A. 1997. 'Neoliberalism and the Society of Development: Emerging Trends and Unanticipated Facts.' *Population and Development Review*, 23 (2), 229–259.
- Porter, L. and C. Warrender. 2009. 'A Multivariate Model of Police Deviance: Examining the Nature of Corruption, Crime and Misconduct.' *Policing and Society*, 19 (1), 79–99.
- Punch, M. 2009. *Police Corruption: Deviance, Accountability and Reform in Policing*. London: Willan Publishing.
- Raab, G. and H. B. Milward. 2003. 'Dark Networks as Problems.' *Journal of Public Administration Research and Theory*, 13 (4), 413–440.
- Ratcliffe, J. H. 2002. 'Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice.' *Policing and Society*, 12 (1), 53–66.
- Ratcliffe, J. H. 2003. 'Intelligence-Led Policing.' *Trends and Issues in Crime and Criminal Justice*, 248.

- Ratcliffe, J. H. 2008a. 'Intelligence-Led Policing.' In *Environmental Criminology and Crime Analysis*, Ed. R. W. Wortley and L. Mazerolle, 263–282. Cullompton, Devon: Willan Publishing.
- Ratcliffe, J. H. 2008b. *Intelligence-Led Policing*. Cullompton, Devon: Willan Publishing.
- Ratcliffe, J. H. 2008c. 'Knowledge Management Challenges in the Development of Intelligence-led Policing.' In *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*, Ed. T. Williamson, 205–220. Chichester: John Wiley and Sons.
- Ratcliffe, J. H. and R. Guidetti. 2008. 'State Police Investigative Structure and the Adoption of Intelligence-led Policing.' *Policing: An International Journal of Police Strategies & Management*, 31 (1), 109–128.
- Ratcliffe, J. H. and J. Sheptycki. 2009. 'Setting the Strategic Agenda.' In *Strategic Thinking in Criminal Intelligence*, Ed. J. H. Ratcliffe. 2nd ed, 248–268. Sydney: The Federation Press.
- The Regulation of Investigatory Powers Act 2000 (c.23) (RIP or RIPA) Parliament of the United Kingdom, London.
- Reiner, R. 1992. *The Politics of Police*. Hemel Hempstead: Harvester.
- Reuter, P. and J. Haaga. 1989. *The Organization of High-Level Drug Markets: An Exploratory Study*. Santa Monica: RAND.
- Richelson, J. T. 1999. *The U.S. Intelligence Community*. 4th ed. Colorado: Westview Press.
- Robertson, S. 1997. 'Intelligence-Led Policing: A European Union View.' In *Intelligence-Led Policing – International Perspectives on Policing within the 21st Century*, Ed. A. Smith, 21–23. New Jersey: International Association of Law Enforcement Intelligence Analysts Inc.
- Rogers, K. 2009. 'Developments in Australian Strategic Criminal Intelligence.' In *Strategic Thinking in Criminal Intelligence*, Ed. J. H. Ratcliffe. 2nd ed, 13–27. Sydney: The Federation Press.
- Sampson, R. J., Laub, J. H. and C. Wimer. 2006. 'Does Marriage Reduce Crime? A Counterfactual Approach to Within-individual Causal Effects.' *Criminology*, 44 (3), 465–508.
- Scott, M. S. 2000. *Problem-Oriented Policing: Reflections on the First 20 Years*. Washington DC: COPS Office.
- Serious Organised Crime Agency (SOCA). 2006. *The UK Threat Assessment of Serious Organised Crime 2006/07*. London: Serious Organised Crime Agency.
- Sewell, J. 1999. *Controversial Issues in Policing*. Boston: Allyn and Bacon.

