Australian Government
Australian Institute of Criminology

AIC reports
Research Report 10

Organised crime research in Australia 2018

Russell G Smith (editor)

© Australian Institute of Criminology 2018

ISSN (Online) 2206-7280

Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the *Copyright Act 1968* (Cth), no part of this publication may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Inquiries should be addressed to the publisher.

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release.
The online versions available on the AIC website will always include any revisions.

All publications in the Research Report series are subject to peer review–either through a double-blind peer review process, or through stakeholder peer review. This report was subject to double-blind peer review.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

PART I: UNDERTAKING ORGANISED CRIME RESEARCH.....VI

Chapter 1: The state of organised crime research in Australia 1

- Professor Roderic Broadhurst, Professor of Criminology, School of Regulation and Global Governance, Australian National University
- Dr Adam Masters, College of Arts and Social Sciences, Australian National University
- Dr Russell G Smith, Principal Criminologist, Australian Institute of Criminology
- Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Chapter 2: A network perspective on fusion 9

- Associate Professor Chad Whelan, School of Humanities and Social Sciences, Deakin University
- Associate Professor David Bright, Associate Professor of Criminology, College of Business, Government and Law, Flinders University

Chapter 3: Can we forestall terrorism and frustrate organised crime by means of metadata retention?..... 18

- Professor Rick Sarre, Adjunct Professor of Law and Criminal Justice, School of Law, University of South Australia

Chapter 4: The who, not the what—analysing public knowledge on organised criminals 25

- Dr Adam Masters, College of Arts and Social Sciences, Australian National University

PART II: UNDERSTANDING HOW ORGANISED CRIME GROUPS OPERATE.....34

Chapter 5: Insiders versus outsiders—alternative paths to criminogenic knowledge 35

- Douglas MC Allan, Director of Financial Crime and Anti-Money Laundering and Counter Terrorism Studies, Australian Graduate School of Policing and Security, Charles Sturt University

Chapter 6: Responding to organised crime through intervention in recruitment pathways 50

- Dr Russell G Smith, Principal Criminologist, Australian Institute of Criminology

Chapter 7: Disengagement from involvement in organised crime—processes and risks..... 61

- Dr Kaylene Douglas, Governance and Executive Services, South Australian Department for Correctional Services
- Dr Russell G Smith, Principal Criminologist, Australian Institute of Criminology

PART III: EXPLORING RELATIONSHIPS BETWEEN ORGANISED CRIME AND OTHER CRIMINALACTIVITIES.....70

Chapter 8: Organised crime and terrorism nexus—implications for Australia: a research note..... 71

- Dr Rolando Ochoa, Department of Security Studies and Criminology, Macquarie University

Chapter 9: Nexus between unreported and unregulated fishing and other organised maritime crimes 78

- Dr Jade Lindley, Law School, University of Western Australia

Chapter 10: Criminal innovation and illicit global markets—transnational crime in Asia..... 87

- Professor Roderic Broadhurst, Professor of Criminology, School of Regulation and Global Governance, Australian National University

Chapter 11: The international darknet drugs trade—a regional analysis of cryptomarkets 95

- Associate Professor James Martin, Criminology Discipline Convener, Department of Social Sciences, Swinburne University of Technology
- Dr Jack Cunliffe, School of Social Policy, Sociology and Social Research, University of Kent
- Dr David Décary-Hétu, Assistant Professor, School of Criminology, University of Montreal
- Professor Judith Aldridge, Professor of Criminology, School of Law, University of Manchester

PART IV: POLICING AND RESPONDING TO ORGANISED CRIME.....104

Chapter 12: Developing and applying a Queensland Crime Harm Index—implications for policing serious and organised crime 105

- Professor Janet Ransley, School of Criminology and Criminal Justice, Griffith University
- Professor Kristina Murphy, School of Criminology and Criminal Justice, Griffith University
- Professor Susanne Karstedt, School of Criminology and Criminal Justice, Griffith University
- David Bartlett, Research Fellow and Sessional Lecturer, School of Criminology and Criminal Justice, Griffith University
- Lucy Forrester, School of Criminology and Criminal Justice, Griffith University
- Maurice Carless APM, Assistant Commissioner, Intelligence and Covert Services Command, Queensland Police Service

Chapter 13: Impact of ballistic evidence on police investigations into organised crime..... 115

- Anthony Morgan, Research Manager, Australian Institute of Criminology
- Penny Jorna, Research Analyst, Australian Institute of Criminology

Chapter 14: Effectiveness of anti-money laundering obligations in combating organised crime with particular reference to the professions 124

- Associate Professor David A Chaikin, Business Law, University of Sydney

Chapter 15: Third party co-production of cybersecurity 131

- Dr Lennon YC Chang, School of Social Sciences, Monash University
- Dr Lena Y Zhong, Department of Applied Social Sciences, City University of Hong Kong
- Professor Emeritus Peter Grabosky, ANU College of Asia and the Pacific, Australian National University

Part I: Undertaking organised crime research

Chapter 1: The state of organised crime research in Australia

Roderic Broadhurst, Adam Masters, Russell G Smith and Rick Brown

This collection of papers presented at the second national Organised Crime Research Forum is a measure of the state of organised crime research in Australia. In 2016, the Australian Institute of Criminology and the Australian National University established the first Organised Crime Research Forum to bring together researchers and practitioners from around the country to present and discuss their work. The main purpose was to raise the profile of a pressing global and domestic crime problem and to forge research partnerships between law enforcement agencies and the university sector: research partnerships that could help improve the evidence base needed to adapt and develop ever more effective responses to the threat of organised crime. While many forms of criminality rightly occupy our attention and resources, organised crime and its transnational dimension is a persistent threat with the very real potential to undermine the rule of law and the security of Australia. The public discussion about what to do about organised crime draws mostly on media reports of arrests and drug seizures and cycles between alarm and apathy. The Forum, however, curates discussions about the diverse forms of organised crime, drawing on the insights, experiences and concerns of the participants, and provides a bridge between experts and the broader public.

In 2017, the second Forum was again conducted, with many more participants, including representatives from nearly every state and territory police service and a range of federal law enforcement agencies and government departments, along with academic researchers from across the country. This publication includes 15 of the papers that were presented in June 2017 and represents a significant slice of current research on organised crime in Australia. The feedback from the first Forum highlighted the need to engage police and policy practitioners as more active participants in the Forum and to encourage grounded research focused on the concerns and needs of those involved in investigating and suppressing organised crime.

Organised crime research in Australia, as elsewhere, faces numerous challenges. Apart from the elusiveness of organised criminal activity, definitional differences across jurisdictions and discipline experts can limit a broader research perspective, often needed to situate local and global manifestations of organised crime. Common challenges also include the currency,

reliability and validity of the available data and, when combined with data access restrictions, serve to separate the academic research 'outsider' from the practitioners' experiential knowledge and intelligence databases. Finally, ensuring the relevance of research, whether by academics, practitioners or policy makers, is best shaped by the open dialogue and discussion fostered by the Forum.

Definitions

One of the challenges in conducting research into organised crime is to adopt an operational definition that is both workable and useful. As Smith observes in Chapter 6, a widely adopted definition of an organised criminal group is provided in Article 2 of the United Nations Convention Against Transnational Organized Crime (UNTOC):

> a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit (United Nations 2004: 5).

There are, however, many other ways of defining organised crime. Klaus von Lampe (2017), for example, gathered together over 150 different definitions of organised crime, including seven from Australia. The definition employed by the Australian Criminal Intelligence Commission, for example, is broader and includes 'all crime of an entrepreneurial nature and/or that committed to support a criminal enterprise, whether by a group or an individual' (ACIC 2015: 10). Maltz (1976) offered a general definition by distinguishing between the functions and activities of organised crime groups. Many jurisdictions pragmatically combine notions of serious and organised crime, in recognition that the distinction between crimes which require a high degree of organisation and crimes by criminal organisations (groups or networks of criminal actors) may not be operationally discerned. Fijnaut et al. (1998) also note that organised crime groups are:

> groups focused on obtaining illegal profits, [who] systematically commit crimes that seriously damage society and are reasonably capable of shielding their criminal activities from the authorities (Fijnaut et al. 1998: 26).

Fijnaut et al. follow the well-established perspective that organised crime is principally motivated by profit and power. Others who apply the profit–power functions of organised crime include Gambetta (1993: 2; emphasis in original), who argued that the use of violence by organised crime 'is a means, not an end; a resource, not the final product. The commodity that is really at stake is protection'. In short, Gambetta argued that protection for illicit markets is the

central feature—or business—of mafia-like organised crime groups. Taking protection as the key element of a more generalised approach to organised crime, analysis of the dark markets by Martin et al. in Chapter 11 would require a refocusing on the providers of such markets and their capacity to provide protection. The operators of cryptomarkets offer the nominal protection of anonymised exchanges that enable vendors of illicit goods to trade. They also offer escrow services and other means of ensuring a trusted market, such as vendor and product ratings—achieving, it might seem, the perfect blend of secrecy and efficiency so essential to the success of organised crime groups. Nevertheless, vendors and consumers operating in illicit cryptomarkets face constant disruption from competitors (for example, via distributed denial of service attacks), exit scams by vendors or market operators and law enforcement activities. Organised crime involvement in these profitable, novel cryptomarkets and other forms of cybercrime is growing rapidly and also requires unconventional methods for providing protection, but they remain vital if contracts are to be honoured in illicit markets, virtual or real.

Varese (2011) traced a series of attempted transplantations of mafias outside their region of origin. Success or failure depended on the incorporation or replacement of existing providers of protection. Such work is critical to Australian reflections on organised crime, particularly because some of the work in this report demonstrates the presence of such mobile and ethnically diverse groups. Masters' Chapter 4 touches on the 'ndrangheta, whose Calabrian roots saw offshoots emerge in Australia nearly a century ago. In Chapter 10, Broadhurst illustrates the diversity and mobility of organised crime groups throughout Asia, forming part of the drug supply chain affecting Australia. As Australia is a nation predominantly composed of migrant groups, the elements required for successful transnational criminal activity with established or newly formed overseas organised criminal groups are always present.

Tying the work of Gambetta, Varese and others such as Paoli (2003) and Tilly (1985) together is that of Cockayne (2016), who uses a strategic perspective to analyse among organised crime groups the imperative for political power and influence. Australia has not been immune to organised criminal groups attempting to infiltrate labour organisations and the institutions of the state. In recent years, investigative reporting has revealed such approaches (eg McKenzie, Hichens & Toft 2015). Cockayne's work demonstrates that hidden political influence and power underpin the perceived status and social capital of criminals—beyond that of economic success or the ability to deploy violence as a commodity. Political influence also has a symbiotic effect and can entail the capture of state agencies or agents, smoothing state intrusion into illicit markets and, at times, also reducing the need to deploy violence. While Cockayne's thesis applies more directly to less developed nations, Broadhurst in Chapter 10 reminds us that we exist in a region with a diverse range of political systems, many of which are far more vulnerable to organised criminal infiltration than Australia.

The UNTOC definition itself is often contested because it focuses on organised crime 'groups', rather than organised 'crime' itself (Paoli & Vander Beken 2014) and may sometimes be ineffective—for example, in jurisdictions that eschew laws against criminal conspiracy or those that lightly sanction some offences associated with organised criminal activity. The UNTOC approach has the virtue of universality but may limit the scope of criminality deemed organised

and subject to mutual legal assistance. Lindley in Chapter 9 also draws from the United Nations (UN) to provide a firm definition of an organised crime type—defining illegal, unreported and unregulated fishing per the UN Food and Agricultural Organisation's standard. Smith, in Chapter 6, explores a definition of organised crime in order to determine the characteristics of those who choose to join such groups. This diversity of definitions reflects a drive by academic scholars to publish internationally relevant work and also reflects the diversity of criminal entrepreneurs/enterprises. Although important for constraining the legislative powers of agencies, such definitions can act as a constraint on academic research, particularly among criminologists, who often argue that legal definitions are too narrow to capture deviant behaviour.

Australian legislative definitions

The principal federal legislative definition of Australian organised crime is found in section 4 of the *Australian Crime Commission Act 2002* (Cth). This is repeated in the enabling legislation passed by state and territory parliaments. The Act defines organised crime by focusing on the offences which constitute a 'serious or organised crime'. It should be noted that this definition extends the limited but universal UNTOC meaning of organised crime to include 'serious or' as well as 'organised crimes'. Section 4 lists 18 offences—theft; fraud; money laundering; currency violations; illegal drug dealings; illegal gambling; obtaining financial benefit by vice engaged in by others (pimping); extortion; violence; bribery/corruption of or by public officials; perverting the course of justice; bankruptcy and company violations; harbouring criminals; forging passports; firearms; armaments dealings; illegal importation or exportation of fauna into or out of Australia; and cybercrime—plus a catch-all for offences of the same general nature as those enumerated.

This list is considerably shorter than the offences identified under the United States (US) *Racketeer Influenced and Corrupt Organizations Act* (RICO). It does, however, cover some uniquely Australian features, such as the export/import of fauna, and the trade in firearms—a constitutionally limiting aspect of United States efforts to control organised crime. The infiltration of labour unions by the mafia was a specific driver for the US Congress to pass the RICO Act (Jacobs & Cooperman 2011; Jacobs & Peters 2003; Witwer 2005, 2008).

More recently, state and territory parliaments have passed laws focused on who is an organised criminal, rather than what is organised criminal conduct (see RoLIA 2013). The focus of these laws was on criminal association and sought to disrupt criminal groups' capacity to organise. So-called anti-bikie laws, developed over the last decade, allow police to declare groups to be criminal organisations, with their members subject to restrictions of movement or associations or arrest in defined circumstances. Earlier versions of these laws in South Australia and New South Wales were struck down by the High Court of Australia; however, some state legislatures have amended the laws to provide a legal tool for law enforcement to use to limit the illegal activities of proscribed groups (RoLIA 2013; Ayling & Broadhurst 2014).

Data

Data validity, currency and access issues are discussed in a number of the chapters, with some valuable reflections on how to overcome these challenges. Apart from ethical clearance, bureaucratic barriers provide further challenges to conducting research, because permission is invariably required to obtain access to documents, case files and personnel to interview. Prosecutorial and investigative records provided robust data for Whelan and Bright in Chapter 2 and Morgan and Jorna in Chapter 13, who assessed the utility of police ballistic data to identify organised crime links to firearms crimes.

Court, prosecutions and investigative material provide the foundation for other state-sanctioned data sources. Chaikin in Chapter 14 considered the role of private sector actors—financial managers, lawyers, accountants, board members and others—as gatekeepers to prevent money laundering by organised crime. He used data from financial intelligence units to demonstrate the vulnerabilities inherent in Australia's regulatory model, which as yet does not require lawyers and accountants to report suspicious transactions.

Not all organised crime data presented in this volume originated from official or state-sanctioned sources. Allan, in Chapter 5, reviewed in detail complex fraud cases in order to ascertain the planning and organisation required to undertake large-scale deception offences. Data-scraping, or capture of the internet, has emerged in recent years as a new source of material on internet illicit markets, as Martin et al. show in Chapter 11. In many cases, data validity rests on the confidence criminal actors and their clients have in discussing offending, post-facto in the case of interviews, or the anonymity of the internet.

Case studies also provided data for contemporary research into Australian organised crime. Whelan and Bright, in Chapter 2, reviewed the purpose, structural design and challenges behind the creation and operation of criminal intelligence fusion centres, whose purpose is to better combine limited law enforcement resource and expertise. Sarre, in Chapter 3, used the ongoing debate regarding the retention of email, mobile phone and other metadata as a tool for combating extremism and organised crime to stimulate some lively discussion about the potential over-reach of new surveillance technology and our reliance on metadata to conduct complex investigations.

Engagement

The Forum itself provided an opportunity to assess both the levels of researcher–practitioner engagement and the relevance of the research. The aforementioned discussion of Sarre's chapter, while illustrative of some disconnect, also highlighted the value of the Forum and the importance of dialogue. Already, there is more engagement than in the past and a greater willingness among agencies to share data and intelligence, and access to data for many of the presentations rested on established researcher–practitioner engagement (eg Whelan & Bright). Morgan and Jorna in Chapter 13 demonstrate how a new national ballistics data system was used to link cases, including cold cases and those involving organised crime. However, such cooperation is not all data access driven. The State Crime Command of the Queensland Police

required data creation in the form of a crime harm index suitable for their jurisdictional context (Ransley et al. in Chapter 12). Such indices have growing value for practitioners in an evidence-based policy environment and one where law enforcement resources may be rationed. Similarly, a harm scale will provide a foundation for a better understanding and response to the harm caused by organised crime.

Current trends in research

There were three overarching research trends emanating from the presentations given at the Forum: understanding the harm caused by organised crime and what capacities are needed for an effective response; the potential of social network analysis to map the morphology of crime groups; and the emergent trends in organised crime, including changes in illicit products and criminal methodology.

Understanding the harm caused by organised crime was directly addressed by the Queensland Police project being conducted by Ransley et al. (Chapter 12). However, harm underpinned the concerns of Broadhurst in his analysis in Chapter 10 of '…how the recreational use of "ice" or amphetamine type stimulants (ATS, e.g. methamphetamines, ecstasy), and new psychoactive substances (NPS, e.g. synthetic opiates like fetanyl) as well as cocaine, have revitalised traditional crime groups'. Not only have traditional crime groups received a boost from the growing illicit markets; new entrepreneurial groups are taking advantage of the profitability of narcotics in Asia as a source of both supply and demand. The resurgent Asian trade in illicit drugs is typically enmeshed with other criminal activities. In Southeast Asia, other criminal activities most likely to impact on economic growth, resource sustainability and governance include: counterfeiting of high street goods; wood and wildlife products trafficking—illegal logging, exotic and protected trade, wild meat trade; illegal disposal of e-waste and prohibited chemicals; and human trafficking and smuggling, including sex and labour trafficking (see Chapter 10). Thus, the harm of organised crime is diversified across economic, environmental and social spheres.

The structure of this publication

The 14 substantive chapters have been arranged in four sections. After this introductory chapter, the first section examines how organised crime research is undertaken, where data come from, how information and intelligence can be used to greatest effect, what members of the public know about organised crime, and the sources from which they obtain their knowledge.

This is followed by three chapters that examine how organised crime groups operate, particularly how one learns to become a criminal, what recruitment practices are used to seek out and enrol new members of organisations, and how individuals who no longer wish to be involved with organised crime seek to disassociate themselves from the groups. These chapters all provide important insights into how membership can be limited by intervening at appropriate decision points.

Section 3 explores the relationships between conventional organised criminality and other types of crime. This includes the differences that exist between organised crime and so-called volume crimes that occur on a widespread scale, and the relationship between organised criminality and acts of terrorism. A specific case study is then described of the relationship between unregulated fishing and organised maritime crime. The section finishes with an analysis of innovative practices in Asian illicit global markets, followed by a regional analysis of illicit drug cryptomarkets.

The final section looks at law enforcement and other responses to the problem of organised crime. The use of an organised crime harm index is examined in terms of its implications for law enforcement, while the impact of a national database for ballistic evidence is considered for police investigations. Two final chapters look at the effectiveness of anti-money laundering regulations as a means of combating organised crime, and how third party partnerships (co-production of regulation) can be used to enhance responses to organised cybercrimes. Widening the administrative and civil law response has also been important in broadening the means to disrupt organised crime groups. The enforcement of health and safety and fire regulations have proven helpful in disrupting the activities of organised crime groups (Ayling & Broadhurst 2014).

This work presents the research of over 20 scholars, from a variety of disciplines, working on organised crime problems in, or affecting, Australia. A question for future consideration is how the current body of research differs from that conducted outside Australia and what reasons could be advanced to explain any differences that exist. It is unlikely that the nature of Australian organised crime is in itself unique, although Australia's diverse responses may uniquely shape its form, reach and influence. Equally important will be attention to the transnational activities of crime groups in our region and what may be done at the regional and international level to suppress them. The research presented here makes use of criminological theory and social scientific methods and would benefit from better understanding of the regulatory and policy environment in which organised crime is being addressed in Australia. The purpose of the Organised Crime Research Forum is to help to create the dialogue needed to bridge the gap between evidence, policy and practice. It also should stimulate the uptake of new methods and encourage the exploration of new and emerging issues that can help develop our understanding and response to organised crime.

Conclusion

Organised crime research strives to add to the often elusive evidence about how organised crime operates and who is involved. Different approaches to defining organised crime, ethical data collection and access, as well as meaningful academic–practitioner engagements, are continuing challenges. This collection shows that many of these challenges are potentially surmountable, although a systematic research agenda is yet to emerge. The current piecemeal approach to researching organised crime across various academic, private sector and government agencies' interests can lead to duplication and uncoordinated efforts. However, this disconnect also allows room for innovation and experimentation essential to better understanding of organised crime and, if channelled to greater investment in systematic data collection and linking, could serve to develop methods to counter its influence on Australia and its neighbours.

References

URLs correct as at March 2018

Ayling J & Broadhurst R 2014. Organized crime control in Australia and New Zealand, in Paoli L (ed), *The Oxford handbook of organized crime.* Oxford: Oxford University Press

Australian Criminal Intelligence Commission (ACIC) 2016. *Illicit drug data report 2014–15*. Canberra: Australian Criminal Intelligence Commission. https://www.acic.gov.au/publications/intelligence-products/illicit-drug-data-report

Australian Criminal Intelligence Commission 2015. *The costs of serious and organised crime in Australia 2013–14: Methodological approach*. Canberra: Australian Criminal Intelligence Commission

Cockayne J 2016. *Hidden power: The strategic logic of organized crime.* New York, NY: Oxford University Press

Fijnaut C, Bovenkerk F, Bruinsma G & Van de Bunt H 1998. *Organized crime in the Netherlands*. The Hague: Kluwer International

Gambetta D 1993. *The Sicilian Mafia: The business of private protection.* Cambridge, MA: Harvard University Press

Jacobs JB & Cooperman KT 2011. *Breaking the devil's pact: The battle to free the teamsters from the mob.* New York: New York University Press

Jacobs JB & Peters E 2003. Labor racketeering: The Mafia and the unions. *Crime and Justice: A Review of Research* 30: 229–82

McKenzie N, Hichens, C & Toft, K 2015. *The Mafia in Australia: Drugs, murder and politics.* Television. Directed by McKenzie, N, Hichens, C & Toft, K. Melbourne: Australian Broadcasting Corporation

Maltz MD 1976. On defining 'Organized crime': The development of a definition and a typology. *Crime & Delinquency* 22(3): 338–46

Paoli L 2003. *Mafia brotherhoods: Organized crime, Italian style*. New York: Oxford University Press

Paoli L & Vander Beken T 2014. Organized crime: A contested concept, in Paoli L (ed), *The Oxford handbook of organized crime*. Oxford: Oxford University Press

Rule of Law Institute of Australia 2013. *Criminal organisation control legislation and cases 2008–2013* [Online]. Sydney: Rule of Law Institute of Australia. http://www.ruleoflaw.org.au/education/case-studies/organised-crime-australia/

Tilly C 1985. War making and state making as organized crime, in Evans PB, Rueschemeyer D & Skocpol T (eds), *Bringing the State back in*. Cambridge, UK: Cambridge University Press

United Nations 2004. *United Nations Convention Against Transitional Organized Crime and the protocols thereto*. New York: United Nations. http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

Varese F 2011. *Mafias on the move: How organized crime conquers new territories*. Princeton, NJ: Princeton University Press

Von Lampe K 2017. *Definitions of organized crime*. http://www.organized-crime.de/organizedcrimedefinitions.htm

Witwer D 2005. *Corruption and reform in the Teamsters Union.* Champaign: University of Illinois Press

Witwer D 2008. The racketeer menace and antiunionism in the mid-twentieth century US. *International Labor and Working-Class History* 74: 124–47

Chapter 2: A network perspective on fusion

Chad Whelan and David Bright

Fusion centres have proliferated in recent years as 'coordinating hubs' for the collection, analysis and dissemination of national security intelligence across federal, state and local law enforcement agencies and related stakeholders (eg Chermak et al. 2013). A fusion centre has been defined as an 'entity where different units within the intelligence and security community and other agencies work together on one or more threats' (Persson 2013: 9) and which 'analyse and disseminate data on suspicious individuals or activities, assist with investigations, [and] identify potential threats' (Monahan & Regan 2012: 301). The 'fusion' concept refers to both a process of intelligence collection and sharing and the facility at which intelligence is collected and shared (Carter & Carter 2009). As a process, fusion refers to the analysis of information collected from multiple sources with the overarching aim of improving the sharing of information and knowledge among member agencies (Rojek & Kaminski 2011). As a facility, a 'fusion centre' usually refers to the physical co-location of several agencies or representatives of agencies within a single facility.

Fusion centres can be understood as examples of security networks (Whelan 2012; Whelan & Dupont 2017). Following the public administration literature, security networks are defined as 'groups of three or more legally autonomous organisations that work together to achieve not only their own goals but also a collective goal' (Provan & Kenis 2008: 232). When viewed as organisational forms, security networks have two basic sets of properties: structural and relational. Structural properties relate to such attributes as the composition or membership of networks and the specific design that the network employs. Relational properties concern the factors shaping the relationships between actors at both the inter-organisational level (ie agencies) and interpersonal level (ie employees of agencies).

Whelan and Dupont (2017) recently distinguished between four ideal types of networks: information exchange networks, knowledge-generating networks, problem-solving networks and coordination networks. As with most typologies, these are ideal types, and most security networks will demonstrate features of more than one. However, most networks will tend to favour one of these four functions over and above the others. The focus here is principally on those fusion environments that would be considered 'knowledge-generating networks'—that is, initiatives that exist for purposes beyond simply information sharing but that are not intended to coordinate roles and responsibilities ('coordination networks') or necessarily develop solutions to defined, shared problems ('problem-solving networks').

The focus here is on the internal workings of fusion centres as they attempt to share information and/or collaborate on common goals. More specifically, this research highlights the application of network concepts to the dynamics of fusion centres and related environments and then calls attention to the underlying structural and relational properties of such environments. This research draws on a larger ongoing project in which the principal objective is to look inside the operations of fusion centres and related environments in Australia. In-depth interviews and focus groups were conducted with members of Australian criminal intelligence and law enforcement agencies involved in formal fusion-related environments comprising three or more organisations. This chapter focuses on the National Criminal Intelligence Fusion Capability of the Australian Criminal Intelligence Commission (ACIC), formerly the Australian Crime Commission (prior to 1 July 2016), which 'brings together more than 20 partner agencies to build the intelligence picture to respond to serious and organised criminal threat' (ACIC 2016). The Fusion Capability is comprised of a national fusion centre, physically located in Canberra, and Joint Analyst Groups (JAGs), which are multi-agency groups located in major state jurisdictions.

A focus group was facilitated with managers and team leaders of the ACIC Fusion Capability (10 participants; October 2015), and interviews were conducted with four intelligence analysts from the ACIC Capability and with each of the managers of the JAGs located in Melbourne and Sydney (late-2015 and early-2016). The researchers employed a semi-structured interview schedule but encouraged participants to discuss other related issues and used follow-up questions to explore participant responses in further detail. Focus group and interview data were coded using NVivo 11. Coding concentrated on classifying emerging themes from the interviews. It should be noted that it is the personal views of interviewees that are quoted, and these views are not necessarily representative of any of the organisations referred to in the chapter.

Networks and fusion

A network perspective can significantly enhance our understanding of how fusion centres and related entities form and function. Fusion centres can typically be viewed as either 'information sharing' or 'knowledge-generating' security networks (Whelan and Dupont 2017). For example, some fusion centres are established almost exclusively for the purposes of sharing data or information and so fall into the first category of the ideal-types. Other fusion centres share information and then attempt to collectively analyse that information to produce their own collective intelligence assessments, which fall into the knowledge-generating category.

The properties of networks include 'the nodes (agencies) that comprise the network, the ties that connect the nodes and the patterns or structures that result from those connections' (Ahuja, Soda & Zaheer 2012: 435). Network structure can be described using a range of measures, including the number, identity and characteristics of agencies, the nature and strength of ties and the overall pattern of connections. The 'organisational network' literature identifies two ideal types of processes underpinning network formation: goal-directedness and serendipity (Kilduff & Tsai 2003). Goal-directed networks are formed when actors (eg agencies) share a goal and the network is constructed in a deliberate effort to achieve this goal.

Serendipitous networks are not formed to achieve a pre-existing goal and may be established and evolve through random, haphazard processes.

Fusion centres can be viewed as 'goal-directed' organisational networks. Goal-directed networks are formed to achieve an explicit shared goal or purpose among those agencies who join the network, usually via mandate or through purposeful efforts to facilitate coordination. The challenge is to agree on shared goals while facilitating achievement of agency-specific goals. Conflicts arising over goal specification and achievement can lead to the failure of goal-directed networks. Not all actors in goal-directed networks are structurally homogenous or necessarily equal (Whelan 2017), and their effectiveness is likely to be dependent on navigating differing organisational cultures and competing priorities and promoting network-wide trust (Whelan 2016a, 2016b).

Structural properties

Membership

The formation of network ties is usually considered to be a two-way process. For example, for a new agency to enter into an existing network, that agency must be 'motivated' to join the network, and agencies—or at least the lead agency—within the network must recognise the value of including the new agency (note that this process is unlikely when agencies are legally mandated or co-opted to join a particular network). When the goals of any specific agency align with the goals of a network, that agency is more likely to be motivated to join, and the network similarly motivated to include, the goal-aligned agency.

In theory, advantages accrue to fusion centres when a diverse range of agencies is included. When the number of agencies is increased, the 'bandwidth' of the network is also increased (Carter & Carter 2009) and a larger quantum of data and information is collected and disseminated. In practice, however, while limited membership can constrict the amount and quality of data accessed and exchanged, the more diverse a network is, the more difficult it is to internally manage and coordinate (Whelan 2017).

Interviewees reflected on these observations from the network literature. For example, a participant of the ACIC focus group highlights the challenge of getting 'buy-in' from partner agencies:

> It has been a considerable task seeking the buy-in, getting the buy-in from partners, to make fusion a success, because it wouldn't have been a success had we not had that buy-in. And that's an ongoing journey. And for us it's been about demonstrating value for money, the value proposition for our partners.

Interviewees suggested that a key factor shaping agencies' decisions on whether or not to join fusion-type environments is resource constraints. The closer the alignment between the goals of a fusion centre and the goals of a (potential) member organisation, the more likely agencies are to find the resources required to invest. However, some agencies that are more pressed for resources will not invest unless goal alignment is particularly strong. As one interviewee from a JAG suggests:

> It all comes down to resource availability and putting that into the context of a returnable investment. So some agencies are better off than others with resources that can afford to put somebody in all day, every day, in an ongoing capacity. Others who aren't so flush with bodies and analytical resource will come in if the return on investment is proposed. So agencies will say I'll put a body in if what you are doing is directly relevant to my mission and my mandate and you're clear in what you seek to deliver and how it will benefit my agency.

Design

Network structure and the relative positioning of agencies is crucial to information exchange across the network. Poor integration and coordination can lead to deficits in information sharing. Integration challenges are even more acute when network member agencies are geographically dispersed. Security networks must balance the density of ties with network centralisation—the extent to which one, or a few, actors have a proportionally large number of connections to other actors—because of a trade-off between efficiency (dense ties) and greater coordination (via centralisation). Calibrating density and centralisation is, therefore, a careful balancing act.

Common network designs, also applicable to fusion, include all-channel and hub networks. In the former, all actors are connected to each other. In the latter, actors are brokered through a central or 'lead' organisation. Activities such as information sharing and decision making are coordinated by this hub, and network members may not interact directly.

In terms of design, interviewees and focus group participants made several observations pertaining to networked structures of fusion centres and related entities. In particular, interviewees commented on the traditional model, whereby agencies are co-located. As a member of the ACIC suggested, this traditional model has evolved to the extent that the fusion centre is no longer the only element of fusion:

> At the start, it was partners into the centre, physically located within the centre. Today, we have that. But we've also got our own staff; not necessarily from fusion but from other agencies, from elsewhere in our regional office, sitting out with our partner agencies, particularly in the mini-fusion cells.

The interviewee refers to the ACIC's 'mini-fusion cells', which denote the state JAGs, as well as other ties to fusion centres hosted by other agencies. In the words of one interviewee, JAGs constitute the 'arms and legs' of fusion, in that they provide reach from Canberra to the geographically dispersed regions in different Australian states.

Many interviewees from the ACIC referred to this as a 'hub-and-spoke' model, a centralised network in which the ACIC fusion centre is the hub and the JAGs represent the spokes. Hub-and-spoke models can facilitate efficient cooperation but may work best when one organisation has sufficient recourses and legitimacy to play the role of the 'hub' (Provan, Fish & Sydow 2007).

While the co-location model was often identified as an ideal outcome, the fact that agencies are geographically dispersed and have various resource constraints means that more dynamic models—what we might call 'core-periphery' models—are necessary. The previously quoted JAG interviewee also notes:

> What we've come to appreciate is that in an environment where budgets are shrinking, resources are tight, but priorities are changing and our demands are increasing, we have to take a flexible resourcing approach. So we can't ask for a full-time investment all the time in an ongoing capacity. We have to be flexible enough to say come in for the duration of a project, we'll work together on it, and then you can go back to your respective agencies.

This comment underscores the dynamic nature of fusion environments and the need for all network members to continually adjust and realign goals and to monitor and reshape network design.

Relational properties

Organisational culture

Organisational culture is widely regarded as being a difficult concept to define, with various versions and competing conceptions existing in the literature. In a leading approach, Schein (2010: 17) uses the term 'group', defined as any 'social unit that has some kind of shared history', as the basis from which to approach organisational culture. The strength of any particular group's culture will depend on many factors, including the length of its history, the stability of its membership and the types of experiences its members have shared. Culture refers to the shared beliefs, values and attitudes that form over the course of a group's history and which influence how it thinks and acts in relation to all aspects of its functioning.

The focus groups and interviewees repeatedly discussed their perceptions of cultural differences between agencies.

Common examples include differing organisational cultures between police and criminal intelligence agencies, where police agencies are focused on arrests and prosecutions, whereas criminal intelligence agencies, at least as it is explained here in the context of the ACIC, are more focused on intelligence analysis and appreciating the 'bigger picture'. Consider the following quote from a member of the ACIC:

> We have a lot of subcultures in our fusion centre. That's based on where we come from and the fact that there are some secondees that come into the agency, particularly to use their policing powers in a very traditional sense...And they keep those cultures alive because they are only here for two years; they will go back to their own agency…They have learnt what works well for them in their agency and they're not going to change that (ACIC Fusion Capability Focus Group).

Another interviewee highlights the need for individuals to attempt to understand and appreciate the variety of cultures within fusion environments. By referring to such environments as being akin to a 'melting pot', the interviewee suggests that organisational cultures can break down over time:

> Fusion environments are funny where people come in and they are a typecast of their organisation's culture and you bring them into an environment where you've got a clash of cultures, it does become a melting pot…Once you find out that you've got a common purpose and objective in what you're doing, those sort of become moot points and you learn to work with each other and value what each other is about…You are here to work together and you have to appreciate each other's backgrounds, purpose and mission. And they will differ...But you work with it (ACIC JAG Interview).

Cultural differences clearly exist within fusion environments, but that does not necessarily mean, according to participants, that differing cultures are a negative variable.

Organisational and interpersonal trust

Trust, like culture, has been defined in different ways and takes many forms (eg Bachmann & Zaheer 2006). One influential view of trust defines the term as 'a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another' (Rousseau et al. 1998: 395). Distinguishing between personal and organisational trust is difficult, although one of the leading approaches suggests that interpersonal trust is the trust one places in 'their counterpart' and inter-organisational trust is the trust one places in 'the partner organisation' (Zaheer, McEvily & Perrone 1998: 142).

Interviewees repeatedly discussed the relationship between interpersonal and inter-organisational trust. They often suggested that one leads to the other and noted that fusion centres often require both forms of trust to perform well:

> I think one leads to the other [interpersonal trust and organisational trust]. So you develop, well in my experience…you start small. You build a relationship through…a commitment of some sort. And then you've got that initial trust; then you share that experience with the rest of the agency or with teams within the rest of the agency. If it's seen to be something that is important, for a higher-level involvement, then that kind of provides the basis for forming the agency-to-agency arrangements (ACIC Fusion Centre Focus Group).

Evoking a familiar metaphor, the interviewee refers to institutional trust as the 'bricks' and interpersonal trust the 'mortar', in forming relationships between network members:

> I would have thought that institutional trust is kind of like the big rocks and the interpersonal trust is like the sand or the water that would fall between the cracks. And if you didn't have one or the other the whole thing doesn't work. But institutional pieces are the slow evolution of departments talking at departmental level…But it's the people who sit between that, take the rough edges off and smooth it out (ACIC Fusion Centre Focus Group).

Fusion centres and related environments clearly involve multiple levels of trust. Indeed, focus group participants repeatedly emphasised the importance of inter-organisational and interpersonal trust for fusion centres. Many respondents also spoke to the idea of fostering 'a culture of trust', highlighting the relationship between organisational culture and trust.

Conclusion

This chapter has outlined the application of a network perspective to understanding the complex structural and relational dynamics of fusion centres and related environments. There is a notable dearth of empirical research on fusion centres; moreover, the research that does exist is almost exclusively United States-focused (eg Carter & Carter 2009; Lewandowski, Carter & Campbell 2017; Ratcliffe & Walden 2010; Taylor & Russell 2012). Given the significance of fusion centres for inter-agency collaboration, fusion environments are critically important areas for further research.

Comparative research, looking at different fusion centres across the ideal-types of security networks (Whelan & Dupont 2017), represents an important first step in any research agenda, since the underlying purpose of fusion centres is likely to vary according to how they organise and operate. It is too early to speculate about the benefits of fusion centres, and particularly the effectiveness of different models of fusion (eg co-located vs core/periphery), for criminal intelligence, given the current state of original empirical research. While there are many applications of a network perspective that have been beyond the scope of the chapter to address, this research has focused on the structural properties shaping the design and membership of fusion centres and the relational properties that considerably impact how they form and function.

Acknowledgements

The authors would like to sincerely thank all participants for taking time out of their busy schedules to participate in this study.

References

URLs correct as at February 2018

ACIC 2016. Retrieved from https://www.acic.gov.au/about-crime/taskforces/national-criminal-intelligence-fusion-capability

Ahuja G, Soda G & Zaheer A 2012. The Genesis and dynamics of organizational networks. *Organization Science* 23(2): 434–48

Bachmann R & Zaheer A (eds) 2006. *Handbook of trust research*. Cheltenham, UK: Edward Elgar

Carter D & Carter J 2009. The intelligence fusion process for state, local, and tribal law enforcement. *Criminal Justice and Behaviour* 36(12): 1323–39

Chermak S, Carter J, Carter D, McGarrell EF & Drew J 2013. Law enforcement's information sharing infrastructure: A national assessment. *Police Quarterly* 16(2): 211–44

Kilduff M & Tsai W 2003. *Social networks and organizations.* London: Sage Publications

Lewandowski C, Carter J & Campbell W 2017. The role of people in information-sharing: Perceptions from an analytic unit of a regional fusion center. *Police Practice and Research* 18(2): 174–93

Monahan T & Palmer NA 2009. The emerging politics of DHS fusion centers. *Security Dialogue* 40(6): 617–36

Monahan T & Regan PM 2012. Zones of opacity: Data fusion in post-9/11 security organizations. *Canadian Journal of Law and Society* 27(3): 301–17

Persson G 2013. *Fusion centres—lessons learned: A study of coordination functions for intelligence and security services.* Stockholm: Swedish National Defence College

Provan K & Kenis P 2008. Modes of network governance: Structure, management and effectiveness. *Journal of Public Administration Research and Theory* 18(2): 229–52

Provan K, Fish A & Sydow J 2007. Interorganizational networks at the network level: A review of the empirical literature on whole networks. *Journal of Management* 33(3): 479–516

Ratcliffe J H & Walden K 2010. State police and the intelligence center: A study of intelligence flow to and from the street. *IALEIA Journal* 19(1): 1–19

Rousseau D, Sitkin S, Burt R & Camerer C 1998. Not so different after all: A cross-discipline view of trust. *Academy of Management Review* 23(3): 393–404

Rojek J & Kaminski RJ 2011. An assessment of the utility of a state fusion center by law enforcement executives and personnel. *IALEIA Journal* 20(1): 1–17

Schein E 2010. *Organizational culture and leadership*, *4th ed*. Hoboken, NJ: Jossey-Bass

Taylor R & Russell A 2012. The failure of police 'fusion' centers and the concept of a national intelligence sharing plan. *Police Practice and Research* 13(2): 184–200

Whelan C 2012. *Networks and national security: Dynamics, effectiveness and organisation.* London: Routledge

Whelan C 2016a. Informal social networks within and between organisations. *Policing: An International Journal of Police Strategies & Management* 39(1): 145–58

Whelan C 2016b. Organisational culture and cultural change: A network perspective. *Australian & New Zealand Journal of Criminology* 49(4): 583–99

Whelan C 2017. Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration. *Security Journal* 30(1): 310–27

Whelan C & Dupont B 2017. Taking stock of networks across the security field: A review, typology and research agenda. *Policing and Society* 27(6): 671–87

Zaheer A, McEvily B & Perrone V 1998. Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science* 9(2): 141–59

Chapter 3: Can we forestall terrorism and frustrate organised crime by means of metadata retention?

Rick Sarre

In order to frustrate and block those who would orchestrate organised crime or perpetrate violence in the name of some particular ideology, governments now have the capacity to keep track of mass electronic data, referred to as metadata. Branch (2014) defines metadata as, simply, data that puts other data into context. Metadata is an electronic building block that can be used in investigations into terrorism, organised crime and crimes that are carried out online (such as those dealing with child exploitation materials).

We are all familiar with phone tapping. This telecommunications data contains the contents of the conversations themselves. Metadata, by contrast, does not contain content. It is simply information about the telephone numbers or message links involved in the communication, the location of the caller and receiver, the date and time of the calls and the length of the conversation. It includes data pertaining to Short Message Service (SMS) text messages sent and received. Uniform Resource Locators (URLs) and World Wide Web (www) browsing histories are said to be specifically excluded from the metadata retention law, although the Internet Protocol addresses of users' devices are accessible (Fernandes & Sivaraman 2015). What this means is that the locations of the devices that are sending messages can be tracked. Getting a warrant to access telecommunications (conversation) data is much more difficult than accessing metadata; hence, the great interest shown by law enforcement agencies in the gathering and analysing of the latter.

With the ubiquity of 'smartphones' today, any agency that has been granted a licence to track and retain metadata will find an enormously rich trail of information regarding users' locations, calls and networks. However, the qualms arising from this new phenomenon are many and varied, especially about the universal nature of the collection, the lack of consent of those whose metadata is being collected and the fact that metadata can be collected without the need for an agency to apply for a warrant (Branch 2014: 10).

The crucial question that flows from this is: how does a society find an acceptable balance between the rights of its citizens to enjoy freedom from the prying eyes of others, and the legitimate interests that the state might have in monitoring them? In July 2015, the then Australian Communications Minister (and now Prime Minister), Malcolm Turnbull, expressed the task in this way:

> [W]e need to recognise that getting the balance right is not easy (not least because the balance may shift over time) and we are more likely to do so if there is a thoughtful and well informed public debate—weighing up the reality of the national security threat, the effectiveness of particular proposed measures and then asking whether those measures do infringe on our traditional freedoms and if so whether the infringement is justifiable (Turnbull 2015).

Have we got that balance right? An appropriate equilibrium must be struck between forestalling crime and terrorism using all available electronic means, while not unduly curtailing the legitimate rights to privacy that citizens in modern democracies currently expect to enjoy. In the paragraphs that follow, there is an examination of what Australia's new laws do (and what they do not do) in relation to this quest today.

The legislation

In 2015, new laws came into force in Australia requiring telecommunications service providers to retain and store their 'metadata' for two years so that it remains available for analysis by anti-terrorism strategists and organised crime fighters (Sarre 2017a). This was not the first foray into this legislative territory. Australia's legislative journey regarding the retention and management of telecommunications data has evolved steadily over the last two decades.

It began with amendments to the *Telecommunications (Interception and Access) Act 1979* (Cth), followed by the enactment of the *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* (Cth) and the passage of the *National Security Legislation Amendment Act (No. 1) 2014* (Cth). These Acts combine to permit Australian Security Intelligence Organisation (ASIO) operatives to access metadata without a warrant if they are satisfied that accessing the information is in connection with the performance by ASIO of its functions (Rodrick 2009). Other Acts give the executive arm of the government other powers (Australian Parliament 2016), including the power to declare certain organisations illegal and to impose control orders on citizens whom it believes to be a danger to public order (Lynch, McGarrity & Williams 2015).

Metadata retention emerged as a potential strategy with the release, on 24 June 2013, of the report of the Joint Committee on Intelligence and Security (Australian Parliament 2017). The Joint Committee discussed the idea that telecommunications data be stored for up to two years in case it was required by law enforcement or security agencies, noting that such a scheme would be of 'significant utility' to national security agencies.

However, the Joint Committee also said that a metadata retention scheme raised fundamental privacy issues. The committee did not make a recommendation on the subject, however. It formed the view that a metadata retention policy must be a decision of government, and it was not for the Joint Committee to determine what the government should do.

The then Prime Minister, Tony Abbott, and his government moved quickly on the matter and introduced into the Australian Parliament the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. The Bill required telecommunications companies to retain metadata for two years to enable access by ASIO, the Australian Federal Police (AFP) and other federal, state and territory law enforcement agencies, if they had any interest in the data.

The list of such agencies was initially a long one (some 80 agencies, since reduced to 21 in 2017), such as government agencies (including local government), crime commissions, corruption watchdogs, customs agents and corporate regulators, not all of which command the full confidence of the public (Kearon 2013).

In the parliamentary discussion that followed, Greens Senator Scott Ludlam, a fierce critic of the scheme, foreshadowed dire consequences:

> Access to private communications records is already out of control in Australia, with telecommunications regulator the ACMA [the Australian Communications and Media Authority] reporting 580,000 warrantless demands in the last financial year. Mandatory data retention simply adds warehouses full of new private information to this broken access regime. I am not one who believes that if this bill passes into law, we will wake up on the following day in an authoritarian dystopia. Things are rarely that simple. But in the few years I've been working up close to Government, I've learned one important lesson: Governments cannot be trusted. This Government, the one before it, the one that will come after it (Ludlam 2015).

The Prime Minister at the time, Tony Abbott, was undeterred, offering the following:

> To help combat terrorism at home and deter Australians from committing terrorist acts abroad, we need to ensure our security agencies are resourced properly and have the powers to respond to evolving threats and technological change (Cited in Grattan 2015).

The government sought to allay concerns by assuring naysayers that the new protocols place useful data in the hands of those who can use it to detect criminal and terrorist activities, to demand strict controls of those who keep the data and to install adequate protections, such as safeguards for whistleblowers.

Indeed, the legislation gives a role to the Commonwealth Ombudsman to assess agency compliance with the requirements of both Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (preserving and accessing stored communications) and Chapter 4 (accessing metadata) of the Act. The Act became law on 26 March 2015, and became operative on 13 October that year.

Concerns

There are ongoing issues associated with this legislative approach. Each of these will now be examined in turn.

Privacy

The concern here is that governments may use metadata for purposes unrelated to the original collection. Under Section 6(1) of the *Privacy Act 1988* (Cth) (the Act that is best designed to ensure that the public is able to enjoy their privacy), 'personal information' is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. This means that the Act does not apply to the use of algorithms that assess anonymous data. In other words, the metadata retention scheme will not be amenable to legal challenge on the grounds that it breaches the Privacy Act. Hence, the protections in that Act relating to exclusions for purposes unrelated to the collection of data are not applicable.

Civil liberties

It has been argued that these laws erode the democratic freedoms that they are designed to protect. Any 'over-reach' undermines Australian freedoms and does so to a far greater extent than the laws of other comparable nations. Democracies such as France, Germany and Israel have not legislated for mass metadata collection. They rely, instead, on more targeted means to combat terrorism (Gal 2017).

In the event that ministerial discretion is based upon regulations that do not need to be put up for parliamentary scrutiny, there is potential for 'mission creep' or the extension of policy implementation in practice that goes beyond the scope of the 'mission' that was initially approved. Metadata retention has the capacity to be caught up in mission creep.

International access to metadata

In October 2015, in *Schrems v The Data Protection Commissioner and Digital Rights Ireland Ltd (Case C-362/14)*, the European Court of Justice was asked to determine a challenge to the 'Safe Harbour' agreement. This agreement, between the European Union and the United States, was formed in 2000 and was designed to protect private data collected by internet companies. Specifically, it protects data collected in Europe when that data is shared with US providers.

The court found that US legislators fell short of providing the sort of privacy guarantees that their European subsidiaries were bound by, and, therefore, the agreement was unsustainable. In other words, the 'Safe Harbour' agreement could not proceed, because it did not comply with European human rights law. One could imagine a similar problem arising with Australian metadata. Can Australian lawmakers guarantee that all countries analysing Australian metadata do so while preserving the privacy safeguards set out under Australian legislation? The answer is not immediately clear.

Future-proofing

Will metadata continue to be useful for agencies, given the ingenuity of wrongdoers to defeat the system? In other words, is metadata retention 'future proof'? The answer appears to be no. Technologies that frustrate data collection are readily available and widely used. Any person today can use a device that cannot be traced to the sender, or a virtual private network (VPN) that will allow encryption, or a secure drop system based on Tor, or the 'Onion Router'.

The encrypted messaging app Wickr likewise circumvents data retention, because it is a US-based service whose metadata cannot be captured by Australian telecommunications companies. It also uses encryption which, it claims, is 'uncrackable'. Indeed, anyone can communicate across Australia using international platforms such as Phantom Secure, Blackberry, WhatsApp, Tango, Threema and Viber, all of which use some form of encrypted messaging service.

Counter-productivity

There is an argument that the data retention laws may even be counterproductive if they are perceived to be targeting unfairly certain groups of citizens. Indeed, in April 2017, an AFP operative sought and acquired the call records of an Australian journalist without a warrant. The AFP Commissioner, Andrew Colvin, quickly acted to alert the media and to offer the opinion that there was no ill will or bad intent. While this assurance is comforting, the ease with which the access was obtained remains a matter of concern.

Government 'over-reach'

Governments that introduce innovations such as metadata retention laws are best held to account if citizens remain vigilant and vocal. Can we safely assert that an appropriate balance has been struck between the required levels of surveillance for the public good and the rights of individuals to be free from the prying 'eyes' of government, especially when so much of this outsourcing is in the hands of the private sector (see, further, Sarre 2017b; Prenzler & Sarre 2017)? The answer to this question remains equivocal.

Effectiveness

It is still too early to say whether the new laws are operating as planned or whether they are having the desired effect.

There has been anecdotal evidence from time to time that the government has disrupted a number of terrorist incidents and serious criminal activity, but there has been no actual evidence that the disruption was caused or even aided by government agency access to metadata. Because of the secrecy that usually shrouds issues related to national security, it is virtually impossible for the public to assess whether the actions of security agencies are effective or necessary, or even what they might actually involve.

Summary of the evidence

One can summarise the above evidence as follows: agencies that have access to metadata are generally compliant with the legislation. But we are less sure about our right to anonymity, especially given that the Privacy Act is not applicable to metadata collection. And, while there are still guidelines to ensure that metadata is not used for purposes other than those outlined in the law, the dangers of 'mission creep' are ever-present, and the links to 'big data' manipulation remain unexplored.

Moreover, we cannot guarantee that our 'Five Eyes' colleagues will adopt the same strict standards as Australian agencies in the collection and storage of metadata (to avoid the possibility of mistakes, for example). Nor can we guarantee that the retention policy cannot be circumvented entirely by encrypted international service providers. Moreover, there is good reason to suspect that the retention regime might indeed be counterproductive if it fails to win hearts and minds or focuses unduly upon people, such as journalists, who are endeavouring to preserve 'the right to know' that is essential to democratic principles. Finally, the evidence of effectiveness is anecdotal only and is supplied, without direct evidence, by the security agencies themselves.

It is worth remembering that, on 7 September 1939, just after Australia had declared war on Germany, the then Prime Minister, Sir Robert Menzies, called upon Australians to respond to the call but not to overreact to the threat (Menzies 1939). Malcolm Turnbull reflected, in July of 2015, upon Sir Robert's words, as follows:

> [Prime Minister Menzies] was leading Australia into a war against Adolf Hitler, a foe whose march across Europe must have seemed nearly irresistible. This was an existential threat. And he introduced a National Security Bill that gave extensive powers to the Government to control the economy and much of Australia's daily life in what was to become a total war effort. His warning to the House of Representatives should resonate down the years to all of us, especially those in the party he founded: 'The greatest tragedy that could overcome a country would be for it to fight a successful war in defence of liberty and to lose its own liberty in the process' (Turnbull 2015).

The Prime Minister might wish to reflect upon this wisdom as the government considers the effect of the legislation in the current political and worldwide security environment.

Conclusion

Researchers engaging in evaluation exercises need to keep in mind the range, breadth and volume of metadata that is currently available and how it is accessed. Policymakers need to keep all the above considerations in mind as they review the implementation of the metadata retention policy to ensure that it does what it set out to do, and in a manner that is justifiable and acceptable to a rapidly expanding body of citizens and organisations to whom it applies. Finally, legislators need to keep in mind all the above considerations, in order to ensure that no policy sacrifices liberty in the pursuit of a goal that is not easily nor readily attainable.

References

URLs correct as at February 2018

Australian Parliament 2016. *Advisory report on the Criminal Code Amendment (High Risk Terrorist Offenders) Bill 2016*. Canberra: Parliamentary Joint Committee on Intelligence and Security

Australian Parliament 2017. *Review of the implementation period of the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2014, 13 April*. Canberra: Joint Parliamentary Committee on Intelligence and Security

Branch P 2014. Surveillance by metadata. *Issues* 109 (December): 10–13

Fernandes C & Sivaraman V 2015. It's only the beginning: Metadata retention laws and the internet of things. *Australian Journal of Telecommunications and the Digital Economy* 3(3). http://telsoc.org/ajtde/index.php/ajtde/article/view/21

Gal U 2017. The new data retention law seriously invades our privacy—and it's time we took action. *The Conversation* 16 June. https://theconversation.com/the-new-data-retention-law-seriously-invades-our-privacy-and-its-time-we-took-action-78991?sa=pg2&sq=metadata&sr=1

Grattan M 2015. $131 million for companies' metadata retention in budget boost to counter terrorism. *The Conversation* 12 May. https://theconversation.com/131-million-for-companies-metadata-retention-in-budget-boost-to-counter-terrorism-41637

Kearon T 2013. Surveillance technologies and the crises of confidence in regulatory agencies. *Criminology and Criminal Justice* 13(4): 415–30

Ludlam S 2015. Data retention: we need this Opposition to oppose. ABC *The Drum* 27 February. http://www.abc.net.au/news/2015-02-27/ludlam-we-need-this-opposition-to-oppose/6269504

Lynch A, McGarrity N & Williams G 2015. *Inside Australia's anti-terrorism laws and trials*. Sydney: New South Publishing

Menzies RG 1939. *Hansard*. (Australia, House of Representatives) 7 September: 165

Prenzler T & Sarre R 2017. The security industry and crime prevention, in Prenzler T (ed) *Understanding crime prevention: The case study approach*. Samford Valley, Queensland: Australian Academic Press: 165–81

Rodrick S 2009. Accessing telecommunications data for national security and law enforcement purposes. *Federal Law Review* 37(3): 375–415

Sarre R 2017a. Metadata retention as a means of combatting terrorism and organized crime: a perspective from Australia. *Asian Journal of Criminology* 12: 167–79

Sarre R 2017b. The surveillance society: a criminological perspective, in Viano E (ed), *Cybercrime, organized crime, and societal responses: International approaches*. New York City: Springer: 291–300

Turnbull M 2015. *Magna Carta and the rule of law in the digital age*. Speech to the Sydney Institute, Sydney, 7 July

Chapter 4: The who, not the what—analysing public knowledge on organised criminals

Adam Masters

Since the early twentieth century, the Calabrian mafia—known variously by state and national police services as the Black Hand Society, Mafia, Camorra, the Honoured Society and 'ndrangheta—has had a presence in Australia. (Archival reports show that police and security services misidentified the 'ndrangheta for decades, conflating them with the Sicilian Cosa Nostra and Neapolitan Camorra.) While such a presence has, at times, been both confirmed and denied by government authorities and elected representatives, we are now at a stage of accepting its unquestionable presence as part of the Australian and international underworld. Well researched by the police and affiliated law enforcement and security agencies, the 'ndrangheta data gathering project outlined in this chapter aims to provide an empirical basis for academic analysis of the 'ndrangheta in Australia. Further developments in the subsequent 18 months have been incorporated to provide a fresh perspective on this long-term research project.

For the past several years, John Dickie at University College London (UCL) has led a small team researching the Australian 'ndrangheta (http://www.ucl.ac.uk/australian-ndrangheta). The word 'ndrangheta derives from the Greek term for honoured society. Other terms used in relation to the 'ndrangheta include 'ndrina ('ndrine pl.), which, according to the Italian Anti-Mafia Parliamentary Commission, is an autonomous subgroup in control of a small town or neighbourhood. If more than one 'ndrina is in the same town, they form a locale. Collectively, members of the 'ndrangheta are referred to as 'ndranghetisti (Varese 2011b: 31–32).

The UCL Australian 'ndrangheta research group has set itself the following research questions:

- How much can we discover, using both Australian and Italian sources, about the origins and development of Calabrian organised crime in Australia?
- How can we situate the history of the 'ndrangheta in Australia with regard to such issues as criminal legislation, policing, xenophobia, illegal markets, corruption and the non-Italian underworld?

- What relationship is there between the history of the Italian community in Australia (in particular the Calabrian community) and the history of the 'ndrangheta?
- How was the 'ndrangheta organised and how did it operate in Australia compared to the situation in Calabria?
- How significant have continued links between Australia and Calabria—in terms of organisation, personnel, kinship, and criminal enterprise—been in shaping the 'ndrangheta Down Under?
- What has been the public profile of 'ndrangheta crime in Australia over time? How has it been represented in official discourses and the media?
- What can Australian legislators and law enforcement learn from Italy about the 'ndrangheta and the fight against it?
- What can the Australian case teach us about the way the 'ndrangheta specifically, and mafia organisations more generally, spread into new territories?

Two of these have direct influence on the present 'ndrangheta data gathering project. Firstly, how much can we discover, using both Australian and Italian sources, about the origins and development of Calabrian organised crime in Australia? In brief, the answer is, quite a lot, thanks to the advent of open government policies and the explosion of reliable web-based sources of information.

The second two-part question relates closely to the first: what has been the public profile of 'ndrangheta crime in Australia over time? [and] how has it been represented in official discourses and the media? The data collection to answer the first question allows us to harvest textual representations required by the latter part of the second question. As a database of Australian 'ndrangheta related information grows, a picture of the 'ndrangheta's criminal profile in Australia should emerge.

What academia knows about the Australian 'ndrangheta

The academic research on the Australian 'ndrangheta is a limited subset of the broader research on this globalised criminal group. Naturally, the earliest research on the 'ndrangheta in general emanated from Italy, when they became the subject of specific inquiry, separately to the Sicilian Cosa Nostra (Paoli 1994). Italian scholars noted that, while state attention had focused on the Sicilians in the post-war decades, and academics variously analysed the Cosa Nostra influence on national politics (Della Porta 2004; Della Porta & Vannucci 2007; Paoli 1997) and judicial corruption (Della Porta, 2001), the Calabrians had quietly consolidated income and power free from academic scrutiny. Scholars of the mafia began to consider the 'ndrangheta in comparative work, as determined efforts were made to identify common social (Blok 2002; Dickie 2016; Ianni 1971; Paoli 2003), economic (Gambetta 1988, 1993; Paoli 2004; Skaperdas 2001) and political (Della Porta & Vannucci 2007; Paoli 1997; Skaperdas 2001) features for the various mafias. Importantly, Varese (2011a, 2011b) built on these works to explore how the Italian mafias and similar organised crime groups could successfully transfer themselves into new territories—including Australia.

Unlike the American offshoot of the Sicilian mafia—known in US law enforcement circles as La Cosa Nostra—far less attention has been paid to the Calabrian mafia émigrés in Australia by academics. A series of killings in the 1960s, colloquially referred to as the Melbourne Market Murders, received some attention from media analysts keen to see how Italian migrants were referred to in the press (White & White 1983). McCoy (1980, 1986) included the 'ndrangheta in his broader overviews of Australian organised crime. Little else emanated from the academic literature prior to the late twentieth century.

In recent years, a more focused approach has emerged. Nuzzi and Antonelli (2012) led matters with their Italian exposé of the 'ndrangheta's activities in Australia. What lent strength to their work was data obtained from an Italian police officer who had been seconded to the National Crime Authority in the 1990s. Freed from some of the constraints imposed by government secrecy, this work provided insight into the 'ndrangheta's structure, activities and membership rituals and corroborated many of the accounts previously published by investigative journalists (Bottom 1979, 1984, 1985, 1988; Moor 2009; Silvester & Rule 2009). Since Nuzzi & Antonelli's work, the UCL Australian 'ndrangheta researchers have provided a steady output, consolidating information from a variety of sources. Anna Sergi began by consolidating what is known about the movement of 'ndranghetisti to Australia as part of the wider Italian diaspora to the Southern hemisphere (Sergi 2015). Stephen Bennetts (2016) also analysed the early migration and establishment of the 'ndrangheta. Sergi returned in 2017 to compare how the 'ndrangheta were policed in Italy, the United States, Canada and Australia (Sergi 2017) as a follow up to her work with Anita Lavorgna (2016), which used the Australian case to support their theorising on what it meant to be, or to be becoming, a member of the 'ndrangheta. While the history and theorising are useful to our understanding of the Australian 'ndrangheta, data outside official records is diffuse and provides only a limited view into this part of the underworld. Building a dataset to enable detailed empirical analysis widens the view available to academic researchers.

Method

Obtaining current organised crime data from law enforcement agencies entails a range of problems. Cressey (1967) first noted this half a century ago. Working in collaboration with state authorities can limit the ability of researchers to openly publish their findings or can adversely influence research outcomes (Rhodes, 't Hart & Noordegraaf 2007), because security, investigative and judicial concerns are all paramount in comparison to researcher needs. Compounding this is the fact that reliable data on organised crime is scarce, representing an ongoing problem. Even the best data from official sources is limited by not only the knowledge gaps government agencies experience when investigating the underworld, but the dishonesty of 'ndranghetisti and their code of silence, or omertá (Varese 2011b: 49–50). The 'ndrangheta data gathering project therefore focuses on open source material.

Researching open sources

Open Source Information (OSIF) is defined by the North Atlantic Treaty Organisation (NATO) as:

> data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the OSIF world (NATO 2001: 2–3).

Guidance provided by NATO standard (NATO 2001) has since been added in the light of presentations at the 2017 organised crime forum (Kowalick 2017; Zolghadriha 2017). In this approach, the research mirrors to a great extent criminal intelligence analysis—recreating knowledge outside the confines of government agencies. Using open source information, a database has been created of publicly reported incidents and individuals associated with the Australian 'ndrangheta. Data collection remains ongoing, and the database is relatively small, so in-depth analysis is currently unavailable.

The Factiva™ newspaper database provided the initial data source. This database enables subscribers to search and access full text media reports from 1986 onward, with some older material also included. A test search of the term 'mafia' on Factiva on 15 October 2015 returned 28,926 results. The search captured not only reports of organised crime, but also thousands of references to entertainment media (eg television, film and computer gaming guides). 'Camorra' also proved ineffectual, particularly because the Australian media has moved on from that specific term. Thus, a more focused approach with snowballing became the approach, using 'ndrangheta as a search term.

Coding

The newspaper reports were downloaded and coded to identify features related to the media article itself, geographic information, criminality, connections to major events and perceptions of crime.

Article information

The data coded includes the title, media source and date of relevant media articles. Coding indicates whether the article is (g) general or (s) specific in nature—that is, focused on a particular 'ndrangheta case. These may include links and references to other cases. General articles are all others which include overviews or general commentary not linked to contemporary criminality—for example, anniversary reviews of significant incidents like the 1977 disappearance of anti-drugs campaigner Donald Mackay, who was probably murdered on the orders of the 'ndrangheta. Mackay's remains are yet to be found (see Moor 2009; Small & Gilling 2016).

Geographic coding

Geographic coding indicates 'ndrangheta activities in (A) Australia, (I) Italy or (O) other countries. Further coding is included for regions and a free text field for specific locations (eg Canberra, Gioia Tauro). This coding enables analysis of interactions between differently located groups.

Criminality

The coding for criminality records up to four main crime types discussed in the article. Table 1 provides the coding for crime types. Some codes may not be used. For example, if Dickie's (2016) historic analysis of the 'ndrangheta withdrawing from prostitution holds true for Australia, no data will be coded PR.

Table 1: Coding for crime types reported in media articles about the 'ndrangheta

AD	Arms Dealing	MC	Minor crimes, traffic etc.
Ass	Assault	Mur	Murder
CC	Computer crime	PR	Prostitution
DT	Drug Trafficking	SC	Sex Crimes
EP	Extortion/Protection	SS	Sexual Servitude
Fr	Fraud	Th	Theft
HT	Human Trafficking	PC	Political Corruption
Kid	Kidnapping	ML	Money Laundering

Connections

Links to significant events or reports are coded in this category. Events include Royal Commissions, named police operations and significant literature (mainly journalistic). Also included are significant crimes, which may be the subject of multiple inquiries. For example, the murder of AFP Assistant Commissioner Colin Winchester comes up in multiple inquiries and police operations; therefore, reference to the murder is more appropriate than listing multiple inquiries. As per crime, up to four links are captured, although more may be present. Table 2 identifies the significant events or reports identified to date. Coding for 'Pol'[itics] enables future comparison with the situation in Italy and Della Porta's (2004) work and provides data for an area of interest to UCL group member, Anna Sergi. Two significant police operations are included, but, as more are identified from media reports or other sources, the list will grow. Italian/Australian links are coded to identify cases of 'ndrangheta transnational criminality.

Table 2: Coding for links and connections with significant events and reports			
GW	Melbourne Gangland War	Pol	Politics/politicians
WRC	Woodward Royal Commission	MM	Mackay Murder
CRC	Costigan Royal Commission	OS	Operation Seville
WM	Winchester Murder	PRC	Police Royal Commission
NCA	NCA Bombing	OC	Operation Cerberus
IA	Italian/Australian links	VMM	Victoria Market Murders

Perceptions in Australia

This last category captures data coded by White and White's (1983) analysis of media reporting related to the Victorian Market Murders in the early 1960s. White and White's (1983) original work used the murders to analyse media depictions of migrant communities. By capturing the same data, this project hoped to trace the evolution of media portrayal of the 'ndrangheta in Australia. The coding determines whether the victim had respectability in the community, reflected by the tone/language or statements within the article (Y/N); views on the Italian community—respectable (Y), conflicted (N); whether the 'ndrangheta are present in Australia or denied by the journalist or interviewees (Y/N); whether mafia-like crime is alien to Australia (Y/N); if criminals had contempt for society (Y/N); and the consequences of migration for society—positive (Y) or negative (N). The coding of values is only captured for articles specifically related to Australia. However, early indicators are that media reporting of 'ndrangheta has moved a long way from the issues of the 1960s when the Victorian Market Murders occurred. Recent media reports no longer deny the 'ndrangheta presence, and there is little discussion on 'ndrangheta activity impacting on the broader Italo-Australian community. At a minimum, this coding enables tracking of changed values and perceptions in relation to organised crime in Australia.

Qualitative data

In addition to the coded data, the data gathering includes qualitative information. The main aim of the qualitative information is to identify individuals associated with the 'ndrangheta in Australia. Because of similarities among names and close kinship in many instances, qualitative data is essential to distinguish between fathers, sons, brothers, uncles, cousins and other male relatives. Female relatives are also identified, because they provide affinal kinship links between 'ndrangheta clans. Whenever possible, names are supplemented with nicknames, dates of birth, places of birth, migration data, known residences, criminal associates and familial ties. Not all this information is immediately available from media articles.

Other sources complement the database of media reports, including material from true-crime literature (Bottom 1979; Moor 2016; Silvester & Rule 2009; Small & Gilling 2016), publicly available reports (Costigan 1984) and archival holdings (National Archives of Australia, 1928–1969, 1937–1964, 1964–1964, 1964–1966, 1965–1968).

Finally, textual extracts from all sources provide details of criminal associations, criminal records on arrest and/or convictions for individual actors. These extracts provide a link back to the data source for key information. Such thick, descriptive material further allows for the investigation of discrepancies, contradictions and confusion. The various descriptions in the media and literature of the first 'ndranghetisti to arrive in Australia agree on how they arrived—via the ship *Re d'Italia*—yet disagree on the number and identity of the individuals.

Ethical research?

Research on individuals, their associates and their relatives raises questions of privacy and ethics—particularly because many relatives have no known criminal record. A description of the research project was provided to the Australian National University Research Ethics and Integrity Human Ethics Manager, who advised that, given the public nature of the information, the issue of consent for the subjects does not arise. Even so, future output from the database will remain sensitive to the potential for collateral damage to the privacy of 'ndranghetisti relatives and associates. Where required, data will be anonymised, and all publishable research will be referred to the appropriate ethics committees.

Early results

Although in its infancy, the database already shows promise for future research. The search of Factiva on 15 October 2015 for 'ndrangheta resulted in 579 hits, with 138 duplicates, leaving 441 relevant articles. Coding and disaggregation identified 121 'ndrangheta members, relatives or associates in Australia. Research to confirm the qualitative data identified a further 40 individuals. Further snowballing will grow the database significantly once the project moves fully into the true-crime literature and other data sources. A sub-project to explore intergenerational criminality added 46 names of an 'ndrangheta cell ('ndrina) arrested in Melbourne in 1957. A Victoria Police report on an Australian Security Intelligence Organisation (ASIO) file provided an excellent starting point for intergenerational research. Over 100 descendants were identified, none of whom is known publicly to be engaged in criminality (Masters, Fox, Scott-McLean & Hiu Tung Chow, 2017). This early finding empirically challenges public assumptions of intergenerational criminality. More empirical work will follow as the database grows.