- Shelley, L. I. 1998. 'Transnational Organized Crime in the United States: Defining the Problem.' *Kobe University Law Review*, 32 (1), 77–91.
- Skaperdas, S. 2001. 'The Political Economy of Organized Crime: Providing Protection When the State Does Not.' *Economics of Governance*, 2 (3), 173–202.
- Starey, T. 2005. 'Getting the Message – A Comparative Analysis of Laws Regulating Law Enforcement Agencies' access to stored communications in Australia and the US.' *Media and Arts Law Review*, 10 (1), 23–55.
- Stelfox, P. 2008. 'Investigative Practice and Performance Management: Making the Marriage Work.' *Policing*, 2 (3), 303–310.
- Stewart, C. 2006. 'Telstra Secretly Helped Hunt Bali Bombers.' *The Australian*. October 7.
- Sutherland, E. 1949. *White Collar Crime*. New York: Holt, Rinehart & Winston.
- Sykes, G. and D. Matza. 1957. 'Techniques of Neutralization: A Theory of Delinquency.' *American Sociological Review*, 22 (6), 664–670.
- Telecommunications (Interception) Amendment Act Cwlth*. 2006. Australia.
- Transparency International. 2011a. *Corruption Risk Assessment Topic Guide*. London: Transparency International
- Transparency International. 2011b. *Global Corruption Report: Climate Change*. London: Transparency International.
- United Nations. 2000. *United Nations Covenant against Transnational Organised Crime*. Geneva: United Nations General Assembly.
- United Nations. 2002. *Results of a Pilot Survey of Forty Selected Organized Criminal Groups in Sixteen Countries*. Geneva: United Nations Office on Drugs and Crime.
- United Nations Office of Drugs and Crime. 2008. *World Drug Report*. United Nations Office of Drugs and Crime.
- Van Duyne, P. C. 2000. 'Mobsters are Human Too: Behavioural Science and Organized Crime Investigation.' *Crime, Law & Social Change*, 34, 369–390.
- von Lampe, K. 2004. 'Organized Crime and Trust: On the Conceptualization and Empirical Relevance of Trust in the Context of Criminal Networks.' *Global Crime*, 6 (2), 159–184.
- Wall, J. 2012. 'Search and Surveillance, and the Exclusion of Evidence in New Zealand: Clarity or Confusion.' *The International Journal of Evidence & Proof*, 16 (2).

- Walters, P. 2009. 'Organised Crime is AFP Focus: Tony Negus.' *The Australian*. September 8.
- Wardlaw, G. and J. Boughton. 2006. 'Intelligence-Led Policing: The AFP Approach.' In *Fighting Crime Together: The Challenges of Policing and Security Networks*, Ed. J. Fleming and J. Wood, 133–149. Sydney: University of New South Wales Press.
- Warr, M. 1996. 'Organization and Instigation in Delinquent Groups.' *Criminology*, 34 (1), 11–37.
- Waters, G., D. Ball and I. Dudgeon. 2008. *Australia and Cyber-Warfare, Canberra Papers on Strategy and Defence*, 168. Canberra: Australian National University E Press.
- Weber J, Kurke L. D. Pentico. 2003. 'Why Do Employees Steal?' *Business and Society*, 42 (3), 359–380.
- Weisburd, D. and J. E. Eck. 2004. 'What Can Police Do to Reduce Crime, Disorder, and Fear?' *The Annals of the American Academy of Political and Social Science*, 593 (1), 42–65.
- Weisburd, D., S. Mastrofski, A. M. McNally, R. Greenspan and J. Willis. 2003. 'Reforming to Preserve: COMPSTAT and Strategic Problem-solving in American Policing.' *Criminology and Public Policy*, 2 (3), 421–456.
- Willey, D. 2009. 'Italy Police Warn of Skype Threat.' *BBC News*. February 14. <http://news.bbc.co.uk/2/hi/7890443.stm>
- Williams, E. S. 1980. *Australian Royal Commission of Inquiry into Drugs*. Canberra: Royal Commission.
- Williams, P. 2001. 'Transnational Criminal Networks.' In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Ed. J. Arquilla and D. Ronfeldt, 61–97. Santa Monica, CA: Rand Corporation.
- Wood, J. R. T. 1997. *Royal Commission into the New South Wales Police Service – Final Report*, Vol. 1, 183. Sydney.