References

URLs correct as at February 2018

Bennetts, S 2016. 'Undesirable Italians': Prolegomena for a history of the Calabrian 'Ndrangheta in Australia. *Modern Italy* 21(1): 83–99. doi: 10.1017/mit.2015.5

Blok, A 2002. Mafia and blood symbolism, in Salter FK (ed), *Risky transactions: Trust, kinship and ethnicity.* New York: Berghahn Books: 109–128

Bottom, B 1988. *Shadow of shame* South Melbourne: Sun Books

Bottom, B 1985. *Connections: Crime rackets and networks of influence Down-Under*. South Melbourne: Sun Books

Bottom, B 1984. *Without fear or favour*. South Melbourne: Sun Books

Bottom, B 1979. *The godfathers in Australia*. Sydney: AH & AW Reed

Costigan, F 1984. *Royal Commission on the activities of the Federated Ship Painters and Dockers Union, Final Report (vols 1–6)*. Canberra: The Government of the Commonwealth of Australia and the Government of the State of Victoria

Cressey, DR 1967. Methodological problems in the study of organized crime as a social problem. *The Annals of the American Academy of Political and Social Science* 374(1): 101–112

Della Porta, D 2004. Political parties and corruption: Ten hypotheses on five vicious circles. *Crime, Law and Social Change* 42(1): 35–60. doi: 10.1023/B:CRIS.0000041036.85056.c6

Della Porta, D 2001. A judges' revolution? Political corruption and the judiciary in Italy. *European Journal of Political Research* 39(1): 1–21. doi: 10.1023/a:1007134509892

Della Porta, D & Vannucci, A 2007. Corruption and anti-corruption: The political defeat of 'Clean hands' in Italy. *West European Politics* 30(4): 830–53. doi: 10.1080/01402380701500322

Dickie, J 2016. Mafia and prostitution in Calabria, c. 1880–c. 1940. *Past & Present* 232(1): 203–36. doi: 10.1093/pastj/gtw012

Gambetta, D 1993. *The Sicilian Mafia: The business of private protection*. Cambridge, MA: Harvard University Press

Gambetta, D 1988. Fragments of an economic theory of the mafia. *European Journal of Sociology* 29(1): 127–45

Ianni, FA 1971. The Mafia and the web of kinship. *The Public Interest* 22: 78–108

Kowalick, P 2017. International Policing: The implications for intelligence sharing and the impacts on transnational serious and organised crime. Paper presented at the Organised Crime Research Forum, Canberra

Masters, A, Fox, H, Scott-McLean, J & Hiu Tung Chow, V 2017. A tale of two mafias. Paper presented at the Australian and New Zealand Society of Criminology Annual Conference: Acknowledging the Past, Imagining the Future, 6–8 December, Canberra

McCoy, AW 1986. Organised crime in Australia: An urban history in Kelly RJ (ed), *Organized crime: A global perspective*. Totowa NJ: Rowman & Littlefield: 234

McCoy, AW 1980. *Drug traffic: Narcotics and organized crime in Australia*. Sydney: Harper & Row

Moor, K 2016. *Busted: The inside story of the world's biggest ecstasy haul and how the Australian Calabrian mafia nearly got away with it*. Australia: Penguin Random House

Moor, K 2009. *Crims in grass castles: The true story of Trimbole, Mr Asia and the disappearance of Donald Mackay, 2nd ed*. Camberwell: Viking

National Archives of Australia 1928–1969. Camorra, Black Hand, Mafia, Mano Nero Society Volume 1. Australian Security Intelligence Organisation; A6122, Subject files, multiple number series, 1915–(File: 3/2/364, Series: A6122, Item Barcode: 13618165). Canberra: National Archives of Australia

National Archives of Australia 1937–1964. Black hand activities in Australia—part 1. Department of Immigration; A6980, Secret correspondence files, single number series with block allocations and 'S' [Secret] prefix, 1932–, (File: S250530, Series: A6980, Item Barcode: 7117081). Canberra: National Archives of Australia

National Archives of Australia 1964–1964, 1964. Commonwealth Police investigation into migrant activity - General [organised crime, Mafia, criminal intelligence; 18 pp]. Attorney General's Department; A432, Correspondence files, annual single number series [Main correspondence files series of the agency] 1929–, (1964/2403). Canberra: National Archives of Australia

National Archives of Australia 1964–1966, 1964–1966. Black Hand Activities in Australia—newspaper clippings—1963. Department of Immigration; A446, Correspondence files, annual single number series with block allocations [Main correspondence files series of the agency], (1964/45214). Canberra: National Archives of Australia

National Archives of Australia 1965–1968, 1965–1968. Black hand activities in Australia—part 2. Department of Immigration; A6980, Secret correspondence files, single number series with block allocations and 'S' [Secret] prefix, 1932–, (S250539). Canberra: National Archives of Australia

North Atlantic Treaty Organisation 2001. *NATO Open Source Intelligence Handbook*. Brussells: North Atlantic Treaty Organisation

Nuzzi, G & Antonelli, C 2012. *Blood Ties: The 'ndrangheta: Italy's new mafia* trans. Hunt J. London: Pan MacMillan

Paoli, L 2004. Italian organised crime: Mafia associations and criminal enterprises. *Journal of Global Crime* 6(1): 19–31

Paoli, L 2003. *Mafia brotherhoods: Organized crime, Italian style*. New York: Oxford University Press

Paoli, L 1997. The political–criminal nexus in Italy. *Trends in Organized Crime* 3(1): 49–56. doi: 10.1007/s12117-997-1137-5

Paoli, L 1994. An underestimated criminal phenomenon: The Calabrian 'ndrangheta. *European Journal of Crime Criminal Law & Criminal Justice* 2: 212

Rhodes, RAW, 't Hart, P & Noordegraaf, M (eds) 2007. *Observing Government Elites Up Close and Personal*. Basingstoke: Palgrave MacMillan

Sergi, A 2017. *From Mafia to organised crime: A comparative analysis of policing models*. Cham: Palgrave MacMillan

Sergi, A 2015. The evolution of the Australian 'Ndrangheta. An historical perspective. *Australian and New Zealand Journal of Criminology* 48(2): 155–174. doi: 10.1177/0004865814554305

Sergi, A & Lavorgna, A 2016. *'Ndrangheta: The Global Dimensions of the Most Powerful Italian Mafia.* New York: Springer

Silvester, J & Rule, A 2009. *Underbelly: The Gangland War*. Melbourne: Allen & Unwin

Skaperdas, S 2001. The political economy of organized crime: Providing protection when the state does not. *Economics of Governance* 2(3): 173–202

Small, C & Gilling, T 2016. *Evil life: The true story of the Calabrian Mafia in Australia*. Sydney, Australia: Allen & Unwin

Varese, F 2011a. Mafia movements: a framework for understanding the mobility of mafia groups. *Global Crime* 12(3): 218–31. doi: 10.1080/17440572.2011.589597

Varese, F 2011b. *Mafias on the move: How organized crime conquers new territories*. Princeton, NJ: Princeton University Press

White, NR & White, PB 1983. *Immigrants and the media: Case studies in newspaper reporting*. Melbourne: Longman Cheshire

Zolghadriha, S 2017. Friends among thieves: The investigation of transnational organised crime networks. Paper presented at the Organised Crime Research Forum, Canberra

Part II: Understanding how organised crime groups operate

Chapter 5: Insiders versus outsiders—alternative paths to criminogenic knowledge

Douglas MC Allan

Within the constraints of this research, this chapter explores variations in how offenders acquire the knowledge, skills and techniques necessary to commit a range of financial crimes. It argues that foundation, or baseline, knowledge required by financial criminals is often learned in legitimate settings, including through on-the-job learning and legitimate daily routines. In the absence of traditional learning opportunities, four alternative learning sources are introduced in this chapter in order to reveal how legitimate knowledge, skills and technique deficiencies are met or augmented, often by organised crime groups, in order to facilitate crime. A clear distinction has been drawn between legitimate knowledge and skill learning and the learning of more specialised criminal techniques. This study contributes to the body of financial crime research on how these crimes are committed and highlights areas in which organisations and law enforcement agencies are able to reduce the opportunity for alternative learning sources that financial criminals may utilise in preparing for their crimes.

Theoretical explanations for how criminals approach their crime

Understanding why financial criminals commit their crimes has kept theorists and legislators busy for decades. Theoretical explanations of crime, ranging from Sutherland's (1947) differential association theory, Akers' (1973) social learning theory, Merton's (1938) strain theory, and rational choice theory (Becker 1962), have all been used in an attempt to explain why financial criminals committed their crimes. These ongoing examinations of why individuals commit financial crimes prompted Braithwaite (1985: 7) to question the continual need to explore the 'who' and 'why', while Levi (1984: 322) asserted that:

> In their obsession with the motivational issues surrounding why people do what they do, criminological theorists have tended to neglect the equally (if not more) important issue of how they are able to do what they do.

Indeed, Edelhertz (1970: 12) rather succinctly suggested:

> Basic to any determination of fruitful avenues of exploration with respect to the prevention, detection, and prosecution of white-collar crime, is an analysis of how it operates.

Cohen and Felson's (1979) routine activity theory begins to address the question of how offenders commit their crimes by exploring how ordinary daily routine activities bring motivated offenders into the presence of suitable victims in the absence of capable guardians. This is seen in Figure 1 below. This explanation has remained largely unchanged and offers the chance to study how crime opportunities arise, as opposed to studying the motivations of offenders; in essence, it is a meta-explanation of how crime opportunities arise. Despite its utility, there is, nonetheless, a difference between understanding how a criminal opportunity comes about and understanding how offenders commit their crimes.

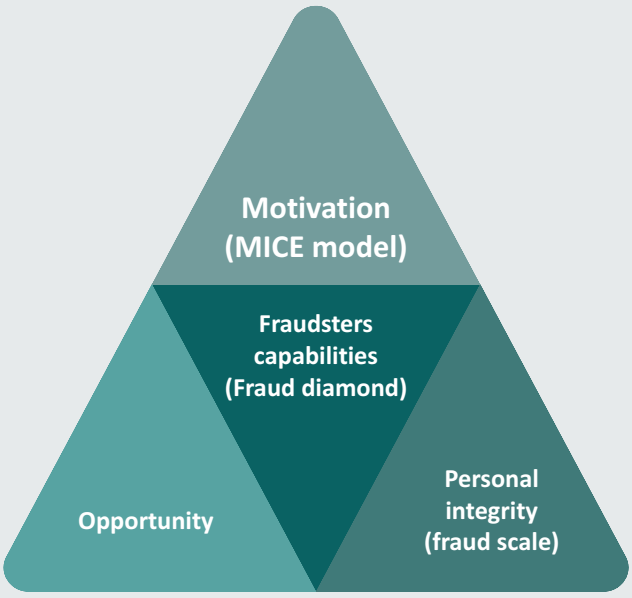
Figure 1: Routine Activity Theory

A growing body of literature that explores how financial crimes occur most commonly starts with the work on trust violators that Cressey (1950) undertook. Cressy hypothesised that fraud occurs when three things are present: (1) motivation to commit financial crime; (2) the internal justification or rationalisation processes adopted by the offender to lessen their culpability; and, finally, (3) the requisite structural opportunity to carry out the crime. However, it was Riemer (1941) who, when seeking to understand embezzlement, purposed a conflict situation as: '(1) the social pull; the opportunity, (2) the social push; the emergency situation

(motivation), (3) the psycho-pathological element involved'—which the fraud triangle itself mirrors. Despite this, the impact of the fraud triangle is such that Schuchter and Levi (2015) suggested that it is second only to Sutherland's (1947) differential association theory as a model capable of identifying the conditions under which white-collar crime occurs. Romney, Albrecht and Cherrington (1980), in suggesting 'fraud could theoretically occur under any situation if a person is motivated enough, even in the absence of outward opportunities or pressures', sought to refute the proposal by Cressey (1950) that all three elements needed to be present in order for the crime to occur, and, as such, 'opportunity is a necessary but not a sufficient condition for crime' (Schuchter and Levi 2015).

Wolfe and Hermanson (2004) proposed the addition of a fourth aspect via their fraud diamond model. They suggested that capability is a necessary inclusion, because of the often complex nature of financial systems and the potential high value of the crimes, and in instances where the crime is long term or ongoing. These factors, Wolfe and Hermanson (2004) suggested, require a level of offender capability specifically in terms of: (a) position function; (b) intelligence; (c) confidence/ego; (d) coercion skills; (e) effective lying; and (f) immunity to stress. The addition of capability addressed a weakness in the fraud triangle, specifically that, unless there is the capability to commit the crime, then the fraud does not occur (Kassem & Higson 2012).
Other studies built further upon the fraud triangle, with Albrecht, Howe and Romney (1984) proposing the replacement of rationalisation with personal integrity, and Dorminey et al. (2010) introducing M.I.C.E—Money, Ideology, Coercion and Ego—as an expansion of the motivation component first proposed by Cressey (1950). Most recently, Kassem and Higson (2012) proposed 'The New Fraud Triangle' as an amalgamation of the work of Cressey (1950), Wolfe and Hermanson (2004), Dorminey et al. (2010) and others, to bring together into one conceptual model the work of many, because 'it is important for auditors to consider all fraud models to better understand why fraud is committed', as shown in Figure 2 below.

Figure 2: The New Fraud Triangle



A strength of the New Fraud Triangle is its ability to focus attention on causal elements associated with fraud, including motivation and personal integrity/rationalisation. In addition, it creates the potential to explore more efficiently the nexus between offender capabilities, opportunity for crime, and something that is not represented in the model, the concept of capable guardianship as expressed by Cohen and Felson (1979).

Efforts to understand the nexus between capabilities, opportunity and guardianship have traditionally taken the form of crime script analysis (Cornish & Clark 2002) with a range of crimes, including fraud (Levi 2008), online stolen data (Hutchings & Holt 2015), public sector corruption (Rowe et al. 2013) and money laundering (Gilmour 2014). The strength of crime script analysis is its capacity to provide detailed knowledge 'about specific procedural aspects and procedural requirements of a crime' by examining multiple crimes of a highly similar or exact nature (Gilmour 2014).

A framework to elicit greater detail around how criminals approach their crimes

When seeking to understand how fraud and financial crimes are committed, an alternative approach to the traditional crime script analysis methodology exists, specifically when we begin with the generalisation that, in order for a complex crime to occur, four related stages need to occur—access, learning, planning and implementation. These related stages, however, are flexible and may occur in one situation whereby an employee with access to a particular financial system learns the financial system via the course of their legitimate occupational role, learns how it responds to unauthorised access, then, with criminal intent, plans their crime with that knowledge, finally implements the crime in a they believe is least likely to result in their detection. In a second scenario, the offender remains apart from the financial system, learns the necessary skills and techniques of offending within the dark web, plans their crime and implements it by obtaining access in a manner that minimises their risk of detection. In each example, these four stages occur, and, while the order may vary depending upon the circumstances, it provides a valid framework against which to begin addressing the question of how these crimes are committed as posed by Levi (1984) and Braithwaite (1985). The chapter now explores the literature that places learning at the centre of the criminal process, namely, differential association theory (Sutherland 1947) and social learning theory (Akers 1973) to understand how criminals acquire the knowledge, skills and techniques needed in order for them to commit financial crimes.

Acquiring criminogenic knowledge

As a distinct element of the framework proposed earlier, learning—specifically how offenders acquire the knowledge, skills and techniques necessary to carry out their crimes—is of interest from an academic and a practitioner's perspective alike (Sutherland 1947). Learning is the process whereby the individual develops the required knowledge, skills, and techniques to carry out particular tasks. In considering white-collar criminals' acquisition of knowledge, skills and techniques, it can be seen that it is in most instances an identical process, using the same legitimate methods, to that of law-abiding workers who have access to financial systems, with the obvious exception of learning criminal motivations and rationalisations.

Sutherland (1947) suggested, when proposing differential association theory as a general theory of crime and one that addressed the white-collar criminal specifically, that this learning process occurs where individuals are exposed to a variety of definitions, some in favour of law violation and others opposed to law violation. Accordingly, the central principle is that, rather than being viewed as an inherited trait, criminal behaviour was communicated in interaction with others, in intimate groups; and the learning taking place involved the learning of both skills and techniques associated with the crime, as well as the motivational, rationalisation and justification aspects (Sutherland 1947). As a result, white-collar crime occurs when the individual is exposed to an excess of definitions in favour of law violation, as compared with definitions in favour of abiding with the law. Matsueda (1988) argued that it was more important that the individual learned the relevant drivers, motivations and rationalisation for committing crime, and this aspect of differential association theory has received more research attention; however, it is the case that, without knowledge, skills and techniques, certain crimes, including many white-collar crimes, may not be possible.

The opportunities available to criminals to learn, however, are not restricted to discourse between professional peers, as the work of Burgess and Akers (1966) identified when integrating social learning theory (Bandura 1963), differential association theory (Sutherland 1947) and operant conditioning (Skinner 1938). Differential reinforcement theory asserts that learning occurs in social and non-social settings via observation, direct instruction and direct and vicarious reinforcement (Burgess & Akers 1966). Akers (1998), in a manner similar to differential association theory, also contended via social learning theory that intimate personal groups remain key to the transmission of knowledge, yet Akers also acknowledged the role of other avenues outside of closely defined family groups. Subsequently, understanding how criminogenic knowledge is acquired and where financial criminals source that learning will aid practitioners in understanding the factors that contributed to crime and provide an opportunity to refine theoretical explanations that seek to explain crime.

Method

The aim of this study is to develop an understanding of the potential sources of criminogenic knowledge and the variables that shape that access. This study involves the analysis of data from 19 law enforcement criminal investigation cases, finalised in a court of law, that were drawn from two Australian domestic law enforcement agencies. Case selection was determined by the following criteria. The financial crime must:

- have occurred within a definable financial system;
- be suitably complex in nature;
- involve fraud that required more than mere deception on the part of one individual;
- be valued at over AU$10,000;
- be committed across multiple jurisdictional boundaries; and
- have required the presence of an employee/internal actor for the crime to occur.

Data collected included interviews with case officers, statements of facts, witness and victim statements, offender interview transcripts and, where available, full case management files.

Data

Of the 19 cases that formed the dataset as seen in Table 1 below, approximately half (n=10) involved principal offender/s who were classified as trusted insiders, who were employed either directly by the victim organisation or on a contractual basis. The remaining nine cases involved principal offender/s who were classified as outsiders, who were external to the organisation they committed their crimes against. In addition to this, seven of the cases were classified as criminal syndicates, which is indicative of a self-organising group where individual members undertook distinct roles in the fulfilment of the joint criminal enterprise; the number of individuals per syndicate ranged from five to 42.

Table 1: Case data overview

Cases		Insider/Outsider status				How information needs were satisfied					
Case number	Crime type	Principal offender/s–Insider	Principal offender/s–Outsider	Associate offender/s–Insider	Associate offender/s–Outsider	Internal masters	Internal learners	Insider –insider	Outsider–victim	Outsider–associate–victim	Outsider–insider–victim
1	Accounting fraud	X			X	X					
2	Debit/credit card skimming		X	X	X				X	X	X
3	Debit/credit card skimming		X						X	X	
4	Debt refinancing	X				X		X			
5	ID manufacturing		X						X	X	
6	ID theft		X		X				X	X	
7	ID theft		X						X		
8	ID theft		X						X		
9	Insider trading	X			X		X	X			
10	Mortgage fraud		X		X				X	X	
11	Mortgage fraud		X	X	X						X
12	Procurement fraud	X			X	X					
13	Superannuation fraud		X	X	X				X		X
14	Tax evasion	X			X	X					
15	Tax evasion	X				X					
16	Tax evasion	X			X	X					
17	Theft as an employee	X			X	X		X			
18	Theft as an employee	X				X					
19	Theft as an employee	X					X				

Results

A selection of the collected data as outlined in Table 1 provides an overview of the cases against a number of variables. From those cases identified as having the principal offender/s as an insider, three distinct subgroups arose. The first insider subgroup (n=8), or Internal Masters, consisted of highly experienced and knowledgeable insiders with high levels of access and mobility across their respective organisations; this group's mastery of their role and organisation was critical to the success of their criminal venture. However, the second insider subgroup (n=2), or Internal Learners, consisted of generally more junior or less experienced insiders who, having lower levels of knowledge and freedom of access, had to actively seek out the knowledge necessary to commit their crimes. The final insider subgroup (n=3), or Insiders, represented cases where the principal (either master or learner) also used an insider within another organisation to address information or data gaps in order to commit their crimes. When looking at the nine cases where the principal offender/s was an outsider, three subgroups also arose. The first outsider subgroup (n=8), Outsider–Victim, represented cases where the principal offender interacted directly with the victim organisation in order to obtain the necessary information that was later used to commit their crimes. The second outsider subgroup (n=5), Outsider–Associate–Victim, consisted of outsider principals who engaged other outsiders, often criminal associates, to interact with the victim organisations in order to acquire necessary information. The final outsider subgroup (n=3), Outsider–Insider–Victim, consisted of outsider principals who used insiders from other organisations to obtain necessary information for them to commit their crimes.

Seven of the 19 cases, specifically case numbers 2, 3, 5, 6, 7, 10 and 13, were crimes committed by groups of offenders classified as organised criminal syndicates. In these cases, the principal offenders were all outsiders who, on three occasions, identified and acted upon the requirement to corrupt insiders within the victim organisation in order to obtain the necessary information and commit their crime. A further connection between all seven cases is that, in every instance, the principal offender/s engaged directly, and in person, with the victim organisations when either flaw hunting (Walsh 2014), free-range negative thinking (Walsh 2014), planning or preparing for their crimes.

Learning opportunities

As has already been discussed, the data in Table 1 reveal initial variations between how principal offenders might source knowledge capable of meeting their information needs and where they might go to obtain it. The research then examined more closely the specifics of those information sources.

Formal education

Analysis of the data revealed that, in approximately half of the cases (n=10), the principal offenders held tertiary qualifications, while in the remaining cases (n=9), they held no formal tertiary qualifications. While general statements like 'the higher the education level, the more

costly the fraud' (Association of Certified Fraud Examiners 2008) are common, research often provides examples where such thinking may not always reflect the reality of every crime (Benson & Simpson 2015; Weisburd et al. 1991). Certainly, the data from this project identified cases where, without formal tertiary accountancy qualifications (as seen in cases 1, 14, 15 and 16), the fraudsters would not have held their occupational positions and therefore would not have been in a position to commit those specific crimes. This was supported by the following observation from one law enforcement official, who suggested:

> they usually were from the top end of town, generally wealthier people from the wealthier end of town, went more often than not, to private schools, tertiary educated.

However, in cases 17, 18, and 19, exactly half of those internal fraudsters in CEO roles held no formal tertiary qualifications; instead, they reached their respective positions by working their way upwards within their organisations. This finding was also replicated in cases 9 and 11, where half of those fraudsters holding positions associated with selling financial products again held no formal tertiary qualifications.

Rather than revealing the necessity for formal tertiary qualifications as a prerequisite to financial crimes, this project provided a more balanced view where, in roughly half the cases, no such requirements existed. In these cases, the fraudsters' access to occupational positions came about, not via tertiary qualifications, but through working their way up within the organisation. This pointed to the proposition that, while access to occupational positions might be a requirement to commit some forms of white-collar crimes, the same could not be said for formal tertiary qualifications in all instances; as such, formal tertiary qualifications were not a universal requirement for access to occupational positions that enabled would-be offenders to commit their crimes.

On-the-job learning

Unsurprisingly, the single largest source of learning as indicated by the data (n=12) was that of employees either learning on the job or completing legitimate in-house training, immediately upon commencement with the organisation or once underway in their particular role within the organisation. In the majority of those cases (n=10), it was the principal offenders who utilised their organisational knowledge in the commission of the crime; in a further three cases, the principal offenders relied upon the knowledge and skills of insiders from other organisations; but in two cases, the principal offenders were outsiders who leveraged information from insiders within the victim organisation to facilitate their crimes. In all 12 cases, the necessary familiarity with the victim organisations' financial systems came about as a direct result of close interaction facilitated by employment, as was highlighted by an interviewee in relation to case 12:

> …they had high levels of specialist skills, this was a fraud against a highly complex procurement process…they knew the procurement of software and so were highly experienced in how these systems were supposed to work and what they were supposed to do.

Exposure to criminal methodologies

A variation to the on-the-job learning opportunities was based on a combination of prior occupational knowledge and exposure to other offenders' current methodologies. In case 19, a former law enforcement official leading a corporate investigation department used law enforcement knowledge and skills from previous employment, financial systems and organisational control, knowledge from current employment and exposure to current fraudsters' modus operandi through the corporate investigations to plan, prepare and commit frauds against the organisation, leveraging the learning that came from the investigation of other criminals. In this case, the nature of the offender's occupational role required them to investigate crimes against the organisation. This provided the offender with the opportunity to analyse the illegal actions of the other criminals, to identify the methodology and the mistakes they made in relation to how and why they were detected and, finally, to adjust the technique in order to successfully commit a new crime.

Exposure to investigative practices

Cases 3, 5 and 7 provided examples of where convicted fraudsters had acquired new knowledge directly from law enforcement prosecution cases to assist them in refining their crimes. In these cases, the law enforcement practices were found in statements of material facts or facts sheets. A facts sheet is a document which prosecuting authorities are legally required to disclose to the accused or the accused's legal representative prior to trial. They contain, among other things, a 'summary of the circumstances surrounding the offence for which an accused is charged' (Western Australia Police Service 2016). The challenge faced by law enforcement agencies and prosecuting authorities is balancing the intended purpose of the facts sheet, to disclose the facts of the case in accordance with the law, against the desire not to reveal police methodology in the process. This difficult balance, when poorly executed, provides a rich source of learning for the repeat offender to determine how and why they were detected, and for the aspiring criminal, it provides a blueprint (albeit unsuccessful) for how a crime may be committed (Ekblom 1997).

While it is inappropriate to divulge specific law enforcement methodology within this context, for the astute reader of the facts sheet it provides a direct insight into how the offender might alter their crime in the future to avoid law enforcement detection (Ekblom 1997). The use of vehicular, physical and device surveillance by law enforcement was evident, with one facts sheet revealing the use of an installed surveillance device to acquire critical evidence; the learning available to the offender in this instance was that a subtle variation to their behaviour might have prevented the law enforcement agency from acquiring evidence at that time and place.

In other cases, there were examples of the activities undertaken by offenders to limit their chance of identification, both at the time of the crime and post-crime. Ekblom (1997), when discussing the adaptable offender, introduced the process of research and development into an offender's pre-crime activities. This opportunity for learning was present in case 6, where the offender's methodology relating to technical crimes was clearly articulated. In this instance, the necessary technology the offenders needed in order to carry out particular crimes, including the name and source location of the required hardware and software and the variations in how the technology was deployed depending on the location and nature of the intended victim, makes this a valuable source for offenders seeking an advantage over law enforcement.

Criminal facilitators

Crime and/or technical facilitators were present in cases 2, 10, 11, 12, 13 and 16. Smith (2014) describes facilitators as individuals who offer skill sets useful to organised crime groups. While cases 11, 12 and 16 are not classified as organised crime cases, they nonetheless utilised facilitators who provided valuable knowledge and skills necessary for the commission of the crime. Case 13, in particular, involved three facilitators: the first provided to the organised crime group the concept and mechanics of how the crime should operate, in return for a service fee; the second provided technical telecommunications expertise; the third provided information relating to internal control mechanisms within the victim organisation. Another example of facilitation included case 16, where an accountant who was resident in an offshore tax haven provided necessary contacts and services to allow Australian-based accountants and their clients to avoid legitimate taxation liability. Case 2 provided the example of the business owners who allowed their premises and payment systems to be used by an organised crime group who were harvesting client debit and credit card data, and case 11 highlighted the role a financial services sector insider played in testing the vulnerabilities in a lender's property valuation systems.

Dark web communities of practice

What might well be seen as a modern day manifestation of Sutherland's (1947) differential association theory and Akers' (1973) social learning theory was present in case 6, where the two principal offenders interacted with others in the dark web, actively seeking out learning opportunities. In a traditional sense, a community of practice, according to Wenger (1998), entails three components: (1) the domain; (2) the community; and (3) the practice. When applied to criminal learning in the dark web, the domain, or interest area, might be the development of bots capable of taking over another's computer, the dark web community, anonymous by its nature but still with a traditional spread of expertise from experts to beginners as found in a range of dark web forums, and, finally, the practice—the criminal endeavour—of distributing bots in order to harvest identity data from unsuspecting online users. This dark web community of practice provides criminally minded individuals with the ability to learn in what Wenger (1998) described as a social environment, because essentially, 'learning is, at its essence, a fundamentally social phenomenon'. Case 6 provided one example of offenders accessing dark web forums where they acquired necessary knowledge, skills and techniques that enabled them to steal identity details and use those to establish false identities which facilitated further financial crime.

Discussion

The nature of a financial system is that of a business structure that facilitates the legitimate exchange of value from one entity or account to another. Value exchanges across financial systems have historically required individuals or groups of individuals with the knowledge and skills necessary to process, record and monitor such exchanges, which in turn dictates that those individuals have the obligatory knowledge, skills and techniques needed to facilitate such activities. The financial criminal, like the legitimate employee, must understand how a financial system operates, both under normal operating conditions and how it operates, or is likely to operate, under abnormal operating conditions, such as when incorrect or fraudulent requests are made of the system. This need for knowledge of how a financial system operates is fundamental to all financial crimes that contributed to this research, including, but not limited to, superannuation, credit card skimming and cloning, procurement and mortgage and insider trading frauds. While learning theories assert that criminal behaviour, as distinct from a working knowledge of a financial system, is acquired via communication in intimate groups (Sutherland 1947; Akers 1973; Benson & Simpson 2018), it was Cohen and Felson's (1979) routine activity theory that acknowledged that much of the necessary systems knowledge is obtained via daily routine activities (McLaughlin & Muncie 2006). In part, at least, a fraudster's daily routines provide them with knowledge of specific financial systems which, in turn, enables the commission of a crime (Cornish 1994; Felson 1998; Smith; 2014), and it is the case that much of this knowledge is, and can be, legitimately acquired via occupational roles and other daily routine activities.

Table 2: Insider learning data

Insider cases								
		Traditional learning sources		Alternative learning sources				
Case number	Crime type	Formal tertiary qualifications	On the job learning	Exposure to criminal methodologies	Exposure to investigative practices	Criminal facilitators	Dark web communities of practice
1	Accounting fraud	X	X				
4	Debt refinancing		X				
9	Insider trading	X	X				
12	Procurement fraud	X	X			X	
14	Tax evasion	X	X				
15	Tax evasion	X	X				
16	Tax evasion	X	X			X	
17	Theft as an employee		X				
18	Theft as an employee		X				
19	Theft as an employee		X	X			

Drawing on all cases where the principal offender was classified as an insider, the data presented in Table 2 identifies a strong correlation between the internal offender and what might be termed legitimate traditional learning sources. Traditional learning sources, including on-the-job learning opportunities, formal tertiary qualifications and knowledge, skills and techniques acquired via routine daily activities, in these cases, provided the necessary knowledge base for these crimes to be committed within the constraints of the individual cases. In most of these cases (n=7), the learning centred on an organisation's internal financial systems and was, in most instances, sufficient to allow the offender to commit their crimes. However, in the remaining cases (n=3), further learning that was not available through legitimate traditional learning sources was sought. In cases 12 and 16, this included engaging with criminal facilitators, while in case 19, this involved studying the criminal methodologies identified as a result of workplace investigations.

A noticeable variation between insiders and outsiders in this study was represented in the data contained in Table 3. In the outsider cases, uniformity of learning sources was less evident, with a wider variety of what might be termed alternative learning sources being accessed.

In this context, the alternative learning sources reveal how offenders in these nine cases supplemented the absence of insider knowledge. This was achieved in a variety of ways, including corrupting insiders within victim organisations, engaging criminal facilitators and learning within the dark web.

Table 3: Outsider learning data

Outsider cases								
		Traditional learning sources		Alternative learning sources				
Case number	Crime type	Formal tertiary qualifications	On-the-job learning	Exposure to criminal methodologies	Exposure to investigative practices	Criminal facilitators	Dark web communities of practice
2	Debit/credit card skimming	X				X	
3	Debit/credit card skimming				X		
5	ID manufacturing	X			X		
6	ID theft						X
7	ID theft				X		
8	ID theft	X					
10	Mortgage fraud					X	
11	Mortgage fraud	X	X			X	
13	Superannuation fraud		X			X	

In nearly all insider cases (n=7), all information needs were satisfied via occupational positions that provided all necessary information. In the absence of direct access to financial systems, however, outsiders were forced to overcome information deficiencies through a range of alternative learning sources. While this is certainly not an exhaustive list, the research identified four alternative learning sources which, within the constraints of this research, assisted criminals to transition from possessing a baseline level of financial systems knowledge to a point where they were able to utilise that knowledge in a way which enabled them to commit a financial crime. Crime facilitators and the dark web, in cases 2, 6, 10, 11 and 13, provided the basis upon which the initial crimes were planned by outsiders, while in cases 3, 5, 7 and 19, exposure to criminal methodologies and exposure to investigative practices provided for both outsiders' and insiders' methods to either vary or improve upon their crimes.

The future

Understanding the nature of how criminal knowledge, skills and techniques are acquired, along with their sources, is an important step towards explaining 'how' financial crimes are committed. When considered within the context of a crime script, this assists with identifying potential points of intervention and disruption. For law enforcement, understanding how criminals learn and where and how they go about accessing necessary alternative learning sources provides a starting point from both a reactive investigative perspective and from a preventative perspective, as has been highlighted in the case of the information that can be gleaned from poorly constructed facts sheets.

It is anticipated that, as the major research project from which these findings arose comes to its completion, further alternative learning sources will be identified. Logically, sources including peer to peer learning (see Sutherland 1947; Burgess & Akers 1966) all play a part in reshaping baseline knowledge in order to commit financial crimes. In addition to this, longitudinal research into the evolution of offender lifelong learning practices would help to provide a more comprehensive picture of the role that passive and active learning has throughout an offender's life course.

References

URLs correct as at March 2018

Akers R 1973. *Deviant behaviour: A social learning approach*. Belmont: Wadsworth

Akers RL 1998. *Social learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press

Albrecht S, Howe K & Romney M 1984. *Deterring fraud: the internal auditor's perspective*. Institute of Internal Auditors Research Foundations

Association of Certified Fraud Examiners 2008. *Profiling a white collar criminal*. Austin, Texas: Association of Certified Fraud Examiners

Bandura A 1963. Social learning and personality development. New York: Holt, Rinehart and Winston

Becker GS 1962. Irrational behaviour and economic theory. *The Journal of Political Economy* 70: 13

Benson ML & Simpson S 2015. *Understanding white-collar crime: An opportunity perspective*. New York: Routledge

Benson ML & Simpson SS 2018. *White-collar crime: An opportunity perspective*. New York: Routledge

Braithwaite J 1985. White collar crime. *Annual Review of Sociology* 11: 1–25

Burgess RL & Akers RL 1966. A differential association-reinforcement theory of criminal behavior. *Social Problems* 14: 128–47

Cohen LE & Felson M 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44: 588–608

Cornish DB 1994. The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies* 3: 46

Cornish DB & Clark RV 2002. Analyzing organized crimes, in Piquero AR & Tibbetts SG (eds), *Rational choice and rational behaviour: Recent research and future challenges*. London: Routledge

Cressey DR 1950. The criminal violation of financial trust. *American Sociological Review* 15: 6

Dorminey JW, Fleming AS, Kranacher M-J & Riley RA 2010. Beyond the fraud triangle. *The CPA Journal* 80: 8

Edelhertz, H 1970. *The nature, impact and prosecution of white-collar crime*. Washington DC: National Institute of Law Enforcement and Criminal Justice

Ekblom P 1997. Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk, Security and Crime Prevention* 2: 249–65

Felson M 1998. *Crime and everyday life*. Thousand Oaks, CA: Pine Forge Press

Gilmour N 2014. Understanding money laundering: A crime script approach. *The European Review of Organised Crime* 1: 21

Hutchings A & Holt T 2015. A crime script analysis of the online stolen data market. *British Journal of Criminology* 55: 596–614

Kassem R & Higson A 2012. The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences* 3: 191–5

Levi M 1984. Giving creditors the business: Dilemmas and contradictions in the organisation of fraud. *International Journal of the Sociology of Law* 12: 321–33

Levi M 2008. Organized fraud and organizing frauds. *Criminology and Criminal Justice* 8: 389–419

Matsueda RL 1988. The current state of differential association theory. *Crime & Delinquency* 34: 277–306

McLaughlin E & Muncie J 2006. *The Sage dictionary of criminology*. London, Sage

Merton RK 1938. Social structure and anomie. *American Sociological Review* 3: 672–82

Riemer SH 1941. Embezzlement: Pathological basis. *Journal of Criminal Law and Criminology* 32: 411–23

Romney MB, Albrecht WS & Cherrington DJ 1980. Auditors and the detection of fraud: The authors provide a unique fraud-risk evaluation questionnaire. *Journal of Accountancy* 149: 63–9

Rowe E, Akman T, Smith RG & Tomison AM 2013. Organised crime and public sector corruption: A crime script analysis of tactical displacement risks. *Trends and issues in crime and criminal justice* no. 444. Canberra: Australian Institute of Criminology

Schuchter A & Levi M 2015. Beyond the fraud triangle: Swiss and Austrian elite fraudsters. *Accounting Forum* 39: 176–87

Skinner BF 1938. *The behaviour of organisms: An experimental analysis*. New York: Appleton-Century-Crofts

Smith RG 2014. Responding to organised crime through intervention in recruitment pathways. *Trends & issues in crime and criminal justice* no. 473. Canberra: Australian Institute of Criminology

Sutherland EH 1947. *Principles of criminology*. Philadelphia: Lippincott

Walsh D 2014. Victim selection procedures among economic criminals: The rational choice perspective, in Cornish DB & Clark RV (eds), *The reasoning criminal: Rational choice perspectives on offending*. New Brunswick: Transaction Publishers

Weisburd D, Wheeler S, Waring E & Bode N 1991. *Crimes of the middle classes: White-collar offenders in the federal courts*. New Haven: University Press

Wenger E 1998. *Communities of practice: Learning, meaning, and identity*. Cambridge: Cambridge University Press

Western Australia Police Service 2016. *Information Statement 2016–2017*. Perth: Western Australia Police Service

Wolfe DT & Hermanson DR 2004. The fraud diamond: Considering the four elements of fraud. *CPA Journal* 74: 38–42

Chapter 6: Responding to organised crime through intervention in recruitment pathways

Russell G Smith

This chapter examines the processes involved in recruitment and the opportunities and incentives that make participation in organised crime attractive for suitably motivated individuals. Armed with a sophisticated understanding of how recruitment takes place, it is possible to develop appropriate intervention strategies that would seek to disrupt recruitment pathways and to make it difficult for organised crime groups to secure the services of potential collaborators.

Considerable research has been undertaken into the daily activities of organised crime groups, including how they fund their operations, maintain control over communities and launder the proceeds of their criminal enterprises. Organised crime groups in Australia include outlaw motorcycle gangs (OMCGs; Holmes 2007; Lozusic 2002), ethnic-based crime groups, family-based crime groups and groups formed on the basis of place of origin, such as prisons (CCC WA 2005). The Australian Crime Commission has noted that:

> …although most organised crime activities in Australia are focused on illicit drug markets, organised crime is increasingly diversifying its activities, with convergences being observed between legitimate or licit markets and illicit markets (ACC 2013: 7).

Theoretical approaches

Criminological theory provides a number of insights into the processes through which crime is commissioned and then takes place. Edwin Sutherland's theory of differential association, for example, developed in the late 1930s in the United States to explain juvenile gang behaviour

(Sutherland 1939). Sutherland proposed that criminal behaviour is learned through a process of social interaction between individuals in which they learn how to commit crimes and to justify their illegal conduct (Sutherland 1939). He argued that, if the conditions favourable to acting illegally outweigh the frequency and intensity of conditions unfavourable to violating the law, then an individual is more likely to decide to break the law (Sutherland & Cressey 1974). Sutherland (1937) developed the theory drawing on his classic study, *The Professional Thief*, in which he analysed and described ethnographically the life and daily routines of professional thieves in the United States.

More recently, Derek Cornish (1994) developed the notion of 'crime scripts' to understand the processes by which criminals conduct their activities. Research of this kind has been applied in relation to the resale of stolen vehicles (Tremblay, Talon & Hurley 2001), cheque forgery (Lacoste & Tremblay 2003) and organised crime (Hancock & Laycock 2010).

Crime scripts, according to Cornish (1994: 161) are a sequence of 'script functions' and accompanying 'script actions' that organise our knowledge and understanding of routine behavioural processes. In the present context, these relate to the identification and engagement of co-offenders who can be encouraged to join in the illegal activity.

The recruitment of a third party to commit a crime can be broken down into a number of routine processes. These include preconditions, initiation, actualisation, doing and post-conditions, and these script functions have corresponding script actions (Cornish 1994). Following the development of an understanding of how organised crime groups may seek to recruit new members, a script analysis can be used to identify the script functions and corresponding actions.

This chapter explores the processes by which recruitment for organised crime takes place, from the perspectives of:

- existing members of organised crime groups seeking out new members to facilitate proposed criminal activities (recruiter pathways); and
- environmental opportunities, which make participation in organised crime attractive for previously law-abiding citizens (recruitee pathways).

Research evidence and anecdotal illustrations of identified pathways are drawn from a number of ethnographic studies of organised crime published in the academic literature. These include Hobbs (2013), Goldstraw-White (2012), Levi (2008), Matrix Knowledge Group (2007), Kleemans and de Poot (2008), Van Koppen (2012), Van Koppen & de Poot (2013), Adler and Adler (1983), Gambetta (2009), Morselli (2005, 2009), Veno (2012) and Mazur (2009). These are clearly only a small selection of the published literature on organised crime, but they provide firsthand, ethnographic accounts of recruitment practices in various organised crime contexts, which are relevant illustrations of the processes identified in this chapter. Generally, there has been little specific research on recruitment processes, apart from one doctoral dissertation that presented an economic model of how government policies can affect membership patterns among organised crime groups (Long 2013).

Recruitment pathways

Recruitment pathways can be examined from the points of view of those who are seeking to recruit new members to become involved in criminal enterprises (recruiter pathways) and those who may be the targets of recruitment initiatives (recruitee pathways). Often, recruitees are individuals without prior criminal connections who are seeking to raise funds in order to maintain their lifestyle or to consort with established crime figures for various reasons, as explained below. The pathways to recruitment also vary according to the organisational structure displayed by the group in question—be it hierarchically based, network based, or of more diffuse, loose arrangements (see UNODC 2002). Having centralised control can often make recruitment activities more targeted and efficient, while unstructured groups, such as those that exist online, often recruit in an ad hoc manner.

Recruiter pathways

Established members of organised crime groups seek out new members for a variety of reasons, including: the skillsets they offer, which might facilitate criminal activities such as the manufacture of illicit drugs or the counterfeiting of payment cards; their ability to use violence and intimidation, which crime bosses might not wish to undertake themselves; skills they possess in facilitating the laundering of the proceeds of crime; and their willingness to engage in high-risk activities involving weapons or explosives or other activities likely to lead to arrest. In addition, organised crime groups can seek to establish relationships with those in influential government positions who can assist in facilitating the flow of information or decisions relevant to proposed criminal activities.

Recruitee pathways

Pathways can also be understood from the perspective of those who are the subject of recruitment. Otherwise law-abiding citizens may seek to become involved in criminal enterprises for a variety of reasons. They might need funds to satisfy debts or lifestyle expenditure; they may have a desire to enhance their financial or social standing; or they might demonstrate an interest in risk-taking activities or possess motivations based in pathological psychological processes (Hobbs 2013; Kleemans & de Poot 2008; KPMG 2013). Rather than commencing criminal activities in isolation, they might seek out known criminals who could be seen to assist in their proposed course of action.

Crime scripts of recruitment

Hancock and Laycock (2010) have applied Cornish's (1994) approach to analysing criminal behaviour through the use of crime scripts to the disruption of organised crime and identified recruitment as one area where disruption might have potential. The present discussion identifies three main stages in the recruitment process as target identification, establishing trust and engaging in compliance, and enforcement script actions.

Target identification

One of the initial tasks which both recruiters and the targets of their recruitment have to undertake is the identification of willing and cooperative collaborators. This activity is fraught with risk, because identifying participants for criminal activity can, itself, be criminal and can also lead to threats of, or actual, violence being inflicted.

Identification by recruiters

Potential criminals are able to be sourced from many occupational and other groups in society, largely based on their interests and the skills they possess. This can include those with experience in telemarketing who can participate in boiler-room investment fraud (ACC 2012), ex-military personnel who have experience in the use of weapons and explosives, and members of the public willing to act as drug or money mules. On other occasions, organised crime groups may seek out those working in the professions, such as lawyers and accountants who can assist in laundering the proceeds of crime or in establishing corporate entities and other vehicles for use in tax evasion (see Choo et al. 2012).

Those working in the information technology and security industries also have attractive skills that organised crime can use. The other productive location for recruitment is the public sector, particularly those working in law enforcement, border control, intelligence and corrections. Rowe et al. (2013) provide examples of recent instances in which public servants in Australia have been recruited by organised crime to provide access to law enforcement intelligence through a range of corrupt practices.

Prisons, in particular, provide many opportunities for inmates to establish ties with other offenders, sometimes individuals with low-level convictions who can be recruited into more serious criminal enterprises, both while incarcerated or after their release. Prison recruitment also carries the benefit that everyone involved can be assured that those whom they approach have criminal records sufficient to warrant a term of imprisonment.

Identification by recruitees

Arguably, a more difficult task exists for those in the law-abiding community who wish to become involved in organised crime. One cannot simply approach people who appear to be criminal and seek membership of an illegal organisation. Some traditional organised crime groups are clearly recognisable, such as the Yakuza with their tattooed bodies (Adelstein 2010) or OMCGs with their club colours and patches (Veno 2012). Even if individuals are recognisably members of a criminal enterprise, there may still be many procedures that they are required to undertake in order to establish trust and to secure membership.

Diego Gambetta (2009) has explored in detail the use of non-verbal cues to facilitate identification of those involved in criminal enterprises and notes how the use of language and behavioural cues can facilitate covert introductions in ways that do not attract attention from authorities or others who may be disposed to report what transpires to the police. Subtle conventions in the use of language, dialect, dress and behaviour are used to ensure that trust and legitimacy in the criminal enterprise are guaranteed.

Serendipitous identification

Finally, identification of potential criminal collaborators may take place accidentally or inadvertently through contact that occurs in common meeting places such as pubs, casinos, gyms, brothels and internet sites. Often, these are places at which individuals with either law-abiding or criminal orientations meet, establish social relationships and begin the process of criminal collaboration. Similarly, unplanned recruitment can also arise within extended families, such as has been documented in the case of mafia families (Tyler 1971), while, more recently, social media have provided abundant ways in which people with common interests can establish relationships—for both legitimate and illegal purposes (Choo & Smith 2008).

On occasions, organised crime groups have simply advertised online for new recruits—such as advertisements for people to undertake credit card skimming operations (Glenny 2011: 203–204). Such online advertising for willing recruits is also prevalent in connection with online consumer scams such as work-from-home scams and online romance and dating fraud. Although increasing in sophistication, many such invitations are barely credible and yet continue to trick unsuspecting individuals into participation (Jorna & Hutchings 2013).

A further example of serendipitous recruitment in the Netherlands concerned a former truck driver who had set up a café to be able to spend more time with his family and who was recruited into transporting heroin for an organised crime group through contacts he had with a group of customers at his café. This provides a clear example of how routine activities can facilitate the recruitment process (Felson & Clarke 1998). The café owner was eventually sentenced to 12 years' imprisonment for heroin trafficking (Van Koppen & de Poot 2013). He explained how he became involved:

> You start talking and ask each other: 'What did you do before and where do you come from?' That's the first thing you do. And when I mentioned I'd been a truck driver for years, that triggered something of course. He should know people, maybe he wants to. But I never wanted to...I wasn't interested at all. I did not need the money and did not bite, it did not fascinate me. After some months, however…After all, they are your frequent customers and you talk to them all the time. There comes a time it goes through your mind that some others you know have the ability to and probably want to do it. At first I thought: I'll do them both a favour and I can earn some additional money, you know. I really did not see the danger in doing it (Van Koppen & de Poot 2013: 82).

Adler and Adler (1983) also found instances of serendipitous recruitment in which law-abiding individuals gradually became involved in drug trafficking in order to make use of their skills or to enhance their income.

Establishing trust

Establishing trust and confidence that the person with whom one is dealing is not an undercover police officer, or someone likely to blow the whistle, is often a lengthy and invasive operation, both for organised criminals and those whom they are seeking to recruit. In many cases, this can entail initiation tasks such as demonstrating criminal skills, providing samples of actual criminal conduct (particularly the use of violence) and showing a willingness to share confidential information with other group members.

In the case of online organised crime groups engaged in sharing child exploitation material, it is often the case that recruits need to supply extensive libraries of illegal exploitation images in order to establish their bona fides and to gain access to group libraries of similar material (Choo & Smith 2008; Wolak, Finkelhor & Mitchell 2011).

Establishing trust in the online criminal world can also require the use of various anonymising and security technologies. In particular, it is important to ensure that one's true identity is not revealed, and so aliases and false identities are invariably used when logging on to illicit websites. Security of data is also required, and organised crime groups now make use of encryption, steganography, biometrics and Tor software that reduces the risk of online activities being monitored by law enforcement. Some organised crime groups also require identity verification, both during enrolment and when undergoing regular checks designed to confirm trust and security of group members. An example exists in the case of OMCGs (Lozusic 2002).

Trust also needs to be maintained during the early stages of group membership, and tests are often used to demonstrate an absence of risk, proof of veracity and loyalty to the organisation. Occasionally, this can entail involvement in successful criminal operations in order to demonstrate skills and, in the case of unsuccessful activities, willingness to be convicted and serve prison time.

Compliance and reinforcement

Further proof of commitment to the cause may require financial investment in the organisation and successful recruitment of new members of the organisation—such as occurs in connection with online networks that share child exploitation material.

Failed recruitment

On occasions, recruitment may be unsuccessful and fail. This can occur where criminal activity is detected by law enforcement and new recruits are suspected of whistleblowing or of being undercover operatives (Mazur 2009). In the case of hierarchically organised networks, sanctions of escalating severity may be imposed, leading to expulsion from membership or threats of, or actual, violence and murder.

Intervening in recruitment pathways

Having explored the various pathways for the recruitment of individuals to engage in organised crime and identified the crime scripts associated with methods of recruitment makes it possible to identify strategies that could be considered to intervene in such pathways so as to make recruitment difficult and likely to lead to detection by law enforcement.

Not all of the available opportunities for intervention may be possible, having regard to privacy, human rights and legislative limitations on taking action. At a minimum, however, the ways in which recruitment takes place can be identified and made obvious and available for official scrutiny. The principal areas to address in connection with recruitment relate to the use by organised crime of anonymity, reliance on professional advisers, convenient meeting locations and the availability of motivated recruitees. There is also a need to publicise the risks associated with involvement in organised crime from the perspective of likelihood of arrest, confiscation of assets and physical harms that may be inflicted both personally and on friends and relatives of recruitees who participate in organised crime.

Addressing anonymity

Firstly, as Hancock and Laycock (2010) rightly emphasised, there is a need to address the use of anonymity among organised crime groups, especially those that operate online. In particular, removing the ability of organised crime to access pre-paid information and communication technologies (ICT) services and regulating the use of anonymising software and encryption for illegal purposes would be beneficial. Further, making effective use of existing lawful databases of persons convicted of organised crime could assist law enforcement with identification of recruitment activities, while enhanced data analysis of financial and cyber intelligence, including associated tracking of funds transfer locations, might be possible.

Regulating professional advisers

Enhanced efforts could also be made to ensure that financial advisers and accountants, in particular, are adequately regulated, to ensure that their services cannot be used, overtly or unwittingly, by organised crime groups.

Additional controls may need to be developed for other occupational groups, such as those in the transportation and ICT industries. Having procedures that could identify high-risk individuals within these sectors could assist in locating red flags for corruption before they are acted upon. For example, enhanced reference checking for those seeking employment in trusted positions in the transport industry and those working in ICT may help to identify individuals who may be subject to corruption. Similarly, having national standards and disciplinary controls for those working in ICT may help to identify high-risk individuals.

Prohibitions could also be enforced against those convicted of serious crimes from forming companies, and enhanced identity checks could be undertaken when businesses are being established that could be used in connection with organised crime. In addition, the use of Australia's anti-corruption regime could be used to identify potential infiltration of government by organised crime groups (Rowe et al. 2013). Allied to this is the need to encourage reporting of serious crime and the protection of those who make reports in the public interest.

Controlling meeting places

There is compelling evidence that recruitment takes place in a limited number of high-risk locations, particularly prisons, pubs, fitness clubs and brothels. Ensuring that fit-and-proper person tests applicable to those in charge of such venues are enforced might help to deter organised crime involvement. Similarly, ensuring that such businesses maintain accurate and verifiable records of members and regular users could also make some premises unattractive to organised crime.

Recent anti-organised crime legislative measures such as anti-fortification laws and anti-association laws could also be useful in ensuring that meeting places frequented by organised criminals are made less desirable places to congregate.

Finally, when police task forces are targeting organised crime groups, it would be beneficial to focus some activity on increasing the probability of detection of organised crime groups when attempting to recruit new members. Improving prison security and further development of corrections agency intelligence could assist in disrupting recruitment activities that take place within prisons, while allowing online data monitoring—with judicial authorisation—would assist law enforcement in identifying high-risk recruitment environments.

Attacking recruitee motivations

Attacking the motivations for involvement in organised crime by otherwise law-abiding individuals is an essential element in breaking pathways to recruitment.

For example, there is now an established awareness of the red flags of individuals becoming susceptible to involvement in serious financial crime (eg KPMG 2013), such as the presence of lifestyle pressures, gambling addiction and business failure.

An illustration of how personal financial difficulties led a senior public servant to be recruited by organised crime to obtain confidential intelligence for the group is the case of the former Assistant Director Investigations at the New South Wales Crime Commission, who became involved with a drug trafficking organisation and the importation of 300kg of pseudoephedrine. His motivations for becoming involved in the criminal organisation were clearly financial gain, to clear himself of debts and to provide for his family. To this end, he entered into an agreement with an informant and a legitimate businessman to import a large quantity of pseudoephedrine concealed in a container of rice (NSW Supreme Court 1422, 8 December 2011). Had the NSW Crime Commission been aware of his financial position, his vulnerability to corruption could have been identified and perhaps prevented. Any such monitoring of personnel would need to comply with privacy and human rights protections.

There is also evidence that neutralising the rationalisations or justifications for involvement in serious crime can be an effective deterrent to individuals acting illegally (Duffield & Grabosky 2001).

Publicising risks

Making organised crime unattractive and unprofitable through the confiscation of assets and use of unexplained wealth laws has been identified as a key strategy in preventing and responding to organised crime (Parliamentary Joint Committee on Law Enforcement 2012). Recent legislation that has sought to proscribe membership of organised crime groups could also have the indirect beneficial effect of deterring individuals from seeking to become new members of such groups through fear of prosecution as a member of a proscribed gang.

Broadhurst, Lauchs and Lohrisch (2014) argue, for example, that many OMCG members are simply motivated by a desire to have 'fun' and to engage in risk taking. Publicising the negative consequences of criminality, including the potential physical and mental harms, risk of imprisonment, loss of livelihood and involvement in addictions, could help to make organised crime appear to be an unattractive lifestyle choice.

Organised crime is a multifaceted, complex phenomenon and, as such, requires a multifaceted response strategy. Initiatives need to be flexible and dynamic and able to meet changes in the nature of organised crime as they become apparent. A key element of preventing and responding to organised criminal activity is to interdict or prevent individuals from being recruited into criminal organisations. This chapter has identified some potential ways in which this may be achieved which reinforce a multifaceted approach in order to combat organised crime.

Acknowledgements

This chapter was originally published as: Smith RG 2014. Responding to organised crime through intervention in recruitment pathways, in Trends and Issues in Crime and Criminal Justice No. 473, Australian Institute of Criminology, Canberra. This revised version is published with permission of the original publisher. Preliminary research was carried out by Cienan Muir during an Internship at the Australian Institute of Criminology.

References

URLs correct as at February 2018

Adelstein J 2010. The last Yakuza. *World Policy Journal* Summer: 63–71

Adler PA & Adler P 1983. Shifts and oscillations in deviant careers: The case of upper-level drug dealers and smugglers. *Social Problems* 31: 195–207

Australian Crime Commission (ACC) 2013. Organised crime in Australia, 2013. Canberra: ACC. https://www.crimecommission.gov.au/sites/default/files/ACC%20OCA%202013-1.pdf

Australian Crime Commission (ACC) 2012. *Serious and organised investment fraud in Australia*. Canberra: ACC

Broadhurst R, Lauchs MA & Lohrisch S 2014. Organized crime in Oceania, in Reichel P & Albanese J (eds), *Handbook of transnational crime and justice, 2nd ed.* Los Angeles, CA: Sage: 501–14

Choo K-KR & Smith RG 2008. Criminal exploitation of online systems by organised crime groups. *Asian Criminology* 3: 37–59

Choo K-KR, Smith RG, Walters J & Bricknell S 2012. *Perceptions of money laundering and financing of terrorism in a sample of the Australian legal profession*. Research and Public Policy series no. 122.1. Canberra: Australian Institute of Criminology

Cornish DB 1994. The procedural analysis of offending and its relevance for situational prevention, in Clarke RV (ed), *Crime prevention studies, vol 3*. Monsey, NY: Criminal Justice Press: 151–96

Corruption and Crime Commission of Western Australia (CCC WA) 2005. *Report to the joint standing committee on the Corruption and Crime Commission with regard to the Commission's organised crime function and contempt powers*. Perth: CCC WA. http://www.ccc.wa.gov.au/Publications/Reports/Documents/Published%20Reports/2005/organised-crime.pdf

Duffield G & Grabosky P 2001. The psychology of fraud. *Trends & issues in crime and criminal custice* no. 199. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi199

Felson M & Clarke RV 1998. *Opportunity makes a thief: Practical theory for crime prevention*. Police Research Series Paper 98. London: Home Office

Gambetta D 2009. *Codes of the underworld*. Princeton: Princeton University Press

Glenny M 2011. *Dark market: Cyberthieves, cybercops and you*. London: Bodley Head

Goldstraw-White J 2012. *White-collar crime: Accounts of offending behaviour*. London: Palgrave Macmillan

Hancock G & Laycock G 2010. Organised crime and crime scripts: Prospects for disruption, in Bullock K, Clarke RV & Tilley N (eds), *Situational prevention of organised crimes*. Cullompton: Willan: 172–92

Hobbs D 2013. *Lush life: Constructing organized crime in the UK*. Oxford: Oxford University Press

Holmes L 2007. Introduction, in Holmes L (ed), *Terrorism, organised crime and corruption*. Cheltenham: Edward Elgar Publishing: 1–28

Jorna P & Hutchings A 2013. *Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey*. Technical and background paper no. 56. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tbp/tbp056

Kleemans ER & de Poot CJ 2008. Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology* 5: 69–98

KPMG 2013. *A survey of fraud, bribery and corruption in Australia and New Zealand 2012*. Sydney: KPMG

KPMG 2010. *Fraud and misconduct survey 2010*. Sydney: KPMG

Lacoste J & Tremblay P 2003. Crime and innovation: A script analysis of patterns in check forgery, in Smith M & Cornish D (eds), *Theory for practice in situational crime prevention*. Crime Prevention Studies 16. Monsey, NY: Criminal Justice Press

Levi M 2008.*The phantom capitalists: The organisation and control of long-firm fraud, 2nd ed.* Aldershot: Ashgate

Long IW 2013. *Recruitment to organised crime*. Cardiff Economics Working Paper E2013/10. Cardiff University, Cardiff Business School, Economics Section. http://patrickminford.net/wp/E2013_10.pdf

Lozusic R 2002. *Gangs in NSW*. Briefing Paper No 16/02. Sydney: NSW Parliamentary Library Research Service

Matrix Knowledge Group 2007. *The illicit drug trade in the United Kingdom*. Home Office Online Report 20.07. London: Home Office

Mazur R 2009. *The infiltrator: My secret life inside the dirty banks behind Pablo Escobar's medellín cartel*. New York: Little Brown

Morselli C 2009. *Inside criminal networks*. New York: Springer

Morselli C 2005. *Contacts, opportunities, and criminal enterprise*. Toronto: University of Toronto Press

Parliamentary Joint Committee on Law Enforcement 2012. *Final report on the inquiry into Commonwealth unexplained wealth legislation and arrangements*. Canberra: Commonwealth of Australia

Rowe E, Akman T, Smith RG & Tomison AM 2013. Organised crime and public sector corruption: A crime scripts analysis of tactical displacement risk. *Trends & issues in crime and criminal justice* no. 444. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi444

Sutherland EH 1939. *Principles of criminology, 3rd ed.* Chicago: University of Chicago Press

Sutherland EH 1937. *The professional thief*. Chicago: University of Chicago Press

Sutherland EH & Cressey D 1974. *Criminology, 9th ed.* Philadelphia: Lippincott

Tremblay P, Talon B & Hurley D 2001. Body switching and related adaptations in the resale of stolen vehicles: Script elaborations and aggregate crime learning curves. *British Journal of Criminology* 41: 561–79

Tyler G 1971. Sociodynamics of organised crime. *Journal of Public Law* 20(1): 41–58

United Nations 2004. *United Nations Convention Against Transitional Organized Crime and the protocols thereto*. New York: United Nations. http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

United Nations Office on Drugs and Crime (UNODC) 2002. *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*. Vienna: UNODC. http://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf

Van Koppen MV 2012. Involvement mechanisms for organized crime. *Crime, Law and Social Change* 59: 1–20

Van Koppen MV & de Poot CJ 2013. The truck driver who bought a café: Offenders on their involvement mechanisms for organized crime. *European Journal of Criminology* 10: 74–88

Veno A 2012. *The Brotherhoods, 3rd ed.* Sydney: Allen & Unwin

Wolak J, Finkelhor D & Mitchell K 2011. Child pornography possessors: Trends in offender and case characteristics. *Sexual Abuse: A Journal of Research & Treatment* 23(1): 22–42

Chapter 7: Disengagement from involvement in organised crime—processes and risks

Kaylene Douglas and Russell G Smith

The study of criminal careers is critical to the understanding of offenders' involvement in crime (DeLisi & Piquero 2011). Unfortunately, relatively little is known about the pathways individuals take into participation in organised crime and how they may later disengage from their involvement (Smith 2014; Thompson et al. 2014). Life-course criminology and the crime desistance literature examine theories of persistence and desistance through adolescence and into adulthood but do so primarily through the lens of street and volume crime (eg Kazemian & Maruna 2009). Disengagement from organised crime is less well understood (Kleemans & de Poot 2008; Vere van Koppen et al. 2010).

Understanding how and why people seek to leave organised crime groups can potentially lead to the development of improved processes and interventions to support those who no longer wish to participate in serious criminal activities.

This chapter uses the term 'disengagement' to describe the process of rejecting a criminal lifestyle. This has been described as the process of separating, or changing behaviour, identity or performance. The process may be passive, in that the individual matures and adopts more prosocial norms, or an active rejection of the group. Disengagement is the process of undergoing personal change, leaving a group and formally transitioning from current member to ex-member (Gjelsvik & Bjørgo 2012; Sweeten, Pyrooz & Piquero 2013).

The lack of relevant research on disengagement from organised crime has been identified by several authors. Vere van Koppen et al. (2010) note that, while the basis for life-course and developmental criminology has advanced, there has been little exploration of these issues in connection with adult organised crime offenders.

Positive life events such as relationships, children and employment are known to strengthen social bonds and have been the focus of desistance research to date. Less work has been directed at considering adverse events associated with the conclusion of life states, such as divorce or the loss of employment, when associated with the onset of involvement in organised crime (Kleemans & de Poot 2008; Vere van Koppen & de Poot 2013).

While there is a substantial body of research on the nature of offences that constitute organised crime, organised crime frameworks and the damaging effects and significant costs of organised crime, there is a distinct lack of research on the reasons and processes by which individuals leave organised criminal activity. Although key criminological theories focus on street crime, and most work on desistance and disengagement concentrates on adolescent youth gang offenders, some of these findings are transferrable to organised crime.

Understanding membership of organised crime groups

Before we can understand the process of disengagement from organised crime, it is necessary to consider what membership of an organised crime group entails (see Smith 2014 for an examination of how individuals become members of organised crime groups). The concept of membership of organised crime groups is problematic, both theoretically and legislatively (Ayling 2011), because membership may be formal or informal. Formal membership may be conferred through a ritual process of pledging allegiance to a specific entity and agreeing to abide by the rules of that group. For example, OMCGs often have formal joining requirements, strict rules of behaviour, such as wearing identifying patches, and respect for a hierarchical structure of chapters (ACC 2013; Barker 2014). However, loose familial networks of offenders, such as those described by Amir (2011), may have no membership requirements other than adherence to a shared culture and relationship ties.

The network structure of many organised crime groups may mean that individuals only participate in some activities as temporary affiliates where their specialist knowledge is required; or they may participate in similar activities for a range of different groups (Morselli 2009). Individuals may not even consider that they are members of an organised crime group—for example, a truck driver and café owner who facilitated connections between his customers and his professional contacts (Vere van Koppen & de Poot 2013). Evidently, membership is not a clear status. If it is difficult to determine what membership really is, it is also difficult to determine what disassociation is and when it occurs.

Obstacles to leaving

The barriers encountered by those wanting to disengage from organised crime are varied. By its very nature, an organised crime group relies on trust, secrecy and the concealment of its operations and collaborations (Bovenkerk 2011). The departure of a member presents a risk that the group's expectation of loyalty and bonds of confidentiality may be broken, leading to the disclosure of information that puts the group in jeopardy (Bovenkerk 2011; Harris 2015). Disassociation may sometimes constitute such an act of betrayal that the group will seek to exact

violent retribution rather than let the member leave and breach the perceived code of honour and loyalty that binds the group (Harris 2015). Once a member has left the group, avenues of protection and security are also dissolved (Bovenkerk 2011; Harris 2015). Often, the fear and potential for reprisals can be enough to deter many members from seeking to leave the group.

Deviant groups exist outside the bounds of normal society and are often described as close-knit 'families' with strong bonds formed among members (Harris 2015). Leaving such a group means leaving the social relationships and severing close friendships, particularly if the group insists that departed members have no further contact (Harris 2015). Members have often invested years of their life in the group and, during this time, become isolated from the wider community and external interactions (Harris 2015). The stigma associated with having been a member of a criminal group can also disrupt, and prevent the formation of new, social ties, increasing the individual's isolation after disengagement and disassociation (Harris 2015; Wright 2006). Further, an ex-member's access to legitimate employment opportunities can be limited, providing few prosocial prospects for creating a new life and identity outside of the criminal group (Gjelsvik & Bjørgo 2012; Lindley 2016).

Leaving can also come at a cost. Individuals are typically lured into the organised crime lifestyle by the offer of money, excitement, status and power, which will typically cease when they leave (Bovenkerk 2011; Campbell & Hansen 2012). Their identity is based on their membership of a group and the social relations and dependence on the group that it brings. The loss of friendship and social ties with long-term associates, as well as the isolation from the community and lack of legal alternatives, can act to dissuade many individuals from leaving the group.

Motivations for leaving

The motivations for disengagement are complex and affect individuals and groups differently (Campbell & Hansen 2012; Harris 2015). The factors influencing disengagement are multiple, varied and interdependent and can best be considered through the use of a cost-benefit analysis. Research suggests that only when the predicted benefits of leaving outweigh the detriments of remaining in the group will members proceed with disengagement (Campbell & Hansen 2012; Gjelsvik & Bjørgo 2012; Harris 2015).

Harris (2015: 31–77) explains the trigger that instigates the disengagement process as a form of 'cognitive opening' that allows individuals to assess their self-identity against the group identity and act to resolve the disparity. Resolution in favour of the individual's values can decrease the level of group influence and therefore result in disassociation. While maturation is probably the most prominent factor in desistance and disengagement research, this primarily applies to younger, adolescent offenders (Laub & Sampson 2001). Despite this, maturation factors still have importance as an explanation for disengagement of the older cohort of organised crime offenders (Kleemans & de Poot 2008; Vere van Koppen & de Poot 2013).

Family and relationships are one of the strongest motivators for disengagement (Decker, Pyrooz & Moule 2014; Harris 2015). The presence of an intimate partner and children can exert pressure on the individual to choose between family obligations and their commitment to the group (Harris 2015). Where members of groups find themselves preferring a more conventional lifestyle, development of family life external to the group can also weaken group ties through

the strengthening of legitimate social and institutional ties (Disley et al. 2012). Gjelsvik and Bjørgo (2012) found that the presence of strong family pressures can encourage disengagement. Similarly, Campbell and Hansen (2012) note that disassociation may be needed to protect family members and members themselves from criminal threats.

The impact of violence on group members is also a strong predictor of disassociation (Disley et al. 2012; Harris 2015). Members who have been subject to threats or intimidation, or who know someone who has been violently victimised, report these incidents as a deterrent to continued membership of groups (Bolden 2013; Campbell & Hansen 2012; Pyrooz & Decker 2011). Similarly, attitudes towards the use of violence can change, causing individuals to reconsider their willingness to participate in violent acts (Harris 2015). This is demonstrated by reports of violent acts having 'gone too far' or not serving the appropriate purpose (Disley et al. 2012: 34; Harris 2015). Whether the violence is inflicted by enemies, fellow members or the individual in question, aggressive behaviour serves as a compelling reason for members to disassociate from criminal groups as they become increasingly aware of the risks arising from violent conduct.

Disillusionment is another theme of disengagement with several different facets. Disagreements about the group's leadership, objectives or actions can exacerbate internal conflict and lead to a negative view of the group (Bovenkerk 2011; Harris 2015; Pyrooz & Decker 2011). Further, if the group does not live up to individual expectations, or if members feel that they are making personal sacrifices that are not being met with equivalent benefits, the justifications for leaving may be present (Disley et al. 2012; Harris 2015). A change in role or status has also served to encourage disengagement from a group by reducing an individual's reputation and identification with other members (Campbell & Hansen 2012; Disley et al. 2012; Harris 2015). The psychological effect of disillusionment thus widens the 'cognitive opening' and generates increasing uncertainty about being a member of a deviant group. Even the stress and burnout associated with group membership can be an important factor in disillusionment (Disley et al. 2012; Harris 2015). In short, in making a decision to leave, individuals must weigh up the various detrimental factors that personally affect them against the benefits which their membership offers.

The process of leaving group membership

There is considerable evidence that it is difficult, if not almost impossible, to leave organised crime groups (Bovenkerk 2011; Brenneman 2014; Decker, Pyrooz & Moule 2014). The ways in which individuals go about disengaging from organised crime groups depend largely on the characteristics of the group (Gjelsvik & Bjørgo 2012; Harris 2015). Tightly controlled and socially closed groups such as OMCGs can resent members leaving and consider departure as abandonment of the group, requiring a hostile response (Harris 2015). However, research has also shown that much disengagement occurs in an easy and cordial manner, with members either negotiating departure or just drifting away from the group (Bolden 2013; Campbell & Hansen 2012; Harris 2015).

The precise methods used often depend on the position and role that the individual in question occupies within the group and their reasons for leaving. The more central and embedded the member, the less likely it is that they will be able to walk or drift away easily (Harris 2015; Pyrooz & Decker 2011). Peripheral members, however, who do not serve a key role in the group can often disengage through lessening their involvement and drifting away from the group over time (Gjelsvik & Bjørgo 2012). This type of covert departure can be more or less successful depending on the type of group. The latter types of disengaging members are less likely to be victims of repercussions—although, if a clean and affirmative break from the group is not made, doubts may remain about their membership status (Harris 2015). Harris (2015) provides an example of an OMCG member who attempted to distance himself by limiting social interactions and walking away from the group; however, the failure of this approach resulted in a public departure and denunciation from the group. Public departures can also be negotiated successfully (Bolden 2013). Campbell and Hansen (2012) offer the instance of a drug trafficker who left after reaching a consensus with his suppliers and who, despite initial fears, suffered no sanctions.

Despite this, a public departure can be confrontational, and some groups respond with violent retribution, threats and harassment or demands for the surrender of assets (Harris 2015). An abrupt departure, also known as 'knifing off' (Maruna & Roy 2007), is often achieved by severing all ties and leaving the area to avoid reprisals from the group. This is demonstrated in Brenneman's (2014) study of Central American gangs, where the penalty for desertion is death. While there are examples of lethal reprisals overseas, such as the 'morgue rule' in which those who leave an organised crime group must be murdered (Brenneman 2014), much of the discourse about 'blood in, blood out' is considered to be myth, perpetuated by groups to discourage disengagement (Bolden 2013: 474; Bovenkerk 2011; Harris 2015).

Organised crime entities operate under a veil of secrecy designed to avoid law enforcement attention and to ensure that their systematic operations can continue (Bovenkerk 2011; Harris 2015). The very nature of the group requires considerable trust and loyalty, and members often devote substantial resources to ensuring that those in the group can be trusted (Harris 2015, and see Smith 2014 on recruitment practices generally). Departing members can be viewed as traitors, and there is considerable risk that the group's secrets may no longer be safe.

Amir (2011) demonstrated that members of organised crime groups can disengage with few complications as they grow older. This is also supported by Harris (2015) and Bovenkerk (2011), who describe older members as having the option to retire or become honorary members. This type of disengagement appears to be less a determination to leave the ideology and behaviours and more about decreasing involvement in organised crime in accordance with ability and stamina.

Religious conversion associated with a change in personal ideology can also underlie the decision to disengage (Bolden 2013; Bovenkerk 2011; Gjelsvik & Bjørgo 2012). Brenneman (2014) discusses the role religion plays in recreating identity and reforming ex-gang members seeking to avoid almost certain death from criminal violence or social cleansing. Turning to God is considered to be transformative and allows ex-members to rebuild their character and adopt prosocial behaviours to contribute to society.

Problems following disengagement

Even after leaving organised crime groups, ex-members can encounter problems relating to their previous identity. If the process of disengagement and formation of a new identity is not publicly recognised, ongoing law enforcement action can be perceived as persecutory and oppressive (Decker, Pyrooz & Moule 2014; Harris 2015; Kazemian 2007). Members who leave deviant groups can also be subject to victimisation from rival criminal groups or enemies (Harris 2015). Evidence indicates, however, that victimisation does decrease after disassociation (Sweeten, Pyrooz & Piquero 2013). The community may also not distinguish ex-members from their previous status, thus creating barriers to forming friendships and restricting opportunities for reintegration, such as through employment and social acceptance (Brenneman 2014). The effect of this type of stigma can result in labelling and secondary deviance (Bolden 2012; Decker, Pyrooz & Moule 2014; Harris 2015).

Further, organised crime can prove to be a profitable business, and ex-members may not have access to legitimate income alternatives outside the group. Ex-members can find it difficult to find employment in the wider community because of a lack of education and transferrable skills (Brenneman 2014; Gjelsvik & Bjørgo 2012). Having lost most of their relationships as a result of their departure, ex-members can be isolated and face problems, including addiction and inability to lead a conventional lifestyle (Brenneman 2014; Harris 2015). Those members who retain ties with organised crime will potentially struggle to disengage successfully and to reconstruct their identity as an ex-member of a group, often falling back into group membership and activities (Bolden 2013; Decker, Pyrooz & Moule 2014; Harris 2015).