Index

- ACC, *see* Australian Crime Commission (ACC)
- accountability, 50
- adaptive capacity, of
networks, 39
- adolescence limited
offenders, 34
- adult onset offenders, 34, 35
- affidavits, 107–8
- AFP, *see* Australian Federal Police (AFP)
- AIC, *see* Australian Intelligence Community (AIC)
- anti-corruption models, 56–68
CIT and, 64–8
effective investigations, 60
nature of corrupt activity
and, 61–2
watchdog commissions,
60–4
- anti-gang legislation, 26
- anti-money laundering
measures, 19, 22–4
- Armed Officers Squad, 58
- Asia Pacific Economic
Community (APEC), 24
- Asia Pacific Group on Money
Laundering (APGML), 24
- Asia Regional Forum
(ARF), 24
- ASIO, *see* Australian Security
Intelligence Organisation
(ASIO)
- Attorney-General Quintet, 24
- Audit Commission, 52, 53
- Australia, 2
CIT legal frameworks in,
71–4, 75
Fitzgerald Inquiry, 42, 45, 61,
63–4, 83
Independent Commission
Against Corruption
(ICAC), 59, 73
independent watchdogs,
61–2
legal responses to organized
crime in, 22–3
use of CIT in, 83–4
- Australian Commission
for Law Enforcement
Integrity (ACLEI), 62,
73–4
- Australian Crime Commission
(ACC), 18, 23
- Australian Federal Police
(AFP), 22, 23, 54, 73–4,
86–7
- Australian Intelligence
Community (AIC), 79
- Australian Security Intelligence
Organisation (ASIO), 22
- Australian Security
Intelligence Organisation
Act (1979), 79
- backbenchers, 43
- Bali Bombings, 22, 86–7, 117
- Bali Process, 24

- Barrett Review, 75
- Blunn Review, 75
- Boucher Review, 75
- bribery, 24, 33, 37, 42, 58, 65
see also corruption
- brokers/brokerage, 37, 40–2, 65
- Cali Cartel, 20
- Canada, 2
 CIT legal frameworks in, 77–8
 legal responses to organized crime
 in, 26–7
- Canadian Security Intelligence Service
 (CSIS), 27
- CCC, *see* Crime and Corruption
 Commission (CCC)
- circuit-switched networks, 70
- CIT, *see* communication interception
 technology (CIT)
- closed networks, 39, 42
- clustered hierarchy, of crime groups,
 15, 16
- CMC, *see* Crime and Misconduct
 Commission (CMC)
- code of silence, 32, 35, 37, 40
- Combined Forces Special Enforcement
 Unit (CFSEU), 26
- Combined Law Enforcement Group
 (CLAG), 24–5
- Commonwealth Investigations Branch
 (CIB), 40
- communication intelligence
 (COMINT), 79
- communication interception
 technology (CIT), 1, 69–95, 97
 in Australia, 71–4, 75, 83–4
 case studies, 86–9
 definition of, 70–1
 directions for, 96–9, 118–20
 effectiveness of, 6–7, 84–9, 104–5
 in Hong Kong, 79
 integrating in investigations, 103–11,
 118–19
 integration of, 6
 issues surrounding, 89–95
 legal frameworks governing, 71–9
 legislative constraints, 89–91, 117
 in New Zealand, 77–9
 practical application of, 81–4
 privacy constraints, 89–90, 91–3, 117
 research on, 2–4
 SIGINT, 79–81
 targeting of, 64–8
 transnational organized crime and,
 81–3
 in United Kingdom, 74–6
 use of, 5, 6–7, 54–5, 57, 70, 113–18
 warrant applications, 85–6
- communication needs, of crime
 groups, 19
- Communications Security
 Establishment (CSE), 79
- community-oriented policing
 (COP), 49
- COMPSTAT, 50–1
- computer statistics, 50–1
- confirmation bias, 33
- Congress, 43
- Coordinated Law Enforcement Unit
 (CLEU), 26
- core group, of crime groups, 15–16, 17
- corruption, 1–5, 29–46
 culture and, 32, 35, 37, 45
 forms of, 31–3
 by government employees, 43–5,
 59–60
 investigation of, 56–68, 83–4, 99–100
 layers of, 41, 59
 networks, 36–41, 46, 57, 115
 noble cause, 32–3, 58
 in other fields, 42–5
 police. *see* police corruption
 by politicians, 43, 45
 public sector, 30, 31, 42–5, 59–60
 theories of, 33–5
 types of, 115
- Council of Europe Convention on
 Cybercrime, 25, 27
- Crime and Corruption Commission
 (CCC), 62, 73
- Crime and Misconduct Commission
 (CMC), 45, 73, 83

- crime intelligence, 104–10
 see also intelligence
 crime prevention, situational, 50
 criminal careers, 34
 Criminal Intelligence Service of
 Canada (CISC), 26–7
 Criminal Justice Commission
 (CJC), 45
 criminal networks, 17–18, 37–9
 capital of, 41
 structure of, 13–18
 trust in, 39–40
 criminals, types of, 34–5
 cyber crime, 21
 cybercrime, 25, 27
- dark networks, 5, 37–9, 41, 46, 57–9,
 68, 115, 116
 data collection plan (DCP), 7–9
 data mining, 100–2
 data retention, 100–2
 Defence Signals Directorate (DSD), 79,
 86–7, 117
 document analysis, 9–10
 drug trafficking, 26, 41
 DSD, *see* Defence Signals Directorate
 (DSD)
- Eastern Europe crime groups, 21–2
 ego networks, 65, 67
 elasticity, of networks, 39
 Electronic Frontier Australia, 90, 93
 electronic mail (email), 21, 70, 72
 electronics intelligence (ELINT), 80
 electronic surveillance, *see*
 communication interception
 technology (CIT)
 encryption devices, 21
 European Convention, *see* Council
 of Europe Convention on
 Cybercrime
 extortion, 31
- Financial Action Task Force (FATF), 22
 Fitzgerald Inquiry, 42, 45, 61, 63–4, 83
 Ford Review, 75
- globalization, 52, 113
 gossip, within networks, 40
 Government Communication
 Headquarters (GCHQ), 79
 Government Communications
 Security Bureau (GCSB), 79
 government employees, corruption by,
 43–5, 59–60
 grounded theory, 6, 8, 114
 grounds to obtain a warrant (GTO),
 107–8
- Hells Angels OMG, 26
 Herbert, Jack, 62, 63, 64, 67
 Hong Kong, 60, 61, 79
 human rights, 27, 91–3
 human trafficking, 24
- ICAC, *see* Independent Commission
 Against Corruption (ICAC)
 Independent Commission Against
 Corruption (ICAC), 59, 83
 HK, 60, 61
 NSW, 61–2, 73
 Independent Police Complaints
 Commission (IPCC), 60
 independent watchdogs, 60–4
 Indonesia, 23, 86–7
 informants, 54
 information and communication
 technology (ICT)
 see also communication interception
 technology (CIT)
 criminal use of, 2, 19–22
 development of, 1–10, 70
 information to obtain a warrant (ITO),
 107–8
 integrity systems, 58
 integrity testing, 5
 intelligence, 51
 collection, 54–5
 communication, 79
 crime, 104–10
 culture and, 93–5
 directions for, 96–9, 118
 doctrine, 5

- electronics, 79
- gathering, 23, 68, 82–3, 93–5, 116
- sharing, by law enforcement, 23, 55, 94–5, 117
- signals, 79–81
- intelligence-led policing (ILP), 4, 52–5, 82, 103–11, 114–16, 119
- Intelligence Probe, 105–7, 119
- Intelligence Services Act (2011), 79
- investigations
 - of corruption, 56–68, 83–4, 99–100
 - integrating CIT within, 103–11, 118–19
 - preliminary, 107, 119
- Investigative Powers for the 21st Century Act (2010), 27, 77–8
- investigative techniques, 60