Promoting disengagement

Given the wide variety of types of organised crime groups, the different contexts and nuances of membership and personal involvement, and the cultural and social factors involved, promoting disengagement from organised crime is a complex challenge. In developing policy frameworks and intervention strategies, it is important to understand why and how members leave organised crime groups. Unfortunately, however, there is little research on the pathways that exist for members to disengage from organised crime. Literature on other deviant groups indicates that disassociation is largely influenced by the dynamics of the group and the characteristics of the individuals involved (Gjelsvik & Bjørgo 2012), which would indicate that disengagement strategies should be designed with specific organised crime groups and individuals in mind.

Creating disillusionment

A review of existing disassociation research indicates that there is potential to cause disruption to certain groups by inducing disillusionment factors, with the aim of weakening the group's foundation (Harris 2015). Strategies that can interrupt leadership and group efficacy can create internal conflict, thereby reducing embeddedness. Evidence also suggests that there are periods during which intervention is likely to be more successful—for example, after a violent or traumatic incident or when the group is failing (Bolden 2013; Disley et al. 2012; Harris 2015). Taking advantage of such factors that are known to trigger disengagement processes, such as violent confrontations, may provide opportunities to instigate strategies to reduce social ties within the group, and thus to motivate individuals to consider leaving.

Increasing risks

As it is known that the motivation to leave a criminal group is influenced by a process of weighing up the costs against the benefits, there is also capacity to increase the risks associated with group membership (Campbell & Hansen 2012; Gjelsvik & Bjørgo 2012; Harris 2015). Policies targeting unexplained wealth and asset confiscation have the potential to drastically affect individual members of organised crime groups. Existing law enforcement strategies, such as the regulation of certain businesses, new deportation legislation and anti-association powers, also show that controlling member relationships can hinder illegal activities (Ayling 2011; Willacy & McClymont 2015).

Disengagement programs

Existing research on leaving deviant groups indicates that the effectiveness of exit or disengagement programs has not been suitably evaluated; however, it appears that institutional interventions are not overly successful (Bovenkerk 2011; Decker, Pyrooz & Moule 2014). Informal and individual processes, including mentoring by ex-members, enhancement of family ties, education and employment programs, reintegration assistance, religious support and prosocial modelling appear to be more successful in supporting effective disengagement (Bolden 2012; Disley et al. 2012; Gjelsvik & Bjørgo 2012; Harris 2015). For example, Lindley (2016) noted that developing legitimate occupational opportunities would promote disengagement from maritime crime by Somali pirates. While the key to disrupting organised crime may be to disrupt the activities and organisation of the group, it seems that supporting and encouraging disengagement through the development of social capital and support for a new identity may be promising if managed in a holistic and community-minded manner.

An example of promising approaches to disengagement from participation in the activities of OMCGs is the public support offered in Scandinavian countries to facilitate those wishing to leave. Jahnsen (2018), for example, describes a number of 'exit' or 'defector' programs that promote collaboration between all levels of the public sector aimed at assisting disassociation. These programs offer traditional police protection for those who fear retaliation; other programs attempt to combine protection with assistance in breaking former social ties and

starting a new life. Assistance is offered in the form of housing and labour market integration programs, education, access to drug rehabilitation programs and different kinds of therapy. In Denmark, the authorities also offer economic support to individuals wishing to remove visible gang-related tattoos (Jahnsen 2018: 10). Similar programs are offered in the United States for former gang members aiming to make a break from their criminal past and remove tattoos signifying gang affiliations (Bakir Poljac & Burke 2008).

Conclusion

This chapter has examined the processes and risks associated with disengaging from involvement in organised criminal activities. Although prior research on the reasons and explanations for disengagement from conventional crime offer some assistance in understanding how disengagement occurs among members of organised crime groups, the parallels are not exact, particularly concerning the seriousness of organised criminality and the measures meted out to those who express a desire to leave group membership. Organised crime group members also demonstrate different traits and personal characteristics, compared with those who engage in less serious and less organised crime. Nonetheless, it is possible to draw parallels between these two types of criminals in terms of the ways they are recruited into criminality (Smith 2014) and the ways members disengage.

Further research on disassociation from organised crime, while potentially difficult to undertake, is necessary to determine the best way to promote disengagement. There is also a need to more fully explore adult-onset involvement in organised crime and the factors that contribute to adult desistance. This type of research will go some way to providing the information needed to assist in the disruption of organised crime groups through the implementation of improved desistance strategies and tools.

References

URLs correct as at February 2018

Amir M 2011. Age and aging in organized crime in Israel. *Crime Law and Social Change* 55: 311–19

Australian Crime Commission (ACC) 2013. *Outlaw motorcycle gangs.* https://www.crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/outlaw-motorcycle-gangs

Ayling J 2011. Pre-emptive strike: How Australia is tackling outlaw motorcycle gangs. *American Journal of Criminal Justice* 36(3): 250–64

Bakir Poljac MS & Burke T 2008. Erasing the past: Tattoo-removal programs for former gang members. *FBI Law Enforcement Bulletin* 77(8): 13–18

Barker T 2014. *Outlaw motorcycle gangs as organized crime groups*. New York: Springer International Publishing AG

Bolden C 2013. Tales from the hood: An emic perspective on gang joining and gang desistance. *Criminal Justice Review* 38(4): 473–90

Bovenkerk F 2011. On leaving criminal organizations. *Crime Law and Social Change* 55: 261–76

Brenneman R 2014. Wrestling the devil: Conversion and exit from Central American Gangs. *Latin American Research Review* 49: 112–28

Campbell H & Hansen T 2012. Getting out of the game: Desistance from drug trafficking. *International Journal of Drug Policy* 23(6): 481–87

Decker SH, Pyrooz DC & Moule RK 2014. Disengagement from gangs as role transitions. *Journal of Research on Adolescence* 24(2): 268–83

DeLisi M & Piquero AR 2011. New frontiers in criminal careers research, 2000–2011: A state-of-the-art review. *Journal of Criminal Justice* 39(4): 289–301

Disley E, Weed K, Reding A, Clutterback L & Warnes R 2012. *Individual disengagement from Al Qa'ida-influenced terrorist groups: A rapid evidence assessment to inform policy and practice in preventing terrorism*. RAND Technical Report. Santa Monica CA: RAND Corporation

Gjelsvik IM & Bjørgo T 2012. Ex-pirates in Somalia: Processes of engagement, disengagement, and reintegration. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 13(2): 94–114

Harris KJ 2015. *Leaving ideological social groups behind: A grounded theory of psychological disengagement (Doctoral thesis). Edith Cowan University, Perth, Australia*

Jahnsen SO 2018. Scandinavian approaches to outlaw motorcycle gangs. *Trends & issues in crime and criminal justice* no. 543. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi543

Kazemian L 2007. Desistance from crime: Theoretical, empirical, methodological and policy considerations. *Journal of Contemporary Criminal Justice* 23(5): 5–27

Kazemian L & Maruna S 2009. Desistance from crime, in *Handbook on crime and deviance*. New York: Springer: 277–95

Kleemans ER & de Poot CJ 2008. Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology* 5: 69–98

Laub JH & Sampson RJ 2001. Understanding desistance from crime. *Crime and Justice* 28: 1–69

Lindley J 2016. *Somali piracy: A criminological perspective*. Farnham: Ashgate Publishing

Maruna S & Roy K 2007. Amputation or reconstruction? Notes on the concept of 'knifing off' and desistance from crime. *Journal of Contemporary Criminal Justice* 23(1): 104–24

Morselli C 2009. *Inside criminal networks*. New York: Springer

Pyrooz DC & Decker SH 2011. Motives and methods for leaving the gang: Understanding the process of gang desistance. *Journal of Criminal Justice* 39: 417–425

Smith RG 2014. Responding to organised crime through intervention in recruitment pathways. *Trends and issues in crime and criminal justice* no. 473. Canberra: Australian Institute of Criminology

Sweeten G, Pyrooz DC & Piquero AR 2013. Disengaging from gangs and desistance from crime. *Justice Quarterly* 30(3): 469–500

Thompson C et al. 2014. Examining adult-onset offending: A case for adult cautioning. *Trends and issues in crime and criminal justice* no. 488. Canberra: Australian Institute of Criminology

Vere van Koppen M & de Poot CJ 2013. The truck driver who bought a café: Offenders on their involvement mechanisms for organized crime. *European Journal of Criminology* 10(1): 74–88

Vere van Koppen M, de Poot CJ, Kleemans ER & Nieuwbeerta P 2010. Criminal trajectories in organized crime. *British Journal of Criminology* 50: 102–23

Willacy M & McClymont A 2015. Rebels boss Alex Vella, stranded in Malta, speaks out over legal battle to return to Australia. Australian Broadcasting Corporation. 13 July. http://www.abc.net.au/news/2015-07-13/stranded-rebels-boss-in-court-battle-to-return-to-australia/6607356

Wright A 2006. The gang as a violent way of life, in Organised crime. London, Willan Publishing: 27–47

Part III: Exploring relationships between organised crime and other criminal activities

Chapter 8: Organised crime and terrorism nexus—implications for Australia: a research note

Rolando Ochoa

Organised crime syndicates, terrorist organisations and other such illegal groups pose a significant national security risk for Australia and the wider world (Hobsbawm 2007; Hoffman & Reinares 2014). This has been evidenced by the increasing number of threats and actual terrorist attacks in developed nations as well as the ever-growing networks of organised crime which operate throughout the world (Galeotti 2014). In developing nations, these groups and their members challenge state institutions and jeopardise successful democratic development. For developed nations, they pose a threat to the lives and livelihoods of their citizens at home and abroad and can harm development already achieved.

Traditionally, organised crime and non-state armed groups have been epistemologically separated, and their study has not often overlapped. Security and international relations experts have focused on the threat of terrorism (Hoffman 2003; Lebovic 2007; Kirshner 2013; Schoultz 2014), and sociologists, economists and criminologists have centred their effort on issues related to organised crime (Reuter 1983; Gambetta & Reuter 1995; MacCoun & Reuter 2001; Morselli 2005, 2009), with some exceptions (Makarenko 2004; Miraglia, Ochoa & Briscoe 2012; Shelley 2014). The emergence of new realities today—a globally connected economy, efficient transport of goods, a myriad technological advances in communications, and changing political environments—forces us to re-assess this separation in order to understand the interlinked dynamics of these groups.

The connections between terrorism and organised crime are yet to be fully understood, yet it is clear that they exist (Makarenko 2004) and will doubtlessly become more complex in the coming years. Crime–terror interactions have been the focus of analysis since the end of the cold war in the 1990s. This is exemplified in the work of Hoffman (1998), Sanderson (2004), Cornell (2005), Treverton (2009) and Arias (2006) at both the theoretical and the empirical levels. Today, strategic links between these types of groups have been singled out as a key factor in our understanding of them. The scale of the illicit market in drugs, arms and other

illegal goods and services makes a very rich backdrop for terrorist/insurgent organisations to operate in and to secure funding and other financial opportunities. This chapter addresses this issue by using comparative methodologies to dissect the internal governance of organised crime and other militant organisations, particularly as they impact the Australian security context. It seeks to uncover the mechanisms through which these organisations interact, merge or compete. This comparative study across groups provides for a rich and nuanced analysis through which better, more effective policymaking may be designed.

The crime–terror nexus has been a source of academic and policy debate for some time now. In fact, it is important to underscore the fact that insurgent organisations have regularly resorted to criminal activities to finance themselves. The Provisional IRA, for example, was well known for carrying out robberies (Naylor 1993). Sanderson (2004) has documented how Hezbollah is engaged in the production of methamphetamines in the United States to secure funding. Ochoa (forthcoming) argues this for the case of kidnapping in Mexico, where both left-wing armed groups and criminal organisations used kidnapping as a means to attain their political and pecuniary purposes. The end of the Cold War saw a changing international context, in which many non-governmental movements saw their income streams challenged, resulting in many politically oriented groups turning to crime to support their causes. The most common interpretation of the crime–terror nexus has been of a 'continuum' (Laqueur 2000: 173) with criminals on one end and terrorists/insurgents on the other. According to this view, these organisations would position themselves at different points along this continuum at different times and would eventually converge into what Makarenko (2004) referred to as a 'black hole' where these groups would sometimes fuse or be muddled together. This interpretation is based on a central understanding, namely, that organised crime has a monetary motivation—that is, they do not have any political allegiance—and that terrorist organisations are motivated by ideology. Hoffman (1998) argues that politically motivated organisations have an 'altruistic' motivation. This means that they are motivated into actions by the notion that they are fighting for a greater good or cause, or to deliver what they perceive as better conditions for a substantial number of people. In this sense, for example, ISIS members would believe that they are fighting to deliver a better, morally superior social structure. Since both types of groups require money to subsist, the argument goes, they will eventually converge and either cooperate or fuse.

The ultimate fusion of these two groups came about with the birth of the notion of 'narcoterrorism'. This expression was used for the first time to refer to Andean-region militant groups in Latin America who began to fund their activities through the growing of coca plants and the production and sale of cocaine. The most notorious of these 'narcoterrorist' groups is the Colombian FARC (Revolutionary Armed Forces of Colombia) who, since the 1980s and 1990s, used the cocaine trade as a source of income to fund their political activities (Treverton 2009). This notion became very politically useful, because it allowed governments to respond to these threats forcefully and to generate a certain discourse which inspired particular fears in the population. The recent uptick in discussions about the terror–crime nexus can be attributed to a number of factors; on the one hand, it has been argued that, as state-sponsored terrorism has declined, these organisations need to secure income from different sources (Grabosky &

Stohl 2010) and thus turn to other money-making activities. The post-9/11 world and the resulting strengthening of anti-terror laws and international cooperation in the matter (Sanderson 2004) have also had an impact on the development of crime–terror links, as funding for insurgent activities becomes more difficult to access. It is important to understand that the debates about these organisations have an important political component: they form around current political discourses, and the policy response to these groups is very much embedded in political expressions, such as drug prohibition. By definition, these discourses tend to simplify what is a very complex issue, and addressing these simplifications is part of the thrust of this proposal.

There are many ways in which terrorist organisations use crime as a way to achieve funding. The abovementioned examples of the Provisional IRA and Hezbollah are among well-documented cases. Pham (2011) found that Al-Qaeda is well positioned in the Maghreb region and is involved in kidnapping and the drug trade there. Thus, we see that criminal activity is central to the funding efforts of today's terrorist organisations. It is important to point out, however, that terrorist groups do not only engage in the sale of illegal commodities like drugs or illicit activities like kidnapping. Indeed, some evidence shows that this may even be counterproductive. Many communities frown upon the sale of drugs, for example. Thus, a militant group may be hesitant to engage in this activity lest they lose community support, a key ingredient in their success and longevity. Reputational considerations necessarily play a part in a group's decision to engage in criminal activities (Freeman 2011). Watts (2007) has found that insurgents in the Niger Delta have profited from stealing and selling oil taken from pipelines. Organised crime regularly engages in legitimate industries such as construction, as has been reported by Gambetta and Reuter as early as 1995. There is no reason to think that terrorist organisations may not have the same incentives. By the same token, criminal organisations use terrorism to further their interests. In 2008, drug trafficking cartels in Mexico's state of Michoacán threw grenades into a packed plaza during the country's independence celebrations, killing eight civilians and injuring hundreds. This was interpreted as a show of force from the cartels against the government's militarisation of the drug war (Ochoa forthcoming). The main argument here is that, eventually, these groups would go through a process of hybridisation or symbiosis where the group's identity would switch from one to the other. These explanations tend to focus on the groups themselves, as opposed to the activities which they carry out. There are, however, some who purpose a stronger focus on the activities of these groups and their relationships to other actors, that is, they propose a better contextualisation of the crime–terror nexus leading to deeper analysis.

Recently, Arias and Hussain (2016) argue that the common interpretations of the crime–terror link have obscured many important details of the relationship. They argue that they do not take into account the full complexity of their interactions and the nuances of their relationships to other actors, namely the state. They argue, along with Wardlaw (1988), that the politicisation of the debate over the crime–terror link has had the unintended consequence of obscuring the wealth of relationships and activities these groups engage in. Indeed, they argue that, in many cases, the state and/or state actors have regular contact with criminal and insurgent actors and that these relationships are as important as those between crime and terror. Arias himself

found this in the case of Brazil (2006). In this sense, therefore 'crime–terror interactions not only affect formal state structures but also impact different foci of power' (Arias & Hussain 2016: 381). They also argue that the roles of criminals and terrorists are not as clear-cut as the proponents of the hybridisation or continuum hypotheses ideate. In their view, criminals, the state and terrorists have many different social and political roles, which determine the characteristics of their interactions; in other words, they assume the importance and fluidity of political considerations by stating that criminals, terrorists and other actors will play a role in the interactions. In their own words:

> ...transnational crime networks, diaspora links, legitimate international trade, and the intervention of a range of foreign states and international non-state actors sustain both organised crime and terrorist violence (Arias & Hussain 2016: 381).

Possible hypotheses and research

Future research would do well to embrace Arias and Hussain's (2016) theoretical proposals and investigate the crime–terror connections by focusing on the complexity of their governance structures and their interaction with a host of other actors, especially with the state, producing more nuanced and deeper understandings of the phenomenon. This has clear implications for Australia. The provision of nuanced and innovative research into the crime–terror link in the Asia-Pacific region will provide policymakers with a better understanding of the problems and thus with an improved capacity to devise adequate policy responses. Three hypotheses for future testing are as follows:

H1: Organised crime and terrorist organisations have long-standing relationships, but these are not as have been usually described in the literature.

H2: These relationships are influenced by the presence and actions of other actors, such as the state and legitimate markets.

H3: The governance mechanisms of these groups allow them to interact and shape each other in different ways, namely, resource flows, strategic allegiances or opportunistic interactions.

Case study examples

Because of the sensitive nature of this issue, it is perhaps best suited for qualitative research. It goes without saying that, should data be available, they should be utilised as well. The following are only briefly considered examples. However, they may serve to illustrate many of the dynamics described above.

Mexico—criminals using terror

Mexican drug trafficking organisations are some of the most powerful organised crime groups in the world. Their presence is global and they control a significant amount of the drug trade in the Western hemisphere. Research on their contact with terrorist groups remains marginal. Research should examine whether, given the extent of their presence worldwide, they would be in a position to enter into relationships with terrorist organisations or engage in terrorism themselves. These groups have used terrorist tactics in their fight for control of drug trafficking, especially since 2006, when the government called in the armed forces to fight the cartels. An example of these tactics is the terrorist incident in Michoacán in 2008, noted above. That act was said to be in direct response to the government's security policies. It illustrates how organised crime groups have used terrorism as a way to achieve their goals. Researching the structure and governance of these groups and their relationships to other actors, as well as how this affects their ever-changing roles, is key to understanding of their modern day dynamics.

Philippines—terrorists committing crime

Since the 1990s, the terrorist organisation Abu Sayyaf (ASG) has been responsible for a number of large-scale attacks causing the deaths of hundreds of people. Their leadership has recently pledged allegiance to the Islamic State. Their stated objective is to establish an Islamic state in the Mindanao region of the Philippines. It is widely known that this group uses widespread kidnapping to secure funds. For example, in 2014, they threatened to kill a German hostage, demanding a ransom of US$5.6m. The German Government complied, and the hostages were released. The case of ASG can be used to illustrate under what circumstances a terrorist organisation will engage in organised crime and whether these groups have any sustained interaction with full-time organised crime (OC) groups. It can also explore the political considerations that have made the ASG one of the foremost examples of a terrorist organisation engaging in organised criminal activity.

Australia—dealing with the threat

In different ways, ASG and Mexican drug cartels present a challenge for Australian policymakers. Recent evidence, which has been corroborated by media outlets and conversations with law enforcement agents, points to the presence of Mexican OC groups in the Asia-Pacific region. Australia is a prime market for drugs, given its high profit margin, and is thus of interest to Mexican cartels. On the other hand, groups like ASG are a direct threat to Australian citizens and interests through kidnapping and monetary loss and also in their capacity to destabilise the political order in the Asia-Pacific region. Research in Australia should seek to establish how these two groups are perceived, tackled and dealt with and to evaluate whether the policies enacted today take into account the complexity of the terror–crime relationship as Arias and Hussain describe it.

Conclusion

Terrorism and organised crime pose a series of important challenges to Australian national security and public safety. Governments have signalled these phenomena as policy areas of priority in the past. While much has been written about the risks of collusion between organised crime and terrorist organisations, the truth is that we know precious little about these connections. While these organisations have traditionally been seen as epistemologically separate entities, new developments in academia and in the behaviours of these organisations have made clear the fact that it will be profitable to study their interactions deeply in the near future. This builds a bridge between criminology and security studies. It will also allow both academics and policymakers to assess the reality of the threat these groups pose. It is important to focus research not only on these groups, however, but also on their relationships to other actors, like the state and society in general, to generate a nuanced picture of their structures, contacts and networks.

As a regional leader, Australia is well placed to take on these research challenges, insofar as they affect its internal and external security. This is a difficult agenda, touching on many sensitive topics like radicalisation, drug trafficking and abuse, and with geopolitical considerations. However, the need for a better understanding of the links between OC and terrorist organisations in the Asia-Pacific region should prove a worthy incentive to support and carry out this agenda of research.

References

URLs correct as at April 2018

Arias ED 2006. *Drugs and democracy in Rio de Janeiro: Trafficking, social networks, and public security*. Chapel Hill NC: University of North Carolina Press

Arias ED & Hussain N 2016. Organized crime and terrorism, in LaFree G & Freilich JD (eds), *The handbook of the criminology of terrorism*. Hoboken NJ: Wiley Blackwell: 373–84

Cornell SE 2005. Narcotics, radicalism, and armed conflict in Central Asia: The Islamic movement of Uzbekistan. *Terrorism and Political Violence* 17(4): 619–39

Freeman M 2011. The sources of terrorist financing: Theory and typology. *Studies in Conflict and Terrorism* 34(6): 461–75

Galeotti M 2014. Global crime today: The changing face of organised crime. NY: Routledge

Gambetta D & Reuter P 1995. Conspiracy among the many: The mafia in legitimate industries, in Fiorentini G & Peltzman S (eds), *The economics of organised crime*. Cambridge: Cambridge University Press: 116–36

Grabosky P & Stohl M 2010. *Crime and terrorism*. London: Sage

Hobsbawm EJ 2007. *Globalisation, democracy & terrorism*. Little, Brown Book Group Limited

Hoffman B 2003. *The logic of suicide terrorism*. Washington: RAND

Hoffman B 1998. *Inside terrorism*. New York: Columbia University Press

Hoffman B & Reinares, F (eds) 2014. *The evolution of the global terrorist threat: From 9/11 to Osama Bin Laden's death*. NY: Columbia University Press

Kirshner J 2013. *Globalization and national security*. NY: Routledge

Laqueur W 2000. *The new terrorism: Fanaticism and the arms of mass destruction*. Oxford University Press on Demand

Lebovic JJH 2007. *Deterring international terrorism and rogue states: US national security policy after 9/11*. NY: Routledge

MacCoun RJ & Reuter, P 2001. *Drug war heresies: Learning from other vices, times, and places*. Cambridge University Press

Makarenko T 2004. The crime–terror continuum: Tracing the interplay between transnational organised crime and terrorism. *Global crime* 6(1): 129–45

Meadows LM & Morse JM 2001. Constructing evidence within the qualitative project, in Morese JM, Swanson J & Kuzel A (eds), *The nature of qualitative evidence*. London: Sage: 187–200

Miraglia P, Ochoa R & Briscoe I 2012. *Transnational organised crime and fragile states*. Paris: OECD Development Co-operation Working Papers (5)

Morselli C 2009. *Inside criminal networks*. NY: Springer

Morselli C 2005. *Contacts, opportunities, and criminal enterprise*. Toronto: University of Toronto Press

Naylor RT 1993. The insurgent economy: Black market operations of guerrilla organizations. *Crime, Law and Social Change* 20(1): 13–51

Ochoa R Forthcoming 2017. *Intimate crimes: Gangs, trust and kidnapping in Mexico*. Oxford University Press

Pham JP 2011. The dangerous 'pragmatism' of Al-Qaeda in the Islamic Maghreb. *Journal of the Middle East and Africa* 2: 15–29

Reuter P 1983. *Disorganised crime: The economics of the visible hand*. Cambridge, MA: MIT press

Sanderson TM 2004. Transnational terror and organised crime: Blurring the lines. *SAIS Review of International Affairs* 24(1): 49–61

Schoultz L 2014. *National Security and United States Policy toward Latin America*. NJ: Princeton University Press

Shelley LI 2014. *Dirty entanglements: Corruption, crime, and terrorism*. Cambridge University Press

Treverton GF 2009. *Film piracy, organised crime, and terrorism* (Vol. 742). RAND Corporation

Wardlaw G 1988. Linkages between the illegal drugs traffic and terrorism. *Journal of Conflict Studies* 8(3): 5–26

Watts M 2007. Petro-insurgency or criminal syndicate? Conflict and violence in the Niger Delta. *Review of African Political Economy* 114: 637–60

Chapter 9: Nexus between unreported and unregulated fishing and other organised maritime crimes

Jade Lindley

Illegal, unreported and unregulated (IUU) fishing is a global issue that requires a global solution. While recent responses have increased awareness among law and policymakers and consumers, there is still a lack of adequate control. In fact, the ongoing nature of IUU fishing facilitates other crimes, such as forced and low paid labour aboard IUU fishing vessels and trafficking fishers into IUU fishing. Lax border control and/or corruption of border officials shield and facilitate the continuation of IUU fishing in many locations. In order to control IUU fishing effectively, drivers enabling opportunity for criminals and barriers to crime control must be understood.

IUU fishing is made up of three separate concepts, defined in the United Nations Food and Agricultural Organization (FAO) International Plan of Action to Prevent, Deter and Eliminate Illegal, Unreported and Unregulated Fishing (IPOA-IUU), adopted in Rome in 2001 (Food and Agricultural Organization 2001). Illegal fishing involves offences contravening domestic and regional fishery management organisation (RFMO) laws; unreported fishing includes non-reporting, misreporting or under-reporting contrary to laws and RFMO measures; and unregulated fishing relates to activities which states have not regulated, as well as the activities of stateless vessels and non-parties to RFMOs (Food and Agriculture Organization 2001: paragraphs 3.1, 3.2 and 3.3). IUU fishing is a broad catch-all concept for a variety of (mostly) illicit fishing activities. It violates, or at least disregards, international, regional and local fishing laws and regulations in order to yield the greatest catch. Lack of awareness of relevant rules is inadequate justification for violation. Regardless of their ignorance, the illegal fishers' activities are condemnable.

Estimates reveal that over 85 percent of global fish stocks are at risk of IUU fishing, and approximately 25 percent of global fisheries are illegal, totalling global losses of close to US$23.5b per year (Ocean Unite 2016; World Wildlife Fund 2015). Beyond the financial loss,

the marine environments and fish stocks within it are at serious risk of endangerment and potential depletion. Further worsening the issue, evidence has emerged of the link between organised crime and illegal fisheries. The scale and organisation of these enterprises are staggering. Significantly, the IPOA-IUU does not address fisheries crime, and neither do most of the measures adopted by regional fisheries management organisations, bodies that operate mostly on the high seas to promote sustainable fisheries. IUU fishing alone is an issue warranting global concern, yet, when it is coupled with organised crime and environmental degradation, the need to effectively respond to the issue is magnified.

IUU fishing is enabled by a number of factors, in particular, corruption and lax regulatory enforcement at several points along the supply chain. Most commonly, IUU fishing is enabled by vessels flagged to open registries, using transhipping, or mixing illegal with legal catches at sea, using ports of convenience, and tax havens (Martini 2013: 3). Each of these methods intends to disregard or in some way evade controls in place to protect marine life, promote fair market share and provide the relevant state with its due revenues. This chapter critically explores the enablers leading to Indo-Pacific IUU fishing and other related crimes at sea, through a criminological lens.

Understanding the enablers of IUU fishing

Understanding the complex and many enablers of IUU fishing is essential to developing a suitable response. Criminals engage in IUU fishing for myriad reasons. Much like other crimes, reportedly greed, ease and profitability, as well as weak governance, poor monitoring and enforcement, contribute to IUU fishing, particularly within territorial waters (Phelps Bondaroff, Reitano & van der Werf 2015: 22). On the high seas, IUU fishing is facilitated by the vastness of the ocean and observance of the freedom of the high seas doctrine (Hardin 1968: 1244). These factors motivate and facilitate offending.

IUU fishing is commonly looked at from a solution-focused point of view by determining the most appropriate legal and regulatory framework to prevent offending. While this is a suitable approach for many crimes, it has not effectively deterred offending, and, therefore, an alternative approach may be more appropriate. Crime opportunity theory predicates that offenders seek out high gain, low-risk criminal opportunities in environments suitable for offending. Crime opportunity theory pioneer, Ronald Clarke, determined that:

> People without pre-existing dispositions [to crime] can be drawn into criminal behaviour by a proliferation of criminal opportunities, and generally law-abiding people can be drawn into committing specific forms of crime if they regularly encounter easy opportunities for these crimes, especially in their occupations (Clarke 2012: 66).

The absence of guardianship at sea and, therefore, the ability to yield additional catch without fear of sanction or infringement may encourage regular fishers to conduct IUU fishing, although the sophistication and organisation of IUU fishing indicates that the majority of offenders are not low-level opportunists.

High-level organisation of IUU fishing suggests that criminals engage in any and all activity in pursuit of maximum profit. Three types of IUU fishers exist: the habitual or repeat offenders; the opportunists; and the ignorant (Victorian Parliament Environment and Natural Resources Committee 2002: 244). While the majority of IUU fishers are organised criminals, some 'ignorant' or 'opportunist' IUU fishers unwittingly or occasionally disregard the law to yield a greater catch by taking advantage of absent regulation of the commercial fishing industry and poor law enforcement. Historically, particularly for ignorant or opportunist IUU fishers, when fish stocks were in abundance, illegal fishing was a low-risk, high-return activity. Even if they were caught, prosecution was unlikely, eliciting minor infringements compared with potential increased profits for selling illegally caught fish (Pew Charitable Trusts nd). It is most likely that 'habitual or repeat offenders' are also highly organised (Victorian Parliament Environment and Natural Resources Committee 2002: 243–5). Indeed, it is possible that some level of organisation exists within all three groups of IUU fishers. However, the habitual or repeat offenders cause the greatest harm because of the rampant nature of offending, requiring criminal organisation to sustain and financially support it.

Organised IUU fishers are more likely to target the vulnerable and most valuable species. In response, global quota restrictions and regulation were sought, to control IUU fishing because of declining fish stocks in many regions of the world. Worst affected by organised IUU fishers are local artisanal fishers and subsistence fishing communities deprived of their livelihoods and of an important food source (United Nations Office on Drugs and Crime 2011). Overfishing has caused entire fishing industries to collapse and has sparked extreme responses such as Somali piracy.

IUU fishing involves the disregard for existing laws, regulations, boundaries and marine life. As such, offenders may be drawn to operate under open registries or flags of convenience. Open registries are often based in developing countries seeking to gain market share of foreign investment by offering advantages for their shipping services. Advantages may include cheaper fees and less red tape than for a vessel registered to a developed country (Lindley 2015). Approximately 17 percent of open registry vessels lack real ownership information, allowing them to evade regulations and control and potentially engage in criminal activity (Phelps Bondaroff, Reitano & van der Werf 2015: 30). Collectively, open registries operate the greatest number of seafaring vessels (Central Intelligence Agency 2017). As such, they also have the most to lose by failing to comply. The grey or black list issued by the Paris Memorandum of Understanding on Port State Control—which publishes the operating standards of flags—identifies poor performers in meeting international operational standards (Paris Memorandum of Understanding on Port State Control 2017). Rather than open registries, it is probable that IUU fishing operates out of unregistered or phantom vessels—rebirthed from previously blacklisted vessels.

Unscrupulous owners benefit from the anonymity provided by the open registry (ITF Seafarers 2018). High fuel prices and decreasing catches, coupled with weak enforcement and few alternative employment opportunities, may enable otherwise legal fishers to engage in illicit activities out of desperation (Phelps Bondaroff, Reitano & van der Werf 2015: 62). Regardless of where the fishers sit within the hierarchy of the organisation, the lack of consequences, due to weak monitoring and enforcement, coupled with high profits, renders IUU fishing an appealing option for those who otherwise do not have employment or engage in even higher risk activities, such as piracy (Phelps Bondaroff, Reitano & van der Werf 2015: 24).

When apprehended, the vessels frequently abscond, switch flags and vessel identities and move on to other states undetected. Their products are caught in the waters of one state, landed in another state, often for processing, and are then exported to the market state. Highly nomadic fleets and the complex nature of truly global business models in fisheries sector supply chains make enforcement next to impossible without regional and trans-global cooperation (INTERPOL 2015: 3).

In recent years, despite an escalation in global awareness and effort to control IUU fishing, organised criminals have taken advantage of weak governance and absent law enforcement at port and sea borders. As such, it is evident that the efforts to control IUU fishing are ineffective.

Explaining IUU fishing links with organised crime

IUU fishing is a profitable, clandestine industry, with conditions that attract organised criminal syndicates. Illegal enterprise theory emphasises the similarities between illegal activities and legal activities (Kleemans 2014). IUU fishing occurs alongside legitimate fisheries but relies on its organised illegitimate activities to enhance profitability to facilitate further criminal offending. Using Illegal enterprise theory to explain IUU fishing and its links with other maritime-based crime broadens the regulatory scope necessary to respond most effectively.

As fisheries are a legal industry, separating illegal fishing operating within it can be challenging. Interception may include looking for anomalies, such as irregular behaviours inconsistent with legal fishing activities and relationships that support the entry of illegal catches onto the legitimate market. Illegal fishing is often a cover for other illicit activities, using the same routes, ports and corrupt border officials to evade interception. Research suggests that frozen, illegally caught fish may provide an effective cover for trafficking other contraband, including wildlife, weapons and drugs (Phelps Bondaroff, Reitano & van der Werf 2015: 62). Despite the UN General Assembly committee on fisheries management and conservation meeting semi-annually since 1991, they only articulated their concern about the link between IUU fishing and organised crime in 2008 (United Nations General Assembly 2008: paragraph 59). Specifically, the Assembly:

> Notes the concerns about possible connections between international organized crime and illegal fishing in certain regions of the world, and encourages States, including through the appropriate international forums and organizations, to study

> the causes and methods of and contributing factors to illegal fishing to increase knowledge and understanding of those possible connections, and to make the findings publicly available, bearing in mind the distinct legal regimes and remedies under international law applicable to illegal fishing and international organized crime (United Nations General Assembly 2008: paragraph 59).

Reiterated in subsequent resolutions, this directive:

> Calls upon States, in accordance with international law, to strengthen implementation of or, where they do not exist, adopt comprehensive monitoring, control and surveillance measures and compliance and enforcement schemes (United Nations General Assembly 2008: paragraph 60).

The aim was to enhance the response to IUU fishing and related crimes. It was endorsed by the UN General Assembly as an issue of great concern, so Member States are charged with the responsibility to act. While there are organised crimes that seek cover from detection by using fishing vessels, such as piracy, contraband trafficking (wildlife, weapons and drugs), and illegal migrant smuggling, other organised crimes facilitate IUU fishing, such as corruption at ports and fishing licence issuers and trafficking workers aboard vessels to conduct IUU fishing. These facilitator crimes are described below.

Trafficking in persons and forced labour aboard fishing vessels

Some fishers are unknowingly trafficked into the fishing industry. Whether at sea on vessels or on land in processing plants, the fishing industry is reported to be a hub for trafficked workers (United States Department of State 2016). In 2000, the UN General Assembly Convention against Transnational Crime was supplemented by a protocol dealing with trafficking in persons. Its definition of trafficking in persons can be summarised as the recruitment, movement or receipt of another person through threat, abduction, fraud, deception or abuse of power for the purpose of exploitation (United Nations 2000).

Organised criminals hide trafficked persons at sea, forcing them to work on the promise of freedom on repaying an incalculable debt. Funds generated from trafficked persons often facilitate large-scale drug hauls (David 2012). Men, women and children are moved within and across borders and, as part of the journey and/or at the end point, are exploited and abused. As well as being cheap labour, children are forced into work in the fishing industry all around the world because their 'small, nimble fingers are useful in releasing the fish from…smaller nets' (Techera & Lindley 2016; Johansen nd). In addition, vulnerable women are trafficked to 'service' the men on board vessels.

According to the International Labour Organization, forced labour involves coercion to work through violence or intimidation, accumulated debt, retention of identity papers or threats to inform immigration authorities (International Labour Organization 2014). Forced and unpaid labour is often found alongside IUU fishing, whereby fishers, generally migrants, willingly agree to work aboard the vessel; however, the conditions they are exposed to daily defy international labour and human rights standards. In the Asia-Pacific, forced labour in the fishing sector accounts for 53 percent of all forced labour in that region (Walk Free 2017: 53). Extensive global research provides countless examples of poor conditions (Walk Free 2017; Environmental Justice Foundation 2017). The 2016 Global Slavery Index noted the:

> abuse of migrant workers on fishing vessels, often young men and boys, who have endured brutal treatment including physical abuse, excessive and inhumane working hours, sleep and food deprivation, forced use of methamphetamines, and face being thrown overboard if they become ill or injured (David 2012).

Workers kept at sea for years at a time support Southeast Asia's $7b annual exports fishing trade (Htusan & Mason 2015). Using low or unpaid workers ensures that organised criminal leaders pocket greater profits.

Corruption and lax border and port control

Central to transnational organised crime is the facilitation of contraband entry across borders. IUU fishing requires corrupt officials to issue illegal licences, ignore catches beyond their licensed amount (legitimate or otherwise), allow fishing outside the agreed zones and defy national, regional and international laws and regulations. States with pre-existing high levels of border corruption, in particular, often have their territorial waters and exclusive economic zones exploited by IUU fishers. Limited law enforcement due to minimal governance further worsens the issue. Somalia provides an interesting example.

Case Study: Somali fisher-cum-pirates

Abandonment of government-issued fishing licences opened Somali waters to IUU fishing during the 1990s. Authorities issued some licences to foreign fishing companies, although after the collapse of the country in 1991, limited oversight of licences led to widespread IUU fishing. Somali warlords saw an opportunity to profit by selling false fishing licences to trawlers (United Nations Secretary-General 2011: paragraph 43). Warlords hired local fishermen to 'intimidate and extort money from foreign fishermen who were unwilling to purchase [licences]' (Advisory Council on International Affairs 2010: 14). The additional vessels fishing under false licences put further stress on the marine habitat. Adequate policing of these fishing practices was entirely absent (Advisory Council on International Affairs 2010: 14). Unsustainable fishing practices, worsened by the greed of the warlords, provoked fishermen to respond aggressively and pursue piracy.

Coastguards are an essential piece of the counter-IUU fishing response. When policing fails to detect and intercept IUU fishing activities at sea, it should be the role of port and border security to ensure that catches meet compliance requirements and are therefore suitable for market. Effective port regulation is essential, to prevent illegal catches from entering the market.

Illegal fishers evade effective port regulation before entering port, concealing their illegitimate catches through transhipment, mixing illegitimate with legitimate catches, making it virtually impossible to tell one from the other (Pew Charitable Trusts 2013; Phelps Bondaroff, Reitano & van der Werf, 2015: 24; Martini 2013: 3). Limited, ineffective and corrupt border control facilitates and potentially exacerbates IUU fishing.

Training enables stricter border control. The international community offers law enforcement training on how to detect and respond to potential crimes crossing the border (United Nations Office on Drugs and Crime 2018). Improving awareness through adequate training reduces the risk of corruption of port officials that allows illegal catches to enter the marketplace.

Conclusion

The chapter set out factors that enable IUU fishing and related maritime crimes, explained through crime opportunity and illegal enterprise theories. While legal and regulatory controls exist, alone these are insufficient in preventing IUU fishing and related crimes. Coupling controls and addressing the drivers enabling the crimes will reduce opportunity for offending. Further research is needed to better understand the most appropriate institutional configuration to lead to effective control of the marine environment, although some research has considered this (Lindley & Techera 2017). The use of emerging technology and further policing may also be critical to the success of IUU fishing control. A thorough understanding of drivers and implementation of regulatory controls should result in reduced opportunistic IUU fishing and related crimes.

References

URLs correct as at February 2018

Advisory Council on International Affairs 2010. *Combating piracy at sea: A reassessment of public and private responsibilities*. The Hague: Advisory Council on International Affairs. https://aiv-advies.nl/download/045f9ea5-c9f0-4bb6-a3c0-bc190e56dbaa.pdf

Central Intelligence Agency 2017. *Merchant Marine*. : Langley: Central Intelligence Agency. https://www.cia.gov/library/publications/the-world-factbook/rankorder/2108rank.html?countryName=AntiguaandBarbuda&countryCode=ac&regionCode=cam&rank=9#ac

Clarke RV 2012. Opportunity makes the thief. Really? And so what? *Crime Science: An Interdisciplinary Journal* 1(3): 1–9. https://doi.org/10.1186/2193-7680-1-3

David F 2012. Organised crime and trafficking in persons. *Trends & issues in crime and criminal justice* no. 436. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi436

Environmental Justice Foundation (EJF) 2017. *Seafood not slavefood*. London: EJF. http://ejfoundation.org/campaigns/oceans/item/seafood-not-slavefood

Food and Agricultural Organization of the United Nations (FAO) 2001. *International Plan of Action to prevent, deter and eliminate illegal, unreported and unregulated fishing (IPOA-IUU)*, adopted 23 June 2001 at the 120th Session of the FAO Council. Rome: FAO. http://www.fao.org/fishery/ipoa-iuu/en

Hardin G 1968. The Tragedy of the Commons. *Science* 162(3859): 1243–8. http://www.geo.mtu.edu/~asmayer/rural_sustain/governance/Hardin%201968.pdf

Htusan E & Mason M 2015. *More than 2,000 enslaved fishermen rescued in six months*. Associated Press, 17 September, accessed 29 January 2018. http://bigstory.ap.org/article/ceecf8df237e49bf8fe59d47fa3515b0/more-2000-enslaved-fishermen-rescued-6-months

International Criminal Police Organization (INTERPOL) 2015. *Second Environmental Compliance and Enforcement Events: INTERPOL Global Complex for Innovation, Singapore, 16 to 18 November: Agenda*. Lyon: INTERPOL. http://www.interpol.int/Media/Files/Crime-areas/Environmental-crime/Meetings/2nd-INTERPOL-Environmental-Compliance-and-Enforcement-Events/Agenda

International Labour Organization 2014. *The meanings of forced labour*, March. http://www.ilo.org/global/topics/forced-labour/news/WCMS_237569/lang--en/index.htm

International Transport Workers' Federation (ITF) Seafarers 2018. *Inside the Issues: Fisheries*. London: International Transport Workers' Federation, accessed 29 January 2018. http://www.itfseafarers.org/ITI-fisheries.cfm

Johansen R nd. *Child trafficking in Ghana*. Nairobi: United Nations Office on Drugs and Crime, accessed 29 January 2018. https://www.unodc.org/unodc/en/frontpage/child-trafficking-in-ghana.html

Kleemans ER 2014. Theoretical perspectives on organized crime, in Paoli L (ed), *Oxford handbook on organized crime*. Oxford: Oxford University Press: 32–52

Lindley J 2015. *Somali piracy: A criminological perspective*. London: Routledge

Lindley J & Techera EJ 2017. Overcoming complexity in illegal, unregulated and unreported fishing to achieve effective regulatory pluralism. *Marine Policy* 81: 71–9

Martini M 2013. *Illegal, unreported and unregulated fishing and corruption*. U4 Expert Answer no 392. U4 Anti-Corruption Resource Centre. Bergen: Transparency International. http://www.u4.no/publications/illegal-unreported-and-unregulated-fishing-and-corruption/

Ocean Unite 2016. *Ending IUU Fishing*. London: Virgin Unit, accessed 29 January 2018. http://www.oceanunite.org/issues/ending-iuu-fishing/

Paris Memorandum of Understanding on Port State Control 2017. *White, Grey and Black List, Secretariat Paris Memorandum of Understanding on Port State Control*. The Hague, accessed 29 January 2018. https://www.parismou.org/detentions-banning/white-grey-and-black-list

Pew Charitable Trusts 2013. *FAQ: Illegal, Unreported, and Unregulated Fishing, A brief from The Pew Charitable Trusts*, September. Philadelphia: The Pew Charitable Trusts. http://www.pewtrusts.org/~/media/legacy/uploadedfiles/peg/publications/fact_sheet/iuufaqwebpdf.pdf

Phelps Bondaroff TN, Reitano T & van der Werf W 2015. *The Illegal Fishing and Organized Crime Nexus*. Geneva: The Global Initiative Against Organized Crime and The Black Fish. http://theblackfish.org/Fishing_Crime.pdf

Techera EJ & Lindley J 2016. *Curtailing Maritime Crime: Countries should look at multinational approaches to regulating and limiting illegal fishing, trafficking, smuggling and other sea crimes*. Honolulu: Indo-Asia-Pacific Defense Forum, United States Coast Guard. http://apdf-magazine.com/curtailing-maritime-crime/

United Nations (UN) 2000. *Protocol to prevent, suppress and punish trafficking in persons, especially women and children, supplementing the United Nations convention against transnational organized crime.* Adopted by resolution A/RES/55/25 of 15 Novemberat the fifty-fifth session of the General Assembly of the United Nations. New York: UN. https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-12-a&chapter=18&lang=en

United States Department of State 2016. *Trafficking in Persons Report 2015*. Washington DC: United States Department of State. https://www.state.gov/documents/organization/245365.pdf

United Nations General Assembly (UNGA) 2008. *Sustainable fisheries, including through the 1995 Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks, and related instruments*. A/RES/63/112 (5 December). New York: UNGA. https://undocs.org/A/RES/63/112

United Nations Office on Drugs and Crime (UNODC) 2018. *Law Enforcement*. Nairobi: UNODC, accessed 30 January 2018. https://www.unodc.org/unodc/en/organized-crime/law-enforcement.html#Border_management

United Nations Office on Drugs and Crime (UNODC) 2011. *Transnational Organized Crime in the Fishing Industry: Focus on: Trafficking in Persons, Smuggling of Migrants, Illicit Drugs Trafficking*. Vienna: UNODC. http://www.unodc.org/documents/human-trafficking/Issue_Paper_-_TOC_in_the_Fishing_Industry.pdf

United Nations Secretary-General 2011. *Report of the Secretary-General on the Protection of Somali Natural Resources and Waters, S/2011/661* (25 October). New York: UN. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2011/661

Victorian Parliament Environment and Natural Resources Committee 2002. *Inquiry into fisheries management: Second report*. Melbourne: Parliament of Victoria. http://www.parliament.vic.gov.au/images/stories/Reports/VPARL1999-2002No166.pdf

Walk Free 2017. *Global Slavery Index 2016*. Perth: The Minderoo Foundation, accessed 30 January 2018. https://www.globalslaveryindex.org/download/

World Wildlife Fund (WWF) 2015. *Illegal Fishing: Which fish species are at highest risk from illegal and unreported fishing?* 29 October. Washington DC: WWF, accessed 30 January 2018. https://www.worldwildlife.org/publications/illegal-fishing-which-fish-species-are-at-highest-risk-from-illegal-and-unreported-fishing

Chapter 10: Criminal innovation and illicit global markets—transnational crime in Asia

Roderic Broadhurst

Spurred by the demand for the recreational use of 'ice' or amphetamine type stimulants (ATS, eg methamphetamines, ecstasy) and new psychoactive substances (NPS, eg synthetic opiates like fentanyl) as well as cocaine, traditional crime groups have revitalised. New entrepreneurial groups strategically capitalise on the opportunities created by these criminal markets, contributing to a surge in the profits from narcotics in Asia and worldwide (UN World Drug Report 2016).

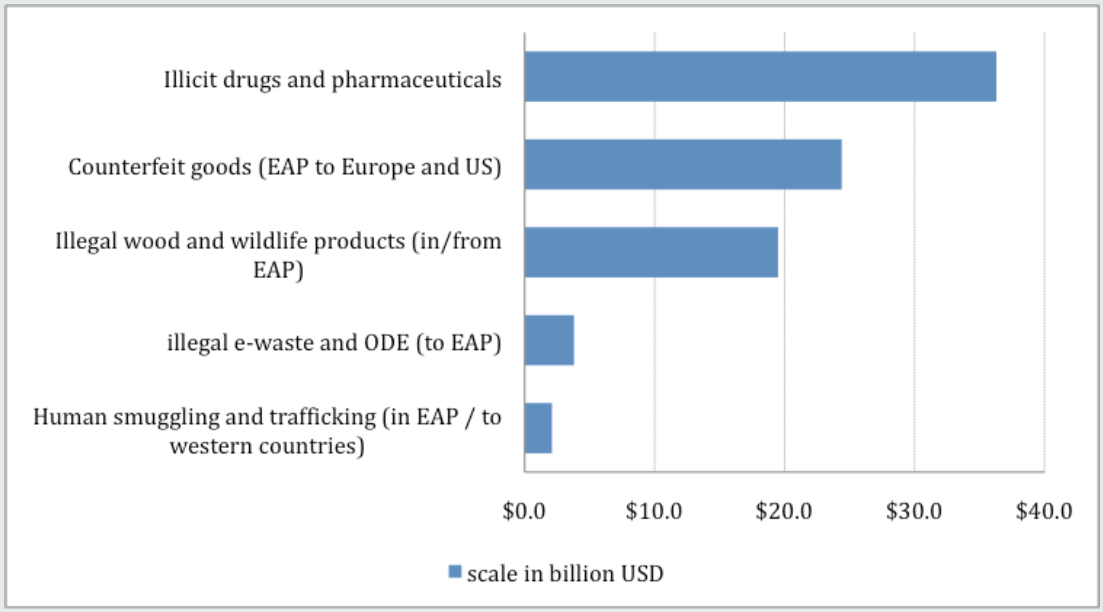
The scope, diversity and form of organised crime in Asia have been re-energised by the opening up and intensification of the region's economy and the development of new infrastructure. Illicit markets for counterfeit high street brands and pharmaceutical products or medicines, scarce timber and exotic wildlife trade are increasingly intertwined with the long established lucrative recreational drug and narcotic market. The organised armed groups that arise to protect these lucrative underground markets amass capital for their expansion and even to challenge or subvert state security (by corruption and fear) and undermine the traditional constitutional monopoly of violence and the protection of state revenue (Cockayne 2016; Broadhurst & Farrelly 2014; Broadhurst & Vy 2012).

In Asia and elsewhere, markets in cheaper synthetic narcotics not dependent on variable opium, cannabis or coca yields have developed, creating demand for the recreational use of methamphetamines ('ice'), other ATSs and NPSs, synthetic opiates and cocaine (O'Connor 2016). Asian crime entrepreneurs engage in an industrial-like global business, exporting precursor chemicals such as ephedrine, manufacturing illicit ATS or NPS drugs, and importing opiates from the Golden Triangle or Afghanistan and cocaine via Africa or directly from South America, often for re-export to the United States and valuable markets in Europe and Australia (Hamilton 2016; UNODC 2010, 2013).

Criminal markets

The illicit supply of narcotics attracts many crime groups and entrepreneurs and remains the single largest and most profitable criminal enterprise attracting venture capital and innovation. Out of the estimated US$90–100b per annum generated by crime flows in East Asia and the Pacific, illicit drugs, including fake medicines, account for over one-third of these profits (UNODC 2013).

Figure 1: Transnational organised crime flows in East Asia and the Pacific (EAP), 2012



Note: Illegal drugs include opiates and methamphetamines within EAP and fraudulent pharmaceuticals from EAP to SE Asia and Africa.
Source: UNODC, *Transnational Organised crime in East Asia and the Pacific: A threat assessment.* UNODC Regional Office for Southeast Asia and the Pacific, Bangkok, April 2013.

In Southeast Asia, drug-related criminal activities include the production and distribution of illegal drug and narcotic products (eg opiates, ATSs) and the trafficking of precursors (eg ephedrine). The mass manufacture of ATSs requires collusion at high levels of government with increasingly complex and diverse forms of organised crime. Fake or counterfeit medicines, particularly erectile dysfunction drugs and narcotic pain relievers, form a significant part of the market at around US$5b (UNODC 2016a).

However, the trade in illicit drugs is typically enmeshed with other criminal activities. In Southeast Asia, other criminal activities most likely to impact on economic growth, resource sustainability and governance include: counterfeiting of 'high street' goods; wood and wildlife products trafficking—illegal logging, exotic and protected trade, wild meat trade; illegal disposing of e-waste and prohibited chemicals; human trafficking and smuggling, including sex and labour trafficking (UNODC 2013, 2016a, 2016b; INTERPOL 2014).

The diversity of the Asian and global market for illicit drugs (and other illicit products) necessitates a variety of organisational strategies and criminal formation (from corporations or cartels through to gangs or single project 'entrepreneurs'). Substantial income is required to finance industrial scale production, supervise cell-networked distribution structures, protect revenues and gain political influence. It is debatable whether illicit drug markets underwrite or finance other illicit markets or whether it is the opposite. However, in Asia as elsewhere, the eclectic range of criminal 'services' on offer merges and overlaps with legitimate commerce. Grey business has flourished, and dual role entrepreneurs are able to navigate with impunity the nexus between the underworld and upper-world. Also crucial is the ability to move money and profits that require expensive financial and legal services and stable 'safe havens'.

Organised crime groups and activities

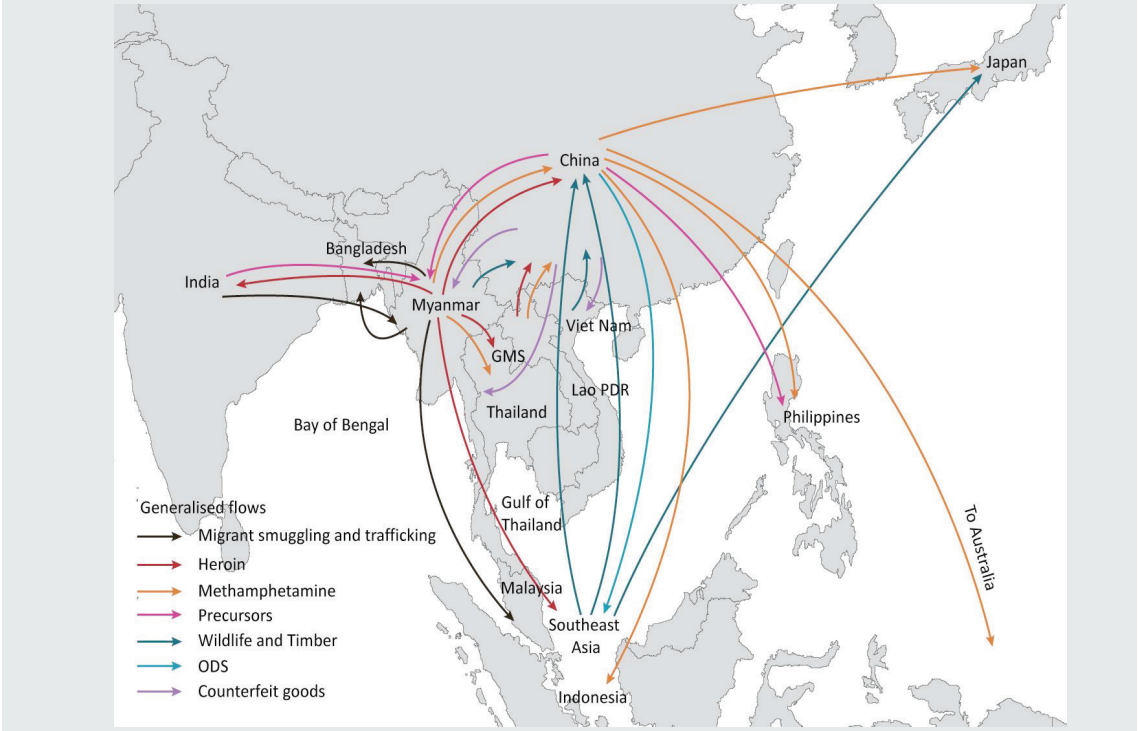
Organised crime groups in East and Southeast Asia are diverse and sometimes ephemeral. Traditional ethnic, language and place identities are no longer critical to safe and secure criminal transactions, and crime groups operate under looser and less hierarchical forms of command and control.

Chinese mafia 'black societies' are involved in illicit market activities, protection services, loansharking, 'money trail' avoidance services and stock market manipulation. Mainland-based groups engage in large scale ATS production and export, while Hong Kong and Taiwan groups finance large drug shipments in the role of lender and insurer. Japanese organised crime groups—yakuza—provide essential protection but are also active in illicit and 'grey' business in the entertainment and recreational drug markets in tourist destinations in the region and South America. Thai mafia, or jai pho, concentrate on the illicit drug trade but also engage in resource theft, small arms trading, human smuggling and trafficking and counterfeit products. Involved in both legitimate and criminal markets, they have ties with the Red Wa (Wa sub-state), élites, police and military. In Australia and New Zealand, Outlaw Motorcycle Gangs have links with Canadian, United States, Thailand, Indonesian and Scandinavian crime groups and operate as importers and financers of the illicit drug trade (summarised from Broadhurst, Gordon & McFarlane 2012; Broadhurst & Farrelly 2014).

The size and reach of the market in illicit drugs reflect patterns of globalisation, economic growth and armed conflict as well as government and civil society responses to the impacts of these markets. In Asia, these markets have grown rapidly, with the opening up of trade and development of China, India and the Association of Southeast Asian Nations (ASEAN) boosted by infrastructure development and increased wealth. The One Belt One Road, the India–Myanmar–Thailand Trilateral Highway and the Trans-Asia Railway Network (eg the Singapore–Kunming rail-link), along with new financial infrastructure (eg Asian Infrastructure and Investment Bank), are quickening the pace of change and development (UNODC 2016c; Broadhurst 2017).

Global flows of illicit drug trade

Figure 2: Generalised flows of criminal trade in the region



Note: ODS =ozone depleting substances
Source: UNODC 2016c: 19

Convergence and connectivity have been observed not only among different Asian crime groups, but increasingly with West African, Iranian, South American and Russian crime groups. These new groups and their associations, alliances or mergers illustrate the global reach of transnational crime. Regional illicit production and supply chains intermingle with the global trade in illicit goods and services. Mexican and South American crime cartels engage with Chinese and African crime groups to obtain and trade cheap precursor chemicals for the ATS market while supplying cocaine and other contraband. A lucrative cross-Pacific and global traffic therefore develops and, aided by Asian trade growth, more transnational crime opportunities emerge (Hutt 2016; Broadhurst 2017).

Myanmar continues to be Southeast Asia's major opium producer and the world's second largest, after Afghanistan. The 2015 Southeast Asia Opium Survey estimated that Myanmar and Lao PDR produced around 820 tons of opium per annum (UNODC 2015). Traditionally the hub of the opium and heroin trade, the Golden Triangle—a lawless borderland at the tri-state confluence of Burma, Lao and China—has turned to the mass production of ATSs, and a thriving cross-border smuggling business operates, drawing small and big crime entrepreneurs. The heroin and ATSs proceed from the Golden Triangle to neighbouring Yunnan China and then onwards—supplying consumers throughout East Asia, notably Japan, Korea and Taiwan. Small quantities of ATS 'ice' pills and high grade heroin produced in Northeast Myanmar are

transported to markets in Bangkok, earning for the successful smuggler up to US$2,000 per run (personal communication Royal Thai Police, November 2016). Larger amounts may be diverted via Cambodia for transshipment to highly profitable overseas markets like Australia, where premium wholesale prices beckon.

The Philippines, Indonesia and other nations in Southeast Asia rely on imported sources of precursor chemicals to produce ATSs for their domestic illicit market, or alternatively acquire ATS pills and opiates from producers in China, Afghanistan, the Golden Triangle and South Asia. In 2016, industrial scale 'ice' labs capable of producing 100kg of methamphetamine daily to supply Australia and Southeast Asian drug users were shut down in the Philippines, and Chinese and Filipinos were arrested (personal communication Philippines National Investigation Bureau, 18–19 March 2017). Similar labs involving African crime groups were discovered in Malaysia. Along with India, where pharmaceuticals are diverted from legitimate producers, China is the major supplier of ephedrine and pseudoephedrine, the main precursors in the manufacture of ATSs (Boykoff & Berlinger 2016).

Despite rapid expansion of 'ice' production in the Golden Triangle, it is estimated that 80 percent of the overall Chinese 'ice' market is produced locally by crime groups operating clandestine methamphetamine labs in Southern China. The size of seizures from underground laboratories suggests a large and profitable business: between January 2015 and December 2016, nearly 5 tons of solid and liquid methamphetamine, just under 3 tons of precursors and 1.5 tons of ketamine were uncovered (Makinen 2016). Chinese organised crime groups also supply foreign illicit drug markets far and wide, illustrating the impact of the globalisation of the illicit trade and the increasing wealth of China and the region (Broadhurst 2017).

Connections between Chinese and Mexican organised crime groups, such as the Sinaloa and Gulf cartels, have been reported, notably with Hong Kong's 14K and Sun Yee On supplying the Sinaloa cartel in Mexico with raw materials to produce crystal methamphetamine (Harris 2015). Police arrested Chinese, Taiwanese and New Zealand men after shipments of methamphetamine with a 'street' value of $AU950m were seized in 2016, along with over 6 tons of illicit drugs and precursors originating from Southern China (ABC News 2016).

Although opiates and ATSs are the predominant illicit drugs in Asia, cocaine imports have been discovered in Hong Kong, allegedly smuggled by a local syndicate specialising in transhipping illicit drugs from South America. Record seizures of 600 kg of ATSs smuggled via the Japanese port of Naha by Taiwanese nationals have also been reported. Illustrating the criminal utility of the direct transpacific sea route, in December 2016 and February 2017, three vessels seeking to deliver high-grade Columbian cocaine to Australian markets via Fiji and Tahiti were intercepted. The Melbourne crime syndicate behind the import is alleged to have had significant global relationships in Myanmar, Singapore, China and Japan (ABC News 2016).

Bloated with cash, organised crime groups, often enjoying a degree of state protection, constantly seek new markets, legitimate and illicit. By meshing with the rapidly evolving forms of connectivity and trade across the region and by mimicking best business practice underpinned by the strategic use of violence, these predatory groups can achieve impressive

access to power and threaten societies which have weak rule of law enforcement. Illicit drug markets are constantly evolving and adapting and therefore require effective global, regional and local responses to reduce supply and demand, while adjusting and initiating regulatory reform and improving treatment mitigation for offending drug users. For example, a recent UNODC assessment noted that ASEAN has not yet managed to create 'a fully operational framework on tackling cross-border crime…By contrast, there are already fully operational and thriving networks of cross-border criminals' (UNODC 2016a: 12).

The scale of the problem, illustrated by record breaking illicit drug seizures, has attracted a sense of urgency about the risks to governance and the region's capacities to disrupt the trade and prevent and reduce harms generated by transnational crime. Economic development has been prioritised by most Asian governments and has trumped concerns about illicit trade and organised crime. Asia has the world's fastest growing economies, but also extremes of inequality and destitution that generate crime and are often ineffectively mitigated by governments. Where competent criminal justice systems operate effectively against illicit markets, trafficking flows and organised crime move to other countries with weaker regulatory and law enforcement capabilities. Displacement also occurs in response to 'strike hard' deterrence policies such as the controversial Philippines 'war on drugs' (Sombatpoonsiri & Aries 2016). Thus, policing organised crime has moved beyond purely localised national responses as it becomes increasingly evident that transnational organised crime groups operate in multi-dimensional globalised illicit markets. The current view of the morphology of organised crime is that loose, project driven networks of actors are involved in a range of illicit activities, and this is driven by the profitable opportunities offered by criminal markets. Thus, strategies aimed at attacking crime groups, such as criminal association laws or other measures to disrupt the trade such as 'war on drugs' campaigns, will not impact broadly on illicit markets unless the markets themselves are regulated (Broadhurst 2017). A handful of capable law enforcement agencies, a patchwork of cross-border mutual legal assistance agreements and a fledging but fragile regional security response from ASEAN, APEC and other multilateral forums are trying to address these challenges (ASEAN 2010).

Eroding the power of organised crime

The 2003 UN Convention on Transnational Organised Crime (UNTOC), signed by most Asian countries, provides a common platform for cross-border cooperation against organised crime and illicit markets. Cross-border cooperation and bilateral mutual legal assistance have developed accordingly; in addition, nascent ASEAN institutionalisation of policing and coordination of customs and immigration provide a framework for improved regulatory responses to criminal markets and organisations. Yet, regional integration and law enforcement capability remain limited, and the lack of effective action to suppress illegal drugs reflects ASEAN's relatively weak integration regarding the common non-traditional security problems (Broadhurst 2017).

Strengthening the monitoring and regulatory control over precursor chemicals should help to reduce the impact of the rise of potent new synthetic opiates. The pharmaceutical industries in India and China are substantial producers supplying traditional domestic medicine markets and are poorly monitored industries. Coordinated action on the suppression of the export of precursor chemicals across the region is essential and could have a significant impact on supply. Improved regulatory and export tracking controls of these precursors are urgently required (O'Connor 2017).

Over the past 50 years, countermeasures at the regional and national level have focused on the disruption of supply and distribution, increased expenditure on law enforcement and ramping up deterrence measures; yet, little sustained reduction has been achieved, and alternative 'harm reduction' approaches, including treatment and decriminalisation and innovative strategies to reduce the demand side, have not developed swiftly.

The Australian Government invests in overseas prevention activities and provides expertise to ensure that law enforcement agencies' cooperation between Australia and its neighbours brings mutual benefits and provides some bulwark against the predatory conduct of criminal groups. Reducing the harm of black markets in contraband invites a reassessment of the policies that fuel unproductive 'drug wars' towards a focus on public health and civil society treatment measures (Amnesty International 2017). Such measures include, in some jurisdictions, the recent legalisation of medical or recreational marijuana; this, in turn, has been associated with a decline in hospitalisation for opiate overdose (Shi 2017; RAND 2018, Powell, Liccardo & Jacobson 2018). Alternative policies to tackle the harms of criminal markets seek the regulation of recreational drugs. The pursuit of the 'lesser evil' of harm reduction would also help to undercut the profits of criminal groups.

References

URLs correct as at February 2018

ABC News 2016. Eight people arrested after $54-million drug seizure off Australian coast, 17 November. http://www.abc.net.au/news/2016-11-17/eight-arrested-over-drug-seizure/8035376

Amnesty International 2017. *If you are poor, you are killed: Extrajudicial executions in the Philippines' 'war on drugs'*. London. http://www.amnestymedia.org/story.asp?ID=MBTFN&uID=109a519.8b168155u94255sd7.95

ASEAN 2010. *ASEAN plan of action to combat transnational crime*. Retrieved from: http://www.aseansec.org/documents/DocSeriesOnTC.pdf

Boykoff P & Berlinger J 2016. *$120 million worth of meth seized in record-breaking Philippines' drug raid*. 28 December. http://edition.cnn.com/2016/12/28/asia/drug-raid-philippines/

Broadhurst R 2017. Transcontinental express: Asia's law enforcers face synthetic drug proliferation. *Jane's Intelligence Review* August: 42–5

Broadhurst R & Farrelly F 2014. Organised crime 'control' in Asia: Examples from India, China and the Golden Triangle, in Paoli l (ed), *Oxford handbook of organised crime*. Oxford: OUP: 634–54

Broadhurst R, Gordon AS & McFarlane AJ 2012. Transnational and organised crime in the Indo-Asia Pacific, in *Routledge handbook of transnational organised crime*. London: Routledge, Taylor & Francis Group: 143–56

Broadhurst R & Vy KL 2013. Transnational Crime in East and Southeast Asia, in Tan ATH (ed), *East and South-East Asia: International relations and security perspectives*. London: Routledge: 223–35Cockayne J 2016. *Hidden power: The strategic logic of organised crime*. Oxford University Press

Hamilton K 2016. The golden age of drug trafficking: How meth, cocaine, and heroin move around the world. https://news.vice.com/article/drug-trafficking-meth-cocaine-heroin-global-drug-smuggling, Vice News, news.vice.com, April 26

Harris B 2015. *A hotspot for Ice: How Mexican drug cartels have infiltrated Hong Kong*. 15 April. http://www.scmp.com/news/hong-kong/article/1759760/how-mexican-drug-cartels-are-moving-hong-kong

Hutt D 2016. *Mexico's feared drug cartels are infiltrating the region*. 7 April. http://sea-globe.com/mexican-drug-cartels-southeast-asia/

INTERPOL 2014. *Pharmaceutical crime and organised criminal groups: An analysis of the involvement of organised criminal groups in pharmaceutical crime since 2008*. https://www.interpol.int/Crime-areas/Pharmaceutical-crime

Makinen J 2016. *Drug seizures soar in China; most suspects are 'farmers and unemployed'.* 16 February. http://www.latimes.com/world/asia/la-fg-drugs-china-meth-ice-20160218-story.html

O'Connor S 2016. Meth precursor chemicals from China: Implications for the United States. US-China Economics and Security Review Commission, Policy Analyst, Economics and Trade, July 18. www.uscc.gov/Research/meth-precursor-chemicals-china-implications-united-states

Powell DR, Liccardo P & Jacobson, M 2018. Do medical marijuana laws reduce addictions and deaths related to pain killers? *Journal of Health Economics* 58: 29–42

RAND Corporation 2018. Study questions link between medical marijuana and fewer opioid deaths: Association appears to be changing as medical marijuana laws and opioid epidemic change. *ScienceDaily* February. <www.sciencedaily.com/releases/2018/02/180207090111.htm>

Shi Y 2017. Medical marijuana policies and hospitalizations related to marijuana and opioid pain reliever. *Drug Alcohol Dependency*. doi: 10.1016/j.drugalcdep.2017.01.006. Epub 2017 Feb 21

Sombatpoonsiri J & Aries A 2016. *Duterte's war on drugs: Bitter lessons from Thailand's failed campaign*. 26 September. http://theconversation.com/dutertes-war-on-drugs-bitter-lessons-from-thailands-failed-campaign-66096

UNODC 2016a. *Protecting peace and prosperity in Southeast Asia: synchronizing economic and security agendas*. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific. https://www.unodc.org/southeastasiaandpacific/en/2016/02/...southeast-asia/story.html

UNODC 2016b. *Transnational Organised Crime in East Asia in the Pacific: A threat assessment*. The Pacific Island Forum Secretariat, Regional Office for Southeast Asia and the Pacific. http://www.unodc.org/southeastasiaandpacific

UNODC 2016c. *World Drug Report 2015*. United Nations publication, Sales No. E.15.XI.6

UNODC 2015. *Southeast Asia Opium Survey 2015, Lao PDR, Myanmar*. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific.

UNODC 2013. *Transnational organised crime in East Asia and the Pacific: A threat assessment*. Bangkok: UNODC Regional Office for Southeast Asia and the Pacific. http://www.unodc.org/toc/en/reports/TOCTA-EA-Pacific.html

UNODC 2010. *The globalization of crime: A transnational organised crime threat assessment*. https://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html

Chapter 11: The international darknet drugs trade—a regional analysis of cryptomarkets

James Martin, Jack Cunliffe, David Décary-Hétu and Judith Aldridge

This chapter presents a descriptive analysis of illicit drug trading conducted via cryptomarkets, 'eBay' style marketplaces operating on the darknet (Martin 2014a, 2014b). Over the past seven years, cryptomarkets have emerged as a significant new vector for the retail and delivery of illicit drugs. One of the least understood aspects of cryptomarket-facilitated drug trading concerns the location of vendors who use the darknet to trade illicit drugs across national borders. While previous quantitative papers in this area have noted the locations of vendors selling drugs on cryptomarkets (eg Christin 2013; Soska & Christin 2015), these previous studies have not differentiated between vendors who are prepared to sell drugs to international or domestic-only clientele. The aim of this research is to fill this gap in knowledge and determine which countries are the most active, in terms of both domestic-only and internationally oriented drug vendors, as well as which countries dominate the trade in particular drugs, specifically cannabis, ecstasy-type products, cocaine, methamphetamine and opioids.

Methods

This chapter is based on data collected using the DATACRYPTO tool (Aldridge & Décary-Hétu 2015) in January 2016. DATACRYPTO is a web-crawler that accesses online cryptomarkets and systematically downloads the HTML page contents before processing this data into a cleaned and analysable format. Eight of the largest markets that were in operation at the time were included in the analysis: Alphabay, Crypto Market, Darknet Heroes League, Dream Market, French Dark Net, Hansa Market, Nucleus and Python Market. The cleaning stage of the data processing separated the data into product listings—including drug type, package quantity and customer feedback on each product with their rating—and vendor level information, including the stated country of origin of the product and the destinations to which the vendor was willing to sell.

This dataset was previously used by Cunliffe et al. (2017), and many of the technical details of the data cleaning process are presented in greater detail in that paper. It is important, however, to reiterate or clarify some points. An important point to reiterate is that this work only focuses on 'active' products and vendors, that is, products/vendors who have made a sale in the previous 30 days. This is an established way of classifying the rate of sales of products on cryptomarkets (Aldridge & Décary-Hétu 2014; Christin 2013; Kruithof et al. 2016) and works on the assumption that feedback is regularly given on these markets, although it is also accepted that this is likely to underestimate true activity rates.