- Joke network, 42, 64–5, 66, 67

- Kennedy Royal Commission, 83–4
- Knapp Commission, 31, 57, 67
- knowledge-managed policing (KMP), 103, 104, 105, 119

- latent traits, 34
- law enforcement agencies (LEAs), 1, 5, 12
 - anti-corruption models of, 56–68
 - Australia, 22–3
 - Canada, 26–7
 - cooperation among, 23, 24
 - corruption in. *see* police corruption
 - knowledge sharing by, 23, 55, 94–5, 117
 - New Zealand, 24
 - policing methodologies and, 47–55
 - as trust-based organisations, 40
 - UK, 28
- leadership, police, 32
- legal affirmation, 33
- life-course criminality model, 33–5
- life-course persistent offenders, 34
- Long, Huey, 43, 45

- Mafia, 13
- media, 45
- metadata, 100–2
- ministers, 43
- mobile phones, 20–1, 70
- money laundering, 19, 22–3, 24, 113
- moral distance, 33
- moral hazard, 32, 33

- National Cyber Security strategy, 25
- National Intelligence Model (NIM), 52–3, 76
- National Security Agency (NSA), 79
- National Threat Assessment Centre, 23
- NATO Cooperative Cyber Defence Centre of Excellence, 4
- network analysis, 46, 64
- networks
 - brokers, 37, 40–2, 65
 - circuit-switched, 70–1
 - closed, 39, 42
 - corruption, 36–42, 46, 57, 115
 - criminal, 13–18, 37–41
 - dark, 37–9, 41, 46, 57–9, 68, 115, 116
 - destabilization indicators, 39
 - ego, 65, 67
 - packet-switched, 70–1
 - redundancy in, 39, 65
 - reputation, 39–40
 - resilience of, 38–9
- neutralization, 36
- New Zealand, 2
 - CIT legal frameworks in, 78–9
 - legal responses to organized crime in, 23–5
- NIM, *see* National Intelligence Model (NIM)
- 9/11 terror attacks, 22, 81
- noble cause corruption, 32–3, 58

- occupational deviance, 31
- offenders
 - persistent, 53
 - types of, 34–5
- official corruption, 3, 4, 5

- official corruption – *continued*
see also police corruption; public sector corruption
- online communication, 20–1, 70, 72
- Operation Anchorage, 54
- Operation Tesco, 57, 58
- Organisation for Economic Cooperation and Development (OECD), 22, 24
- Organised and Financial Crime Agency of New Zealand (OFCANZ), 24
- Organised Crime Agency of British Columbia (OCABC), 26
- organized crime
see also transnational organized crime
 networks, 37–9
 social opportunity structure of, 35
- packet-switched networks, 70–1
- paggers, 20
- Papua New Guinea, 23
- party discipline, 43
- patronage, 43, 45
- phone tapping, 68, 71–2, 73
- police corruption, 30, 115
see also corruption
 brokerage and, 41
 forms of, 31–3
 hierarchy of, 31
 intelligence-led policing (ILP), 115–16
 investigation of, 57–8, 60, 62–8, 83–4
 networks, 37, 41–2, 46
 reasons for, 30, 31
 theories of, 33–5
 trust and, 40
- police crimes, 31
- police culture, 32, 35, 37, 42, 45
- policing methodologies, 4, 5, 47–55, 115
 community-oriented policing, 49
 computer statistics, 50–1
 intelligence-led policing, 52–5, 82, 103–11, 114, 119
 models of, 48–77
 proactive policing strategy, 51, 97
 problem-orientated policing, 50
 traditional model, 48–9
- Policy Integrity Commission (PIC), 62
- politicians, corruption by, 43, 45
- Post-Operational Intelligence Analysis, 109, 119
- predatory policing, 30
- preliminary investigations, 107, 119
- prisoners' dilemma, 63
- privacy rights, 89–90, 91–3, 117
- proactive policing strategy, 51, 97
- problem-orientated policing (POP), 50
- process corruption, 31
- Public Integrity Commission (PIC), 73
- public sector corruption, 30, 31, 42–5, 59–60
see also police corruption
- punishment justification, 33
- Al Qaida, 38
- qualitative research, 6
- Racketeer Influenced and Corrupt Organizations (RICO), 38
- redundancy, 39, 65
- regional hierarchy, of crime groups, 14–15
- Regulation of Investigatory Powers Act (RIPA), 28, 74–6
- reputation, 39–40
- resilience, 38–9
- Royal Canadian Mounted Police (RCMP), 26, 27
- Search and Surveillance Act (2012), 25, 78–9
- Serious and Organised Crime Agency (SOCA), 28, 53, 87–9, 117
- Sherman Review, 75
- Sicilian Mafia, 13
- signals intelligence (SIGINT), 79–81
- SIM (Subscriber Identity Module) cards, 21
- situational crime prevention, 50
- Skype, 21, 70