The Cunliffe et al. (2017) paper focuses on Australia, and therefore, in that paper, an extra level of data cleaning was implemented to capture the specifics of the shipping route descriptions outlined in the detailed vendor and product text fields. With over 60,000 products and over 2,000 vendor descriptions requiring manual inspection of each field, attempting to do this for the broader geographical application within this chapter would have been inefficient. The origins and possible destination countries are therefore taken directly from the main reported fields of the data collection process. The impact of this is expected to be minimal, with Cunliffe et al. (2017) finding that less than two percent of products had contradictory information regarding the headline shipping location and whether the vendor was unwilling to send to Australia.

To aid presentation and to keep this report to a manageable size, this work only contains detailed information on the seven most frequently listed origin countries (as detailed in Figure 1), which account for over 90 percent of the total number of transactions identified worldwide. Five broad drug types are considered: cannabis, ecstasy-type products, cocaine, methamphetamine and opioids. Details of individual products that make up these categories appear in Table 1.

Table 1: Drug categorisations

Drug Category	Drug types included in the category (in decreasing order of frequency within group)
Cannabis	Hash, herbal cannabis, extracts (these cover 85.6% of the group), seeds, synthetic cannabinoid, edibles and drinkable, cannabis products NEC
Ecstasy-type	MDMA (ecstasy) pills, MDMA powder, Mephedrone powder, MDMA capsules, MDA powder (covering 93.3% of group), other ecstasy-type drugs
Cocaines	Cocaine (covering 94.3%), crack cocaine, cocaine/coca seeds, coca leaf, cocaine paste
Methamphetamines	Methamphetamine (not tablet)
Opioids	Heroin (covering 88.5% of the grouping), opium, other opioids

Destinations are split into whether the product was listed as being available only to domestic customers, within their continent (the vast majority being Europe, North America or Oceania) or some large portion of that continent (such as Western Europe), or whether the listing states that it is available to customers worldwide (referred to here as international). In the product specific analysis of Figure 2, products available across any international boundaries (even if within a continent) are combined to allow succinct presentation.

The majority of the analysis presented here is descriptive, looking at the number of vendors or sales by various splits within the data. The exceptions are the price comparisons presented in Table 2. These are calculated using a Poisson regression with robust standard errors (Silva & Tenreyro 2006) controlling for the listed destination, the product weight/the package size (and their square to account for non-linear changes in the pricing as quantities get higher) and the specific drug category of each listing. The base comparator is usually the United Kingdom (UK), the largest European source country for most drug categories except for methamphetamine, where the base is taken to the United States (the UK has only 14 listings for this product).

Results and discussion

Figure 1 displays the total number of unique cryptomarket vendors identified during the period of data collection, as well as the number of transactions they conducted as proxied by the customer feedback that they received. We identified a total of 1,838 unique cryptomarket vendors operating worldwide, with the vast majority of these located in the Anglosphere and Western Europe. The largest number of online vendors is located in the United States (644), followed by the UK (265), Germany (163), the Netherlands (152), Australia (150), Canada (97) and France (49).

Numbers of sales were correlated to the number of dealers operating in each country, with the order of countries in which transactions took place the same as the order of the countries in which the greatest number of vendors are located. The total number of transactions identified worldwide was 92,527, with US based vendors conducting 29,994 transactions, followed by vendors located in the UK (21,386), Germany (11,782), the Netherlands (9,154), Australia (6,274), Canada (3,242) and France (2,273). Vendors located in 'other' countries conducted a total of 8,422 transactions.

Figure 1: Vendors and sales by country of origin and shipping destination, active products only (number of vendors/number of products in brackets)

With the world's largest economy (IMF 2017) and a population of approximately 320 million (UN 2017), the United States was, unsurprisingly, revealed as the country with the largest number of cryptomarket vendors conducting the greatest number of transactions. However, when the number of cryptomarket vendors was measured against national population sizes, a more intriguing picture emerges. The Netherlands was home to the highest number of vendors per capita, with 0.9 vendors per 100,000 of the national population. Australia had the second highest number of cryptomarket vendors per capita (0.65), followed by the UK (0.41), Canada (0.28), Germany (0.2), the United States (0.2) and France (0.07). These numbers indicate that the adoption of cryptomarket technology by drug vendors varies significantly from country to country.

Figure 1 also displays a breakdown of the potential destinations to which vendors located in each country are prepared to send drug consignments. Here we also identify significant divergences between the different source countries. Vendors based in the United States and Australia were those most likely to restrict sales to domestic-only destinations, with 83 percent of Australian vendors and 65 percent of US-based vendors only selling products within their respective countries. European-based vendors were those most likely to list their products for sale internationally, either within the continent or to other destinations worldwide.

One hundred percent of vendors located in the Netherlands sold products internationally, followed by French vendors (90%), German vendors (53%) and UK vendors (51%). Ninety-two percent of Canadian-based vendors were prepared to send drugs internationally, presumably to access the US market.

Cunliffe et al. (2017) explain the very high proportion of domestic-only sales by Australian vendors—which they term the 'island effect'—as a likely product of the relative geographic isolation of the country, with long postal delivery times from Australia to other international destinations acting as a significant disincentive for potential overseas customers. The relatively high price of drugs sold by Australian vendors also makes sales by Australian vendors significantly less attractive, compared to their international competitors. We hypothesise similar reasons for the high proportion of domestic-only sales by US-based vendors—drugs sold by US vendors are relatively highly priced (see pricing discussion below), and the United States is geographically isolated from customer markets in Europe. We also speculate that the size of the US online drugs market further disincentivises US-based vendors from making overseas sales, because vendors located within the United States can still maintain large numbers of transactions without incurring the additional risks associated with international postal deliveries, which involve a greater risk of identification by border protection and law enforcement agencies (Décary-Hétu, Paquet-Clouston & Aldridge 2016).

By contrast, European-based vendors tend to be prepared to send their drugs internationally in much higher numbers. We speculate that this is partly a result of the Schengen shared customs zone, in which mail may pass between European Union member states with more minimal border controls than would otherwise be the case for typical international shipments. The result of this is that the European darknet drugs market appears to be significantly more integrated than in other parts of the world, with a flow-on effect in terms of competition and drug pricing (see pricing section below).

Figure 2 represents the proportion of drug transactions conducted via cryptomarkets, divided according to country of origin. The 'all destinations' category includes sales that are available to domestic, intracontinental and worldwide destinations. The 'international/continental' category excludes domestic-only sales, focusing specifically on transactions by vendors who are prepared to send drugs internationally. When considering all drugs available for sale both domestically and internationally, the data reveal that US-based vendors conduct 32 percent of global cryptomarket drug transactions, followed by the UK (23%), Germany (13%), the Netherlands (10%), Australia (7%) and France (2%). When focusing specifically on international cryptomarket drug transactions, however, a significantly different picture emerges. The UK is revealed as home to the most prolific international cryptomarket drug vendors, accounting for 30 percent of international transactions, followed by Germany (19%), the Netherlands (17%), the US (11%), Canada (6%), France (4%) and Australia (1%).

Cannabis

By drug category, US-based vendors accounted for the greatest proportion of global darknet cannabis transactions (ie international cannabis transactions plus domestic transactions, 36%), followed by the UK (25%), Germany (15%) and Canada (7%). Given its long-standing association with (de facto) cannabis decriminalisation, the Netherlands surprisingly accounts for relatively few international darknet cannabis transactions (5%). France sits equally with the Netherlands, also accounting for 5 percent of international darknet cannabis transactions.

Ecstasy

The Netherlands is home to the most prolific darknet ecstasy traders, accounting for 28 percent of global transactions, followed by the UK (21%), US (17%), Germany (15%), Australia (9%), Canada (3%) and France (1%). The international darknet ecstasy trade is even more comprehensively dominated by the Netherlands, where vendors account for 42 percent of international ecstasy transactions, perhaps an unsurprising finding considering the Netherlands' reputation as a global centre of ecstasy production (AIC 2015; Spapens 2014). The UK and Germany each account for a further 20 percent of international ecstasy transactions, while non-European countries account for a very low proportion of transactions—Canada (5%), US (3%) and Australia (1%).

Cocaine

Vendors located in the UK account for the greatest proportion of global darknet cocaine transactions (37%), followed by the US (23%), the Netherlands (15%), Germany (9%) and Australia (4%). As with ecstasy and cannabis, the international darknet cocaine trade is dominated by European vendors, particularly those located in the UK, who account for nearly half (45%) of the world's international darknet cocaine transactions. This is followed by vendors located in the Netherlands (21%), Germany (10%), France (4%) and Canada (3%).

Methamphetamine

The US accounts for nearly half (47%) of global darknet methamphetamine transactions, followed by Australia at 27 percent. European-based vendors account for a relatively low proportion of methamphetamine transactions, with only 8 percent of transactions originating from vendors based in the UK, 6 percent in Germany and 4 percent in the Netherlands. The relatively low proportion of methamphetamine transactions by European vendors probably reflects the relative unpopularity of the drug, compared to popularity in the United States and Australia (Degenhardt et al. 2016; EMCDDA 2014). Similarly, the international darknet methamphetamine trade is also dominated by the United States, which accounts for 36 percent of international methamphetamine transactions, followed by Germany (16%), the UK (11%), the Netherlands (10%), Canada (9%) and Australia (6%).

Opioids

As with cannabis and methamphetamine, US-based vendors comprise the largest single source of the darknet opioid trade, accounting for 36 percent of global opioid transactions. This is followed by vendors located in the UK (16%), France (14%), Germany (12%), the Netherlands (9%) and Australia (9%). Intriguingly, vendors based in France comprise the largest single source of international opioids, with nearly a quarter (23%) of international transactions originating there. The remainder of the international darknet opioid trade is relatively evenly split between vendors based in Germany (18%), the US (18%), the UK (15%) and the Netherlands (14%). Just two percent of international darknet opioid transactions originate from Canada.

Figure 2: Percentage of sales by country of origin, all destinations and international/continental, and by drug type, active products only

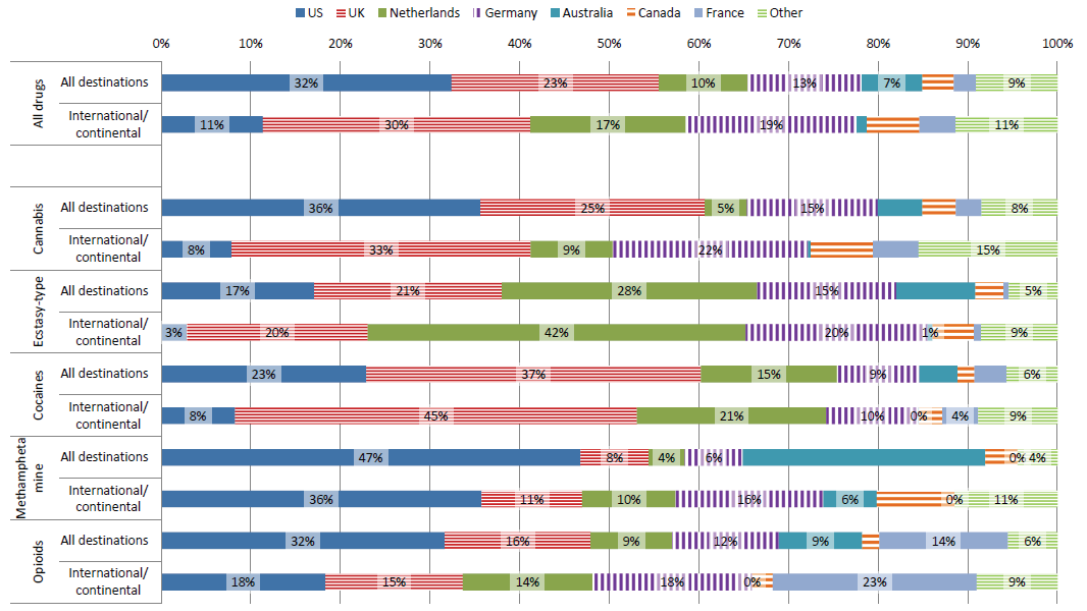


Table 2 contains drug pricing data from the principal countries included in the study. These figures combine prices for drugs that are sold both domestically and internationally. Cannabis is cheapest in the UK and the Netherlands, slightly more expensive in Germany and most expensive in the United States, Canada and Australia, all of which have approximately the same price. A similar picture emerges with pricing of ecstasy-type products, with prices lowest in the UK, Netherlands, Germany and France, 46 percent higher in the United States, 70 percent higher in Canada and more than four times the base price in Australia. Methamphetamine is most cheaply priced in the Netherlands, similarly priced in the United States and Germany and significantly more expensive in Australia. Opioids are again cheapest in the Netherlands, similarly priced in the UK and Germany, 64 percent higher than the base price in the United States and more than three times the base price in Australia. These figures are consistent with the hypothesis that the darknet drugs trade is significantly more integrated and, therefore, more competitive in EU countries, with the effect that increased competition drives prices down. The United States and Australian darknet drug markets appear to be relatively isolated, and this would account for the relatively higher drug prices evident in those countries.

Table 2: Percentage change from base for the expected price of drugs by country of origin, controlling for price, weight and specific drug type to any shipping destination, active products only

	Cannabis		Ecstasy-type		Cocaine		Meth		Opioids	
	Exp(β)	P	Exp(β)		Exp(β)		Exp(β)		Exp(β)	
US	142%	***	146%	***	99%	0.88	(base)		164%	***
UK	(base)		(base)		(base)		272%	0.15	(base)	
Netherlands	108%	0.32	103%	0.78	70%	***	63%	*	60%	***
Germany	120%	*	106%	0.58	89%	0.25	121%	0.39	100%	1.00
Australia	137%	***	425%	***	242%	***	328%	***	197%	***
Canada	158%	***	170%	***	105%	0.58	128%	0.25	144%	*
France	125%	***	101%	0.99	78%	***	N/A		104%	0.80

* = significant at the 95% level ** = significant at the 99% level *** = significant at the 99.9% level

References

URLs correct as at March 2018.

Australian Institute of Criminology (AIC) 2015. *Ecstasy factsheet*. Canberra: Australian Institute of Criminology

Aldridge J & Décary-Hétu D 2015. Sifting through the net: Monitoring of online offenders by researchers. *European Review of Organised Crime* 2: 122–41

Aldridge J & Décary-Hétu D 2014. *Not an 'ebay for drugs': The cryptomarket 'silk road' as a paradigm shifting criminal innovation*. SSRN 2436643Christin N 2013. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace, in *Proceedings of the 22nd international conference on World Wide Web*. ACM: 213–24)

Cunliffe J, Martin J, Décary-Hétu D & Aldridge J 2017. An island apart? Risks and prices in the Australian cryptomarket drug trade. *International Journal of Drug Policy* 50: 64–73

Décary-Hétu D, Paquet-Clouston M & Aldridge J 2016. Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy* 35: 69–76

Degenhardt L et al. 2016. Estimating the number of regular and dependent methamphetamine users in Australia, 2002–2014. *The Medical Journal of Australia* 204(4): 153

EMCDDA 2014. *Exploring methamphetamine trends in Europe*, European Monitoring Centre for Drugs and Drug Addiction Papers. Luxembourg: Publications Office of the European Union

Kruithof K et al. 2016. *Internet-facilitated drugs trade*. Santa Monica CA/Cambridge UK: RAND Corporation: 21–32

IMF 2017. *Report for selected country groups and subjects, World Economic Outlook*. Washington DC: International Monetary Fund

Martin J 2014a. *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Basingstoke: Palgrave Macmillan

Martin J 2014b. Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice* 14(3): 351–67

Silva JS & Tenreyro S 2006. The log of gravity. *The Review of Economics and Statistics* 88(4): 641–58

Soska K & Christin N 2015. *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem.* Proceedings of the 23rd USENIX security symposium (USENIX Security'14). Washington, DC: 33–48

Spapens T 2014. Dutch crime networks, in *Encyclopedia of criminology and criminal justice*. New York: Springer: 1211–19

United Nations 2017. *Total population—both sexes. World Population Prospects, the 2017 Revision*. New York: United Nations Department of Economic and Social Affairs, Population Division, Population Estimates and Projections Section

Part IV: Policing and responding to organised crime

Chapter 12: Developing and applying a Queensland Crime Harm Index—implications for policing serious and organised crime

Janet Ransley, Kristina Murphy, Susanne Karstedt, David Bartlett, Lucy Forrester and Maurice Carless

Contemporary police agencies face complex challenges. Technological, social and economic changes are driving new crime problems, while there remains an expectation that police will continue to perform traditional roles. The Queensland Police Service's Serious and Organised Crime group, for instance, has responsibility for homicides, organised crime, major drug problems and rural and stock crimes but, in recent years, has also assumed roles to deal with financial and cybercrimes, outlaw motorcycle gangs, child abuse and sexual crimes, and racing and gambling crimes. In many cases, the new responsibilities have been driven by external factors, such as royal commissions, media concerns and political platforms, rather than any rational planning process.

Given the expanding scope of policing activity experienced by policing agencies around the world, the problem facing many agencies is how best to target their resources. This has been particularly the case in countries like Britain, where budgets shrank after the 2008 global financial crisis (Ashby 2017). Australian agencies have largely avoided budget cuts but, nevertheless, are increasingly asked to account for how they allocate resources and to evaluate the effectiveness of their activities.

While police agencies serve multiple purposes, their effectiveness is largely measured by how well they respond to and reduce crime. Traditional accountability and performance measures rely heavily on crime counts. But simply counting the numbers of offences says little about the severity of those crimes and their impact on individuals and communities. Traditional performance measures also provide little insight into the non-crime roles of policing, such as crime and traffic injury prevention, responding to low-level but annoying antisocial behaviours and improving public safety. Crime counts also say nothing about how police engage with communities and how much trust and confidence communities have in their police.

As a result of these limitations, there is increasing interest in using the concept of harm to guide police efforts. Below, we outline why harm is relevant to policing and how harm can be measured and ranked. We introduce a project currently in progress, to wdevelop a crime harm index for use by police in Queensland, Australia, which may have broader utility in other jurisdictions in Australia and New Zealand.

Harm, crime and policing

Over the past decade, the incorporation of harm reduction strategies in crime control policy has received increased attention. Jurisdictions including Britain and New Zealand have explicitly identified harm reduction as a primary policing goal (Curtis-Ham & Walton 2017). This trend recognises that 'not all crimes are created equal' (Sherman et al. 2013: 422) and that a focus on reducing volume crimes like residential burglaries and car thefts does not necessarily address those activities which most harm and concern communities. For some communities, the most harmful activities may not be traditional policing targets but instead, quality of life and neighbourhood issues or hidden harms such as domestic violence and child abuse, which are generally under-reported to police (Greene 2014; Ratcliffe 2015).

As a result, researchers and police agencies are increasingly focused on integrating harm-based approaches into crime control, particularly for drug-related and organised crimes (Paoli & Greenfield 2013; MacDonald et al. 2005; UNODC 2005; Maher & Dixon 1999). European countries, in particular, have witnessed such a shift towards a harm-based approach to crime, with national and regional policymaking and law enforcement agencies using harm as a basis for both targeting and prioritising criminal activity (Paoli & Greenfield 2013). Measuring harms offers scope for more informed and evidence-based decision making in targeting police resources and assessing police effectiveness in a meaningful way.

But what does harm mean, and how can it be meaningfully operationalised for policing purposes? Until recently, most research has been focused on measuring harm-related concepts, including the perceived seriousness of various offences, costs of crime and impact of victimisation (Paoli & Greenfield 2013; Stylianou 2003).

Attempts to assess the seriousness of different crimes first became prominent when Sellin and Wolfgang (1964) began reporting on perceptions of crime seriousness. They used community surveys that ranked the relative seriousness of a selected number of offences (Selling & Wolfgang 1964; Wolfgang et al. 1985). From this and subsequent studies, it emerged that there is generally a degree of consensus among the public and criminal justice professionals in their judgments of crime severity (Stylianou 2003). However, Rossi et al. (1974) found that norms relating to crime seriousness are widely diffused throughout subgroups of society, and Levi and Jones (1985) found that, while there was high concordance between public and police participants in England and Wales regarding the seriousness of violent offences and theft, the public rated the seriousness of burglary, fraud and other 'victimless crimes' much more highly than did police officers. Overall, however, studies have consistently found widespread consensus in the perceived seriousness of various offences (Paoli & Greenfield 2013; Figlio 1975; Wilson, Walker & Mukherjee 1986; Rossi et al. 1974; Robinson & Darley 2007).

Critics have argued that this stream of research is flawed because it relies on perceptions, rather than actual measures of seriousness. Further, seriousness may be misinterpreted and not actually equate to harmfulness. The first criticism is seen as problematic, because public perceptions can be inaccurate, swayed by media portrayals, dependent on personal experiences and liable to change over time (Stylianou 2003; Kwan et al. 2000; Shoemaker & Bryant 1987; Cullen, Link & Polanzi 1982; Piquero, Carmichael & Piquero 2008). On the second criticism, the problem is the potential for confusion about the meaning of seriousness; Warr (1989) argues that many respondents are likely to confuse the related but distinct concepts of seriousness and wrongfulness.

An alternative approach is to focus on the costs of various offences. This includes the direct costs to victims, but also indirect financial costs shared by society. Indirect costs might include lost output due to reduced productivity, medical expenses and labour costs, and criminal justice costs resulting from crime, local, state and federal government funds spent on police protection, corrective, legal and adjudication services, and cost of incarceration (McCollister, French & Fang 2010). Multiple studies have focused on economic costs of specific crimes, including drug abuse (Rice, Kelman & Miller 1991; Mark et al. 2001) and domestic violence (Laing & Bobic 2002). Additionally, attention has been paid to the intangible costs of crime, including decreased quality of life, pain, psychological distress and fear of crime suffered by victims of crime (McCollister, French & Fang 2010; Cohen 1988; Cohen & Miller 1998; Moore & Shepherd 2006).

However, there are many challenges in operationalising the cost of crime as a measure for harm-focused policing models. Firstly, the determination of harm is susceptible to inflationary adjustments, with units of cost varying each year (Ratcliffe 2015). Secondly, there are many low volume crimes that result in significant harm that is not easily calculable, for example, child sexual abuse. Ratcliffe (2015) argues that it is low volume – high harm crimes that hold greater importance in a harm-focused policing model. Moreover, many studies that have calculated crime cost estimates categorise offences into large groups and thus are limited by being unable to distinguish between types of offences within these large categories (McCollister, French & Fang 2010). Wickramasekera et al. (2015) systemically reviewed 21 studies that estimated the cost of crime. They concluded that current crime cost estimates in the literature are ineffective.

Crime harm indexes

Recent attention has focused on the development of crime harm indexes. Typically, these indexes incorporate measures of both offence seriousness and the extent of victimisation to develop a single numeric harm value for each offence. These weighted values can then be ranked and prioritised (Ratcliffe 2015; Sherman, Neyroud & Neyroud 2016; Weinborn et al. 2017). As well as facilitating the targeting of resources to the most harmful acts, it has been suggested that an index can be used as a tool to more meaningfully measure police performance and effectiveness. Such an approach complements current movements in policing, such as problem-oriented, intelligence-led and evidence-based policing (Carter & Carter 2009; Ratcliffe 2015). There have been different approaches to developing crime harm indexes.

Community perception models

The Sellin-Wolfgang (1964) study mentioned earlier involved the first widely reported attempt at a crime seriousness index. It used surveys of community perceptions of different offences. It was replicated in many studies in various jurisdictions (Akman, Normandeau & Turner 1966; Riedel 1975) and was trialled in several policing applications (Heller & McEwen 1973). Another index was developed, also using community perceptions, in Hong Kong (Thurstone 1927; Kwan et al. 2002).

In Australia, the National Offence Index (NOI) is a mixed model index constructed based on the Western Australian Crime Research Centre (CRC) Offence Seriousness Index, which operationalised offence seriousness using both public perception surveys and legislated penalties (Andersson 2003; ABS 2009). The NOI is limited, in that it only ranks four-digit offence classification groups. As a result, the index cannot be applied to offences in broader division and subdivision levels (ABS 2009). Additionally, Andersson (2003) notes that multiple offences in the index require re-ranking because of changes in perceived seriousness of offences over time.

Survey-based indexes have been criticised for their costs, the difficulties for survey participants in separating out generic harms from their individual victimisations and the fact that perceptions can change over time (Ratcliffe 2015; Sherman, Neyroud & Neyroud 2016). On the other hand, community surveys have the advantage of reflecting community views, rather than those of officials, judges or police. In this sense, they can provide a democratic approach to assessing harm and an understanding of how communities perceive both crime harms and the appropriateness of the police response.

Indexes based on mixed models

Crime harm indexes based on mixed models have been developed to account for the weaknesses of a singular approach to operationalising harm. Greenfield and Paoli (2013) designed a framework for the qualitative analysis and assessment of harm. The framework consists of a two-dimensional taxonomy of possible gross harms associated with criminal activities. One dimension assesses the bearers of harm, comprising individuals, government entities, private sector entities and the environment. The other dimension assesses types of harms, including those affecting functional integrity, reputation, material interest and privacy. Both the severity and overall incidence of each harm are rated using severity and incidence scales, and then a matrix is developed to prioritise harms (Greenfield & Paoli 2013). This framework has been applied to assess harms associated with cocaine trafficking (Paoli, Greenfield & Zoutendijk 2013), human trafficking, VAT fraud, tobacco smuggling and cannabis cultivation (Paoli, Decorte & Kersten 2015).

Sentencing outcomes indexes

The Canadian Crime Severity Index (CCSI) uses sentencing outcomes. Based on data collected since 1998, the CCSI measures both the severity and volume of police-reported crime and is used as a tool to make comparisons of these measures over time and across jurisdictions

(Wallace et al. 2009). The CCSI operationalises crime seriousness by measuring both the incarceration rate for a particular offence type and the average length of prison sentences (in days) for the specific type of offence (Wallace et al. 2009). Three separate crime seriousness indexes have been developed by Statistics Canada: (1) an index for all crime; (2) an index for violent crime; and (3) an index for non-violent crime (Wallace et al. 2009). Sample tables provided by Statistics Canada indicate that the index uses a wide range of weights, starting at seven, for possession of cannabis, and finishing at 7,042, for first-degree murder (Ratcliffe 2015).

More recently, in Britain, the Office for National Statistics has developed a Crime Severity Score based on mean sentences passed for those convicted of various offences (Ashby 2017), and, in New Zealand, a crime harm index has been developed based on average actual sentences served (Curtis-Ham & Walton 2017).

A key problem with using actual sentence outcomes as the basis of an index is that sentencing typically involves a range of considerations, including offence seriousness but also offender and offence characteristics that can either mitigate or aggravate the actual sentence, along with the need for deterrence and community protection. None of the approaches mentioned separates out these factors to derive an index based purely on offence seriousness. Thus, such indexes are as much measures of sentencing practices as they are of harms.

Indexes based on sentencing guidelines

Hence, an alternative approach to developing an index has emerged, which focuses not on actual sentences but on penalties laid out in formal sentencing guidelines. In the United States, Ratcliffe (2015) developed the Pennsylvania Offence Gravity Score Index using sentencing guidelines available for trial judges. Offence gravity scores were calculated by applying a point value to each offence based on the guidelines, then multiplying that value by the numbers of reported offence incidences to develop a weighted index.

In a similar vein, the Cambridge Crime Harm Index (CHI) developed by Sherman and colleagues (Sherman, Neyroud & Neyroud 2016) uses officially developed sentencing guidelines as a basis, although it has a number of distinctive features. Firstly, it includes only crimes reported to police, excluding police-detected activity such as much drug, traffic and organised crime offences. To exclude offender characteristics, offence scores were based on the lowest starting point in the sentencing guidelines for each offender. Thus, the Cambridge CHI aims to measure harm independently of culpability and sentencing practices (Sherman, Neyroud & Neyroud 2016).

Since its development, the Cambridge CHI has been employed by multiple British police agencies and used in numerous studies, in areas including domestic violence (Bland & Ariel 2015; Barnham, Barnes & Sherman 2017; Dudfield et al. 2017; Bridger et al. 2017; Goosey, Sherman & Neyroud 2017; Button, Angel & Sherman 2017), the crime reduction effects of police hot spot patrols (Weinborn, Ariel & Sherman 2016; Gibson, Slothower & Sherman 2017; Strang et al. 2017), gang injunctions (Carr, Slothower & Parkinson 2017) and the use of automatic number plate recognition (Sidhu, Barnes & Sherman 2017). It has also been applied outside the United Kingdom, in California (Mitchell 2017), Australia and Uruguay (Sherman 2013). Applications in Australia have included studies of family violence in Western Australia (2016) and the Northern Territory (Kerr, Whyte & Strang 2017).

The use of the Cambridge CHI in Australia is problematic for three reasons. Firstly, it was developed based on offences and sentencing guidelines in England and Wales. Although there are similarities, there are also significant differences with laws and practices in Australia. Secondly, as outlined above, the Cambridge CHI methodology specifically excludes police-detected offending, including much drug, violent extremism, organised crime and public order related problems, many of which are significant challenges for most Australian jurisdictions. Thirdly, based as it is on sentencing commission guidelines, the Cambridge CHI expresses official views on crime harm. While Sherman, Bland et al. (2016) argue that it can be imputed that community views have informed the guidelines, there is limited evidence to support this, and, of course, they cannot possibly reflect Australian community perceptions.

Of the indexes outlined, the Cambridge CHI has advantages, including a clear focus on harms, rather than offender or offence characteristics, and a relatively straightforward and transparent approach. It comprehensively ranks all offences (apart from the exclusions already mentioned). But, based on the critiques above, it is suggested that the Cambridge CHI in its original form is not well suited to Australian applications; the next section outlines the methodology used in developing a Queensland CHI.

Queensland Crime Harm Index

The simplest way to develop a crime harm index for Queensland conditions would have been to replicate the Cambridge methodology using local data. Unfortunately, however, like most Australian jurisdictions, Queensland lacks comprehensive sentencing guidelines. While penalties are legislated, a large range of offences share the same penalty level, meaning that it is impossible to distinguish between them in terms of seriousness or harm. So, while the extent of victimisation associated with each offence can be determined from official records, it is impossible to apply the Cambridge CHI method to assess harm and calculate an index ranking. The applications of the Cambridge CHI that have been conducted in Australia (Sherman 2013; Kerr, Whyte & Strang 2017) both acknowledge this issue but applied the Cambridge CHI anyway, in the absence of a ready alternative.

The Queensland Crime Harm Index project is adopting a different approach, using mixed methods drawn from several of the studies outlined in this chapter. Firstly, perceptions of crime harm (not seriousness) were gauged by conducting a representative community survey of 2,000 Queenslanders. Respondents were asked to assess the harm caused by different crimes—to victims, their families and the community at large. Respondents were also asked how police resources should be prioritised in relation to particular problems. The overall objective of the survey was to determine how the community assesses and ranks crime harms and how they think police should prioritise their efforts. Unlike the Cambridge CHI, police-detected offences were included.

Secondly, we conducted a similar survey of police officers. This is important because it can be assumed that most police officers have a more informed view of the extent and impact of crime, at least within their immediate work area. Hence, incorporating their views will help overcome any community misinformation about crime. It also enables comparisons to be made between police and community views.

The analysis of results from each survey also enables differences to be identified based on gender, age, location, prior victimisation and other factors, to determine the extent to which views of harm are shared across entire groups and between communities and police. Based on these findings, an adapted crime harm index will be developed that is reflective of Queensland communities and offences; it will weigh and triangulate both police and community perceptions. In cooperation with the Queensland Police Service, a trial will then be developed to test the extent to which the index can be used to guide strategic and operational decision making.

This index is being developed specifically for Queensland, based on Queensland surveys. However, it is likely to be of interest to other jurisdictions in Australia and New Zealand, because their criminal law and policing approaches are more comparable with Queensland's than with Britain's (where the Cambridge CHI was developed). Further, there is little evidence to suggest much variation in perceptions based on the state or territory in which people live, so the Queensland index could be useful either in itself or as an alternative model for replication in other jurisdictions.

Conclusion

As discussed above, there are clear operational and managerial advantages that flow from the use of a crime harm index, including improved targeting of resources on the most harmful offences and areas and better performance measurement because trends in harm can be compared across time and areas. Prior approaches to developing such an index have been based on community perceptions, sentencing outcomes, mixed qualitative models and sentencing guidelines. While the Cambridge CHI, based on sentencing guidelines for England and Wales, has recently gained currency, there are limitations in applying it in its original form in jurisdictions outside the United Kingdom. The Queensland Crime Harm Index project is developing an index for Queensland using mixed methods, including community and police officer surveys of perceptions of crime harm.