- smuggling, 24
- social identity theory, 33
- social network analysis, 46, 64
- social networks, 21, 36–41
see also networks
- social norms, 36
- social opportunity structure, 35
- standard hierarchy, of crime groups, 14
- Strategic Alliance Group, 24
- surveillance, 5, 64, 65, 67, 68, 81–2, 116
see also communication interception technology (CIT)
- Surveillance Devices Act (2007), 73
- Tallinn Manual on the International Law Applicable to Cyber Warfare*, 4
- telecommunications, 70
- Telecommunications (Interception) Amendment Act (2006), 71–2
- Telecommunications (Interception and Access) Act (1979), 71–2, 83–4, 91
- Telecommunications (Interception and Access) Western Australia Act (1996), 73
- Telecommunications Interception Act (2009), 73
- telephone intercepts, 68, 71–2, 73
see also communication interception technology (CIT)
- terrorist attacks, 22, 81
- terrorist funding, 19, 24
- terrorist networks, 37, 113
- text messages, 20–1, 70, 72
- traditional policing model, 48–9
- Transnational Crime Coordination Centre, 23
- transnational organized crime (TOC), 1, 5, 11–28
 activities of, 12
 in Australia, 22–3
 business operations of, 19–20
 CIT use against, 81–3, 97, 104, 113, 115
 communication needs of, 19, 114–15
 definition of, 12–13
 growth of, 113
 ICT use by, 2, 19–22
 intelligence-led policing and, 53–5
 legal responses to, 22–8
 in New Zealand, 23–5
 policing methodology for, 51
 research on, 2–4
 structure of, 13–18, 114
 suppliers for, 19–20
 understanding, 12–13
 vulnerabilities of, 18–22
- trust, 39–40
- UN Convention Against Transnational Organised Crime (UNTOC), 22, 23, 24, 27, 28
- United Kingdom, 2
 Audit Commission, 53
 CIT legal frameworks in, 74–6
 legal responses to organized crime in, 27–8
 National Intelligence Model (NIM), 52–3, 76
 Serious and Organised Crime Agency (SOCA), 28, 53
 Warrant Authorization Process, 76
- United States, 79, 118
- UN Transnational Organised Threat Assessment for East Asia and the Pacific, 24
- US Drug Enforcement Agency, 20
- visibility, of crime networks, 38
- Voice over Internet Protocol (VoIP), 21, 72–3
- vulnerability, of networks, 39
- warranted inquiries, 108–9, 119
- warrantless inquiries, 107–8, 119
- watchdog commissions, 60–4, 68
- Westminster system, 43
- white-collar crime, 34, 35, 36, 42
- Wood Inquiry, 63
- Wood Royal Commission, 62, 83