References

URLs correct as at February 2018

Akman D, Normandeau A & Turner S 1966. Replication of a delinquency and crime index in French Canada. *Canadian Journal of Corrections* 8: 1–19

Andersson C 2003. *Development of a national offence index for the ranking of offences*. Presented at the AIC/ABS Conference—Evaluation in Crime and Justice: Trends and Methods, Australian Bureau of Statistics

Ashby MPJ 2017. Comparing methods for measuring crime harm/severity. *Policing: A Journal of Policy and Practice*, online advance https://doi.org/10.1093/police/pax049

Australian Bureau of Statistics (ABS) 2009. *National offence index, 2009*. ABS cat. no. 1234.0.55.001. http://abs.gov.au/ausstats/abs@.nsf/mf/1234.0.55.001

Barnham L, Barnes GC & Sherman LW 2017. Targeting escalation of intimate partner violence: Evidence from 52,000 offenders. *Cambridge Journal of Evidence-Based Policing* 1(2–3): 116–42. https://doi.org/10.1007/s41887-017-0008-9

Bland M & Ariel B 2015. Targeting escalation in reported domestic abuse: Evidence from 36,000 callouts. *International Criminal Justice Review* 25(1): 30–53

Bridger E et al. 2017. Intimate partner homicide in England and Wales 2011–2013: Pathways to prediction from multi-agency domestic homicide reviews. *Cambridge Journal of Evidence-Based Policing* 1(2–3): 93–104. https://doi.org/10.1007/s41887-017-0013-z

Button IMD, Angel C & Sherman LW 2017. Predicting homicide and serious domestic violence in Leicestershire with intelligence records of suicidal ideation or self-harm warnings: A retrospective analysis. *Cambridge Journal of Evidence-Based Policing* 1(2–3): 105–115. https://doi.org/10.1007/s41887-017-0009-8

Carr R Slothower M & Parkinson J 2017. Do gang injunctions reduce violence crime? Four tests in Mersyside. *Cambridge Journal of Evidence-Based Policing* 1(4): 195–210. https://doi.org/10.1007/s41887-017-0015-x

Carter D & Carter J 2009. Intelligence-led policing: Conceptual and functional considerations for public policy. *Criminal Justice Policy Review* 20(3): 310–25. doi:10.1177/0887403408327381

Cohen MA 1988. Some cautionary notes on the use of the Sellin-Wolfgang index of crime seriousness. *Journal of Quantitative Criminology* 4(1): 61–70

Cohen MA & Miller TR 1998. The cost of mental health care for victims of crime. *Journal of Interpersonal violence* 13(1): 93–110

Cullen FT, Link BG & Polanzi CW 1982. The seriousness of crime revisited: Have attitudes toward white-collar crime changed? *Criminology* 20(1): 83–102

Curtis-Ham, S & Walton, D 2017. The New Zealand Crime Harm Index: Quantifying harm using sentencing data. *Policing: A Journal of Policy and Practice* online advance, https://doi.org/10.1093/police/pax050

Dudfield G, Angel C, Sherman L & Torrence S 2017. The 'p*ower* curve' of victim harm: Targeting the distribution of crime harm. Index values across all victims and repeat victims over 1 year. *Cambridge Journal of Evidence-Based Policing* 1(1): 38–58

Figlio R 1975. The seriousness of offenses: An evaluation by offenders and nonoffenders. *Journal of Criminal Law and Criminology* 66(2): 189–200

Gibson C, Slothower M and Sherman LW 2017. Sweetspots for hot spots? A cost-effectiveness comparison of two patrol strategies. *Cambridge Journal of Evidence-based Policing. 1(4): 225–43. http://doi.org/10.1007/s41887-017-0017-8*

Goosey J, Sherman L & Neyroud P 2017. Integrated case management of repeated intimate partner violence: A randomised controlled trial. Cambridge Journal of Evidence-Based Policing 1(2–3): 174–189. https://doi.org/10.1007/s41887-017-0012-0

Greene JR 2014. New directions in policing: Balancing prediction and meaning in police research. *Justice Quarterly 31(2): 193–228*

Greenfield V & Paoli L 2013. A framework to assess the harms of crimes. British Journal of Criminology 53(5): 864–85

Heller NB & McEwen JT 1973. Applications of crime seriousness information in police departments. *Journal of Research in Crime and Delinquency* 12(1): 44–50. doi:10.1177/002242787501200105

Kerr J, Whyte C & Strang H 2017. Targeting escalation and harm in intimate partner violence: Evidence from Northern Territory Police, Australia. *Cambridge Journal of Evidence-Based Policing* 1(2–3): 143–159. https://doi.org/10.1007/s41887-017-0005-z

Kwan YK, Chiu LL, Ip WC & Kwan P 2002. Perceived crime seriousness: Consensus and disparity. *Journal of Criminal Justice* 30(6): 623–32

Laing L & Bobic N 2002. *Economic costs of domestic violence*. Partnerships Against Domestic Violence and the University of New South Wales. Australia. http://www.mujereslibresdeviolencia.usmp.edu.pe/wp-content/uploads/2015/03/Economic_costs_of_DV.pdf

Levi M & Jones S 1985. Public and police perceptions of crime seriousness in England and Wales. *British Journal of Criminology* 25(3): 234–50

MacDonald Z, Tinsley L, Collingwood J, Jamieson P & Pudney S 2005. *Measuring the harm from illegal drugs using the Drug Harm Index*

Maher L & Dixon D 1999. Policing and public health: Law enforcement and harm minimization in a street-level drug market. *British Journal of Criminology* 39(4): 488–512

Mark TL, Woody GE, Juday T & Kleber HD 2001. The economic costs of heroin addiction in the United States. *Drug and Alcohol Dependence* 61(2): 195–206

McCollister KE, French MT & Fang H 2010. The cost of crime to society: New crime-specific estimates for policy and program evaluation. *Drug and Alcohol Dependence* 108(1): 98–109

Mitchell RJ 2017. The usefulness of a crime harm index: Analysing the Sacramento Hot Spot Experiment using the California Crime Harm Index (CA-CHI). *Journal of Experimental Criminology*, online advance, https://doi.org/10.1007/s11292-017-9318-y

Moore S & Shepherd JP 2006. The cost of fear: Shadow pricing the intangible costs of crime. *Applied Economics* 38(3): 293–300

Paoli L, Decorte T & Kersten L 2015. Assessing the harms of cannabis cultivation in Belgium. *International Journal of Drug Policy* 26(3): 277–89

Paoli L & Greenfield V 2013. Harm: A neglected concept in criminology, a necessary benchmark for crime-control policy. *European Journal of Crime, Criminal Law and Criminal Justice* 21(3–4): 359–377. doi:10.1163/15718174-21042034

Paoli L, Greenfield V & Zoutendijk A 2013. The harms of cocaine trafficking: Applying a new framework for assessment. *Journal of Drug Issues* 43(4): 407–436. doi:10.1177/0022042613475614

Piquero N, Carmichael S & Piquero A 2008. Assessing the perceived seriousness of white-collar and street crimes. *Crime & Delinquency* 54(2): 291–312

Ratcliffe JH 2015. Towards an index for harm-focused policing. *Policing* 9(2): 164–82

Rice DP, Kelman S & Miller LS 1991. Estimates of economic costs of alcohol and drug abuse and mental illness, 1985 and 1988. *Public Health Reports* 106(3): 280

Riedel M 1975. Perceived circumstances, inferences of intent and judgements of offense seriousness. *The Journal of Criminal Law and Criminology* 66(2): 201–20

Robinson P & Darley J 2007. Intuitions of justice: Implications for criminal law and justice policy. *Southern California Law Review* 81(1)

Rossi PH, Waite E, Bose CE & Berk RE 1974. The seriousness of crimes: Normative structure and individual differences. *American Sociological Review* 39: 224–37

Sellin T & Wolfgang M 1964. *The measurement of delinquency*. New York: John Wiley and Sons.

Sherman LW 2013. The rise of evidence-based policing: Targeting, testing and tracking. *Crime and Justice* 42(1): 377–451

Sherman L, Bland M, House P & Strang H 2016. *Targeting family violence reported to Western Australia police 2010–2015: The felonious few vs. the miscreant many*. Report to the Western Australia Police. Cambridge Centre for Evidence-Based Policing Ltd. https://www.police.wa.gov.au/About-Us/News/New-approach-needed-on-family-violence

Sherman LW, Neyroud PW & Neyroud E 2016. The Cambridge Crime Harm Index: Measuring total harm from crime based on sentencing guidelines. *Policing* 10(3): 171–83

Shoemaker D & Bryant C 1987. Perceived seriousness of crime. *Psychological Reports* 61: 267–72

Sidhu B, Barnes GC & Sherman LW 2017. Tracking police responses to 'hot' policing alerts: Automatic number plate recognition and the Cambridge Crime Harm Index. *Cambridge Journal of Evidence-Based Policing* 1(2–3): 211–224. https://doi.org/10.1007/s41887-017-0016-9

Strang H, Sherman L, Ariel B, Chilton S, Braddock R, Rowlinson T, Cornelius N, Jarman R and Weinborn C 2017. Reducing the harm of intimate partner violence: Randomized controlled trial of the Hampshire Constabulary CARA experiment. *Cambridge Journal of Evidence-based Policing* 1(2–3): 1160–73. https://doi.org/10.1007/s41887-017-0007-x

Stylianou S 2003. Measuring crime seriousness perceptions: What have we learned and what else do we want to know. *Journal of Criminal Justice* 31(1): 37–56

Thurstone L 1927. The method of paired comparisons for social values. *The Journal of Abnormal and Social Psychology* 21(4): 384–400

United Nations Office on Drugs and Crime (UNODC) 2005.*World drug report 2005: Volumes I and II.* https://www.unodc.org/pdf/WDR_2005/volume_1_web.pdf

Wallace M, Turner J, Matarazzo A & Babyak C 2009. *Measuring crime in Canada: Introducing the Crime Severity Index and improvements to the Uniform Crime Reporting Survey (No. 85–004–X)*. Canadian Centre for Justice Statistics. http://www.statcan.gc.ca/pub/85-004-x/85-004-x2009001-eng.pdf

Warr M 1989. What is the perceived seriousness of crimes? *Criminology* 27(4): 795–822

Weinborn C, Ariel B & Sherman L 2016. 'Soft' policing at hot spots: Do police community support officers work? A randomized controlled trial. *Journal of Experimental Criminology*, 12(3): 277–317. doi:10.1007/s11292-016-9260-4

Weinborn C, Ariel B, Sherman L & O'Dwyer E 2017. Hotspots vs. Harmspots: Shifting the focus from counts to harm in the criminology of place. *Applied Geography* 86: 226–44

Wickramasekera N, Wright J, Elsey H, Murray J & Tubeuf S 2015. Cost of crime: A systematic review. *Journal of Criminal Justice* 43(3): 218–28

Wilson P, Walker J & Mukherjee S 1986. *How the public see crime: An Australian survey (Report No. 2)*. Canberra: Australian Institute of Criminology. Retrieved from Australian Bureau of Statistics

Wolfgang M, Figlio R, Tracy P & Singer S 1985. *The national survey of crime severity (No. 96017)*. U.S. Department of Justice Bureau of Justice Statistics. http://www.bjs.gov/content/pub/pdf/nscs.pdf

Chapter 13: Impact of ballistic evidence on police investigations into organised crime

Anthony Morgan and Penny Jorna

The use of firearms by organised crime groups, particularly in high profile incidents of violence between members of rival groups, attracts considerable public interest and can undermine community confidence and wellbeing (Crocker et al. 2017). Firearms are used by organised crime groups as part of territorial disputes and 'turf wars', to promote their image and reputation or as part of personal conflict (ACIC 2016). While there are limited published data on the involvement of organised crime groups in firearm crime, research based on data on seized firearms has demonstrated a high concentration of firearms among serious and organised crime groups (Bricknell 2012). Further, NSW research has shown that at least one-third of 'shoot with intent' and 'discharge firearm into premises' incidents were related to gangs, drugs or organised crime (Fitzgerald 2013).

Not surprisingly, the use of firearms by organised crime groups also attracts considerable attention from law enforcement. There are well known challenges associated with investigating organised crime. Criminal networks are increasingly sophisticated, finding new ways to avoid detection. Victims and offenders involved in violent incidents are often known to one another and have a criminal relationship, meaning that victims may be unwilling to cooperate with police for fear of retribution (Regoeczi, Jarvis & Riedel 2008; BOCSAR 2015). Canadian research has shown that homicides involving firearms are three times more likely to be unsolved, when compared to homicides involving other weapon types, and the involvement of other criminal activities (eg gangs, drugs) significantly increases the likelihood that a homicide will remain unsolved (Dauvergne & Li 2006).

Forensic evidence plays an important role in the investigation of organised crime. This includes ballistic evidence. When a firearm is discharged, it leaves unique microscopic markings on the surface of the bullet and cartridge case. Forensic firearm examiners can use these markings to link cartridge cases and projectiles recovered from a crime scene to a firearm seized as part of an investigation. This can help to determine whether that firearm was used in the commission of the crime being investigated.

Forensic firearm examiners will also attempt to identify matches between two separate case exhibits—bullets or cartridges from crime scenes or recovered firearms—for cases that were not previously known to be related. A match is known as a cold hit. When two separate cases are found to have involved the same firearm, investigators are able to access additional evidence from the linked investigation.

However, in the past, the time required to manually compare two specimens under a microscope to identify and compare markings between two or more exhibits, and the volume of exhibits held by law enforcement organisations, meant that comparisons were typically limited to those situations in which there was intelligence suggesting that two cases were linked (Cork et al. 2008). The likelihood of finding a match was, therefore, low. The advent of automated ballistic imaging and analysis systems in the 1990s significantly improved the capacity of law enforcement to identify links between investigations into firearm crime (Braga & Pierce 2004). Automated systems provide a small number of correlations between potentially linked firearm events within minutes for manual verification by a trained ballistic expert (Braga & Pierce 2004; Yang et al. 2014). This increases the probability of obtaining a match, because the volume of exhibits that can be compared is increased.

These systems have been adopted in dozens of countries, including the United States, United Kingdom, Canada and throughout Europe and Asia. International networks also exist. The first automated ballistic system to be used in Australia was introduced in NSW in 2000. In July 2014, the Australian Ballistics Information Network (ABIN) became fully operational as a national system. The ABIN is managed by the Australian Criminal Intelligence Commission and uses the Integrated Ballistics Identification System (IBIS) technology to provide a national automated ballistic information system to Australian police agencies, thereby enabling both local and national cold hits.

A small number of studies have explored the impact of automated ballistic technology. Braga and Pierce (2004) found that ballistic imaging technology was associated with a more than sixfold increase in the number of cold hit matches per month made by the Boston Police Department's Ballistics Unit. A subsequent evaluation showed that IBIS cold hits generated significant investigative leads in 39 percent of the 44 hits analysed, including three in four homicide matches, while a significant proportion of offenders were arrested as a result of IBIS matches (Braga 2008).

Findings from the more recent evaluation of the US ballistic information system were less positive. Based on interviews with 65 investigators, the research found that National Integrated Ballistic Identification Network (NIBIN) hits did not directly assist investigators in the majority of cases reviewed, partly because of delays in the process of identifying hits and notifying investigators. The additional information from cold hits did help to identify a suspect in 10 percent of cases (n=6), led to an arrest in one case, helped in charging a suspect or obtaining a plea in three cases, and helped with sentencing in one case.

Both Braga (2008) and King et al. (2013) found evidence that the information from hits was used in other ways, such as to eliminate a suspect from consideration, and provided intelligence that had some strategic benefit to law enforcement. This helped to build an understanding of conflicts between gangs and criminally active groups in Boston (Braga 2008). While Braga noted the high proportion of offenders arrested as a result of IBIS matches who were known gang members, there has been limited analysis of the benefits of automated ballistic technology to the investigation of firearm crime involving organised crime groups.

Research aims and method

The current study explored the impact of ballistic evidence on police investigations into firearm crimes involving, or suspected of involving, organised crime groups. It aimed to address the following research questions:

- What was the extent of organised crime involvement in linked incidents of firearm-related crime?
- What were the characteristics of those incidents involving organised crime groups?
- How did the investigations into these cases benefit from the information available from linked cases?

This research was part of a larger study evaluating the impact of ballistic evidence on criminal investigations into firearm crime generally (see Morgan & Jorna forthcoming). As part of that research, a brief questionnaire was developed to gather detailed case information from police investigators to examine the contribution of intelligence obtained through ballistic evidence to the investigation of firearm-related crime.

The contact details of investigators using the ABIN were obtained. Interviews were conducted with investigators throughout 2015 and early 2016. From an initial combined sample of 121 hits, involving 194 unique cases, contact details were provided for investigators involved in 133 criminal investigations. Follow-up interviews were conducted with investigators from 60 criminal investigations, involved in a total of 49 cold hits. The AIC attempted to contact investigators for the remaining 73 cases. Six investigators declined to participate because of the sensitive nature of the investigations, and 67 investigators could not be contacted. This resulted in a response rate of 45 percent.

Limitations

There are some important limitations with the current study that must be acknowledged. The overall response rate to the case file questionnaire was 45 percent, based on the total number of cases with contact information available. However, this represents just 31 percent of all cases that resulted in a cold hit during the study period. The results may not be representative of the entire sample of cold hits and linked investigations. The relatively small sample size also prohibited more detailed analysis, although it still compares favourably with previous research in the United States (Braga 2008; King et al. 2013).

A further limitation relates to the subjective nature of the assessment made by investigators regarding the impact of the ballistic evidence on their investigation. Some investigators found it difficult to separate the ballistic evidence from other developments in the investigation. Moreover, the assessment made by officers is likely to be influenced by the value they place on ballistic evidence—possibly based on past experience—relative to other investigative techniques.

Results

Fifty-three percent (n=32) of the linked cases related to incidents involving organised crime groups. It was not known whether organised crime was involved in a further 30 percent (n=18) of cases (Table 1). This is not surprising, given the challenges associated with assessing whether organised crime groups are involved in an offence, particularly where the identity of an offender is unknown (Crocker et al. 2017; Fitzgerald 2013). Nevertheless, this means that—among those cases where it could be confirmed—organised crime was involved in 76 percent of the incidents linked by ballistic evidence.

Table 1: Organised crime involvement in linked cases

	n	%
Involved	32	53
Unknown	18	30
Not involved	10	17
Total	60	100

Source: Detailed case analysis 2016 [AIC data file]

These cases all involved serious, violent offences (Table 2). Two-thirds of linked cases (63%, n=20) with known involvement of organised crime groups related to the unlawful use of a firearm or discharge of a firearm at prohibited places. Almost one-third (29%, n=9) involved a murder or attempted murder offence.

Notably, three-quarters of the cases in which it was unknown whether organised crime was involved (72%, n=13) also related to an investigation into the unlawful use of a firearm or discharge of a firearm at prohibited places. Given the profile of known organised crime cases, it is highly likely that a significant proportion of these cases involved organised crime groups.

Table 2: Principal offence type

	n	%
Unlawful use of a firearm/discharge of firearm at prohibited places	20	63
Murder	5	16
Attempted murder	4	13
Robbery involving use of a weapon	2	6
Assault	1	3
Total	32	100

Note: Offences classified using the Australian and New Zealand Standard Offence Classifications. Total may not add to 100 due to rounding
Source: Detailed case analysis 2016 [AIC data file]

Prior to obtaining the cold hit, investigators reported that evidence was available from a range of sources (Table 3). Evidence obtained from interviews with witnesses, victims and offenders was available in three-quarters of all cases (72%, n=23). However, investigators also noted that witnesses or victims were often reluctant to assist police in cases involving organised crime groups, typically due to fear of retribution, meaning that limited information was obtained from these interviews.

Surveillance evidence, including CCTV, electronic evidence and intercepted telephone conversations, was the next most common form of evidence (25%, n=8), followed by intelligence (19%, n=6) and physical evidence (16%, n=5), which included DNA, fingerprint evidence and post-mortem reports. Other sources—including evidence gathered via search warrants and covert investigation techniques—were available in a further eight cases (25%). Importantly, ballistic evidence was the only source of evidence available in one-quarter of cases involving organised crime groups, primarily cases involving the unlawful discharge of a firearm (ie drive-by shootings).

One of the main reasons for identifying cold hits is the possibility of gaining access to additional evidence from the linked investigation. For example, one officer described how, in a case involving the discharge of a firearm into premises resulting in injury to the victim, which they suspected as having involved members of an organised crime group, they had been unable to generate any investigative leads because the victim and witnesses were not willing to cooperate. The bullet fragments recovered from the victim's body were provided to forensic firearm examiners within two days of the incident. They were able to establish a link with ballistic evidence seized at a second investigation into the discharge of a firearm into premises, which had occurred around one month earlier. The investigator was able to obtain new physical evidence from the linked case that matched the evidence found at the scene of the incident they were investigating, linking the person of interest to both investigations.

Overall, ten investigators reported that there was new evidence available because of the cold hit. This included new intelligence (n=3), new physical evidence (n=3), additional interviews (n=2) and surveillance evidence (n=1). In six cases, there was some other type of new evidence available, including evidence from covert methods that could not be disclosed during the interview. No new evidence was available from the linked investigation in two-thirds (69%, n=22) of cases.

Table 3: Evidence available pre-hit and additional evidence post-hit due to investigations being linked (n=32)

	Evidence available pre-hit		Additional evidence available as a result of linked investigation	
	n	%	n	%
Interviews (witness, victim and offender)	23	72	2	6
Intelligence (informants and intelligence on criminal groups)	6	19	3	9
Physical evidence (DNA, fingerprints and post-mortem reports)	5	16	3	9
Surveillance (CCTV, electronic evidence, intercepted telephone conversations)	8	25	1	3
Other evidence	8	25	6	19
No evidence available	8	25	22	69

Note: Investigators could identify multiple types of evidence available for each case
Source: Detailed case analysis 2016 [AIC data file]

Nearly half of the cases benefited from the cold hit. Investigators reported that there was a direct benefit to the investigation in 45 percent (n=14) of all cases (Table 4). Ballistic evidence provided significant investigative leads in 16 percent (n=5) of organised crime cases, identified an offender in another 16 percent (n=5) of cases and led to an arrest in four cases (13%). In cases where there was no direct benefit, investigators revealed that the cold hits provided useful intelligence, particularly in relation to organised crime group activity and movements.

Cold hits were more likely to assist an investigation when there were 30 days or fewer between the offence and the investigator being notified of the hit (75% vs 35%), although this difference was not statistically significant based on a Fisher's exact test (p=0.08). However, inactive investigations were no less likely to benefit from a cold hit than investigations that were still active at the time of investigators being notified of a hit (60% vs 44%; p=0.35). This suggests that ballistic evidence may be as beneficial to investigations that have been suspended due to lack of evidence as investigations that are ongoing. Similar trends were observed among the larger sample of cases (Morgan & Jorna forthcoming), suggesting that the importance of timeliness and case status is not unique to organised crime cases.

Table 4: Impact of cold hit on organised crime investigations (n=32)

	n	%
Provided significant investigation leads	5	16
Identified an offender (not yet apprehended)	5	16
Led to an arrest	4	13
No direct impact on investigation (provided general intelligence)	17	53
Unknown	1	3

Source: Detailed case analysis 2016 [AIC data file]

Twelve investigators provided details as to why the hit did not provide more leads. In three cases, the linked investigation did not identify a person of interest relevant for the current case. Investigating firearm crime involving organised crime groups is complicated by the fact that firearms may be passed between and within crime groups, meaning that, while the same firearm may be used, different offenders may be involved. For example, one investigator described how the organised crime group suspected in the linked investigation was not the same group suspected to be involved in the initial investigation. It was believed that the firearm was rarely used and had actually been passed between groups.

Further, investigators highlighted the challenges associated with confirming the identity of an offender or, where the identity of a person of interest was known, connecting that individual to a particular incident. Even when an offender had been apprehended as part of the linked case, there was no way of knowing for certain whether they had been involved in the incident being investigated without additional evidence, such as DNA or fingerprint evidence.

For example, one of the investigators who was interviewed was responsible for investigating a case involving two suspected rival groups or gangs meeting on a public oval and shooting at each other. There were numerous bystanders who were at risk of being wounded, none of whom was able to identify the group participants. The forensic evidence collected consisted only of ballistic evidence. The linked cased related to an incident that occurred several months earlier. There were multiple passengers in a vehicle, and an argument ensued, believed to be over drug money, leading to a firearm being discharged and one of the passengers being wounded. The suspect was arrested and charged. Even with a suspect in custody, investigators were unable to link that offender to the oval shootings due to the lack of physical evidence or witness testimony.

Discussion and conclusion

There are two main findings from this study. Firstly, there is evidence that organised crime groups play a significant role in serious, violent crime in Australia involving the use of firearms. Secondly, there is some promising evidence in support of the impact of the ballistic evidence on investigations into organised crime.

Organised crime groups were involved in at least half of all linked cases that were examined as part of the current study and three-quarters of those cases in which the involvement of organised crime groups (or not) could be confirmed. The vast majority of these cases involved the unlawful discharge of a firearm, often into a residential premise and often directed at rival groups, or the murder or attempted murder of a member of an organised crime group. While other sources of evidence were available to investigators, they were often of limited value, and in a significant proportion of cases the only evidence available to the investigator was ballistic evidence.

Almost half the cases involving organised crime groups that obtained a cold hit directly benefited from the additional information that came from a linked investigation. In many cases, this was the result of new evidence being available. The actual impact varied, ranging from generating new leads to investigate through to resulting in the arrest of the offender.

These findings illustrate the benefits of technological solutions to the investigation of serious and organised crime and add to a growing body of evidence that shows how technology can aid law enforcement when it is well supported and integrated into routine practice. (One police agency involved in the current study has used automated ballistic technology for well over a decade; Lum, Koper & Willis 2016). However, not all cases benefit from linked investigations. Ballistics evidence and automated systems cannot overcome all the barriers to investigating organised crime. There were several examples where it was still not possible to confirm whether the person of interest from a linked investigation was involved in the incident being investigated. Other forms of forensic evidence and investigative techniques are, therefore, still important and beneficial in cases involving organised crime (Higginson, Eggins & Mazerolle 2017).

Acknowledgements

This research was commissioned and funded by CrimTrac (now the Australian Criminal Intelligence Commission) as part of a broader program of collaborative research.

This research would not have been possible without the willing participation of staff from New South Wales Police Force and Victoria Police. The assistance of Courtney Brown, former Research Officer at the Australian Institute of Criminology, in conducting interviews with investigators is also gratefully acknowledged.

References

URLs correct as at February 2018

Australian Criminal Intelligence Commission 2016. *Illicit firearms in Australia*. Canberra: ACIC. https://www.acic.gov.au/publications/intelligence-products/illicit-firearms-australia-report

Braga AA 2008. Gun enforcement and ballistic imaging technology in Boston, in Cork DL, Rolph JE, Meieran ES and Petrie CV (eds), *Ballistic imaging*. Washington DC: National Academies Press: 291–311. DOI: 10.17226/12162

Braga AA & Pierce GL 2004. Linking crime guns: The impact of ballistics imaging technology on the productivity of the Boston Police Department's ballistics unit. *Journal of Forensic Sciences* 49(4): 701–06

Bricknell S 2012. Firearm trafficking and serious and organised crime gangs. *Research and public policy series* no. 116. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp116

Bureau of Crime Statistics and Research (BOCSAR) 2015. *Non-fatal shootings statistics in NSW*. http://www.bocsar.nsw.gov.au/Pages/bocsar_pages/Non-fatal-shootings-statistics-in-NSW.aspx

Cork DL, Rolph JE, Meieran ES & Petrie CV 2008. *Ballistic imaging*. Washington DC: National Academies Press. DOI: 10.17226/12162

Crocker R, Webb S, Garner S & Skidmore M 2017. *The impact of organised crime in local communities*. London: Police Foundation. http://www.police-foundation.org.uk/publication/reducing-impact-organised-crime-local-communities/

Dauvergne M & Li G 2006. Homicide in Canada, 2005. *Juristat* 26(6): 1–26. http://www.publications.gc.ca/pub?id=9.561349&sl=0

Fitzgerald J 2013. *Non-fatal shootings in NSW*. Crime and Justice Statistics Bureau Brief 85: 1–7. http://www.bocsar.nsw.gov.au/Pages/bocsar_publication/bocsar_pub_brief.aspx

Higginson A, Eggins E & Mazerolle L 2017. Police techniques for investigating serious violent crime: A systematic review. *Trends & issues in crime and criminal justice* no. 539. https://aic.gov.au/publications/tandi/tandi539

King W, Wells W, Katz C, Maguire E & Frank J 2013. *Opening the black box of NIBIN: A descriptive process and outcome evaluation of the use of NIBIN and its effects on criminal investigations, Final report*. Washington DC: US Department of Justice and National Institute of Justice

Lum C, Koper C & Willis J 2016. Understanding the limits of technology's impact on police effectiveness. *Police Quarterly* 20(2): 135–63

Morgan A & Jorna P forthcoming. Impact of ballistic evidence on criminal investigations. *Trends and issues in crime and criminal justice*

Regoeczi WC, Jarvis J & Riedel M 2008. Clearing murders: Is it about time? *Journal of Research in Crime and Delinquency* 45(2): 142–62

Yang Y, Koffman A, Hocherman G & Wein LM 2014. Using spatial, temporal and evidence-status data to improve ballistic imaging performance. *Journal of Forensic Science* 59(1): 103–11

Chapter 14: Effectiveness of anti-money laundering obligations in combating organised crime with particular reference to the professions

David Chaikin

Money laundering is a key strength of organised crime, in that it allows the consolidation of unaccountable financial power with pernicious effects on society, including the penetration of legitimate businesses. Successful money laundering will result in the preservation of illicit assets, the financing of new crimes and the corruption of public officials and private enterprise. Organised crime is likely to avail itself of money laundering services in respect of all of its criminal activities that produce illicit monies. The law enforcement community describes modern organised crime as a global business employing professionals and money laundering services to enable its continuing criminal activities. The role of the professions in facilitating the objectives of organised crime is multifaceted and includes the concealment of the proceeds of crime, obscuring the beneficial ownership of assets and evading anti-money laundering (AML) regimes.

AML regulation imposes gatekeeper responsibilities on private sector actors, to protect the financial system from misuse by organised crime. Originally, AML measures focused on drug money laundering and were applied to a limited class of businesses involved in cash transactions, particularly financial institutions. The global AML regulatory regime has expanded those persons who are treated as gatekeepers to include designated non-financial businesses and the professions, as well as the owners and controllers of corporate structures. The effectiveness of this extension of AML obligations in countering organised crime is problematical, given that the AML regime has had limited success in achieving its objectives in relation to financial institutions.

Money laundering

Money laundering has been described as the 'process for the concealment of evidence in which a person seeks to evade responsibility for the ownership, origin or use of funds' (Moscow 2002). This description of money laundering as an abuse of power is highly relevant to the underlying menace of organised crime, in that it suggests that hidden and unaccountable power is an inherently corrupt influence in societies, whatever the political power structure. Money laundering is a key strength of organised crime in that it allows the consolidation of unaccountable financial power with pernicious effects on society, including penetration of legitimate businesses (Australian Criminal Intelligence Commission (ACIC) 2016).

In addressing the risk of money laundering, it should be noted that organised crime participates in a wide range of activities, not only in drug trafficking and money laundering, but in conduct involving the 'mainstream economy', especially various forms of fraud, including card fraud, taxation fraud, investment and financial markets fraud and superannuation fraud (Australian Crime Commission 2015: 62–76). The significance of this observation is that organised crime is likely to avail itself of money laundering services in respect of all of its criminal activities that produce illicit monies.

At one stage, money laundering was viewed as an opportunistic crime, with little evidence of professional syndicates playing a major role (Reuter & Truman 2004: 3, 39). Whether this is still the case for many financial crimes is not clear; however, in relation to high-level drug trafficking and for organised crime generally, money laundering has become a vital tool of its operating business, requiring the services of sophisticated professionals. As the ACIC has emphasised, organised crime operates as a global business that engages professionals to 'advise on complex methods and techniques' and outsources money laundering to 'dedicated service providers and professional organisations' (ACIC 2016: 3). It would seem to follow that, if the business model of organised crime is to be disrupted, there should be increased legislative and enforcement emphasis on professionals. This is reflected in the Financial Action Task Force's (FATF) recommendations which extend AML obligations to the legal and accounting professions (Shepherd 2009: 619).

Organised crime and the professions

Law enforcement frequently claims that the professions are vulnerable to organised crime, particularly the legal profession and the real estate industry in relation to money laundering (AUSTRAC 2017). The professions may facilitate the objectives of organised crime in three ways. Firstly, the professions may assist organised crime in the perpetuation and concealment of predicate crimes by insulating the leadership of organised crime from being connected to such crimes. Professionals may participate in the commission of criminal offences and use their knowledge of the legal system and procedures to subvert the criminal investigatory and prosecutorial process. Secondly, professionals may provide money laundering services to protect the illicit gains of organised crimes. Money laundering services may include concealing the proceeds of crime, obscuring the beneficial ownership of assets through complex corporate

and trusts structures, avoiding or evading tax through exploitation of tax havens or offshore financial centres, and evading regulatory regimes, particularly the detection, freezing and confiscation of illicit assets (AUSTRAC 2015: 5; Attorney-General's Department 2015: 7). Thirdly, and this is related to the second, professionals may advise organised crime on how unaccountable wealth may be ultimately passed to their families, friends and close business associates. Here, the know-how of professional advisers is critical and probably includes knowledge of AML law, family law, bankruptcy law, commercial law and estate planning, as well as accounting and finance. Although there may be violent competition within and between organised crime groups, which may undermine the success of the illicit enterprise, this does not mean that professional advisory services are not critical for the continuation of the enterprise.

The extent of the vulnerability of the professions to organised crime is a matter that has been questioned by lawyers and their professional associations (Law Council of Australia 2017). The Law Council of Australia's viewpoint is credible, in that there is limited evidence as to the extent of professional involvement and complicity in money laundering and other illegal activities (Victorian Law Reform Commission 2016: 36; Choo et al. 2013; Walters et al. 2013). This issue is important because, if the professions are considered to be at low risk of money laundering, then it can be argued that an appropriate regulatory response should be limited, which is consistent with Braithwaite's theories of responsive regulation and the regulatory pyramid (Braithwaite 2002).

AML regulation and the professions

Australia has been a leading advocate of enacting comprehensive AML laws, consistent with global standards, that are designed in part to combat organised crime by creating a regulatory regime that undermines its financial power. However, the objectives of AML laws have expanded beyond targeting drug money laundering by organised crime to encompass other serious criminal offences, such as terrorism, human trafficking, fraud and tax offences (FATF 2012: 3). The wide range of goals of AML may have dissipated the original focus on organised crime. Unlike many other countries, Australia has always viewed AML as a mechanism to attack tax evasion, and this may explain why the tax authorities have become the greatest beneficiary of AML, through using financial intelligence collected from financial institutions (AUSTRAC 2017). While Australia's AML regime has been criticised for its focus on predicate crimes, such as tax evasion, rather than on money laundering (FATF 2015), this has had little impact on governmental policy. This raises a serious question as to whether Australia's AML regime has become primarily a vehicle for the detection of tax evasion and the collection of tax revenue, or for combating organised crime that is, arguably, of secondary importance.

Another major trend in AML is the expansion of the regulatory regime from financial institutions that are involved in cash transactions to a wider class of private sector actors who can facilitate money laundering, including non-cash laundering. The number of individuals and businesses subject to Australia's AML regime has grown from fewer than 4,000 cash dealers in the late 1980s to more than 14,000 reporting entities enrolled under the AML/CTF Act (AUSTRAC 2017). The supervisory challenge of AUSTRAC is: how does it employ its limited

resources to deal with such a diverse range of commercial enterprises, which include massive commercial banks with thousands of employees and billions of dollars of profits and one-person remittance service providers (RSPs—there are more than 5,000 RSPs).

In 2003, global AML standards were applied for the first time to designated non-financial business and the professions (DNFBPs). Under the standards, lawyers, notaries, other independent legal professionals, accountants, real estate agents and trust and company service providers are required to carry out risk-based customer due diligence, report suspicious transactions involving their clients to an external governmental agency, maintain records and file compliance reports. The justification for applying the global AML standards to lawyers is that national and international typologies suggest that certain services provided by the legal profession, such as trust accounts, are vulnerable to criminal misuse (FATF 2008). It is further argued that there would be a significant AML regulator gap if lawyers were not required to act as gatekeepers to the international financial system. At a theoretical level, it may be surmised that organised crime places strategic value on the knowledge, skills, professional secrecy and reputation of the legal profession (Chaikin 2013).

In relation to lawyers, countries such as the United States have refused to countenance any mandatory suspicious transaction reporting requirement. From the US perspective, the requirements entail an unacceptable redefinition of the role of lawyers in the criminal justice system by compelling lawyers to function as whistleblowers, in violation of their traditional fiduciary duties of loyalty and attorney/client confidentiality (Shepherd 2009). A different view has been taken in the European Union, where the Third AML Directive has required member states, including the United Kingdom, to enact comprehensive AML regulation of the legal profession.

In 2006, Australia promised to apply the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) to DNFBPs, including lawyers, within one year of the legislation coming into force. This promise was given after lengthy consultation with the professions and other stakeholders. However, 10 years later, despite criticism by the FATF and another round of consultation following a statutory review of the AML/CTF legislation, the issue of AML regulation of DNFBPs does not seem to have become a priority of the government. In the report on the statutory review (Attorney-General's Department 2016: 151), there is a lukewarm recommendation that the government develop options for regulating DNFBPs and that this be carried out after a cost-benefit analysis of such options.

Effectiveness of AML regulation and the legal profession

Although 198 countries have agreed to apply the global AML standards, national implementation of the standards has been only modestly successful. The enforcement outcomes are also rather weak, as evidenced by the low number of money laundering prosecutions, the relatively small sums of illicit money that have been recovered and the continuing participation of financial institutions in money laundering, despite substantial fines (Government Accountability Office 2016: 11).

Whether a strategy that imposes comprehensive AML regulation of the legal profession will be any more successful in countering organised crime is questionable. However, whether AML regulation of lawyers produces valuable criminal intelligence, and whether the criminal justice benefits justify the violation of privacy and attorney–client confidentiality and compliance costs, are matters which require further examination. An empirical study of US money laundering prosecutions suggests that requiring mandatory suspicious transaction reporting would have little effect, in that any suspicious reporting regime could only possibly be of value in cases where lawyers unwittingly facilitate money laundering (Cummings & Stephnowsky 2010). In the sample study, only six of 123 cases consisted of lawyers who were unwitting dupes of money laundering, and more than 80 percent of these cases concerned real estate money laundering. The Cummings study makes the reasonable assumption that lawyers who are knowingly involved in money laundering will not file suspicious transactions reports. However, the Cummings study, which is based on a limited sample size, did not capture lawyers who were suspicious about their client activities but did not report them to the government because of professional ethical rules.

One problem is that there is a lack of awareness by lawyers of their vulnerability to organised crime, especially in countries which do not have an AML regime applicable to lawyers. The International Bar Association has suggested that there is a 'dangerous lack of awareness' by the legal profession of international crimes, such as corruption (International Bar Association 2011: 25), which is likely also to be applicable to money laundering. In a number of countries, such as the United States, there has been an attempt to increase the legal profession's knowledge of the risks of money laundering through education, ethical training and publications. The focus of such publications has been on informing the legal profession of the risk-based control and preventative measures that should be adopted to avoid being entangled in the illicit activities of their clients (Hudson 2013). The emphasis on client due diligence and ongoing monitoring of higher risk clients is intended to provide protection to lawyers from accusations that they have aided and abetted the criminal or fraudulent conduct of their clients, including money laundering (American Bar Association 2013). However, it is clear from the ethical rules in the United States and Australia that lawyers are not required to perform a gatekeeping role, in the sense of actively assisting the government by supplying financial intelligence, but rather, that lawyers should be better informed as to when they can resign from their mandate so as to avoid providing assistance to the illegal plans of their clients.

For those countries in the EU that have applied AML regulation to the legal profession in a comprehensive fashion, the evidence is inconclusive as to the practical effect of the regulation. There is a patchy record of compliance, in so far as there are large discrepancies between the number of suspicious reports filed by British lawyers, as compared to lawyers in Germany and France (Chaikin 2013; Walters et al. 2013). The PANA Committee of the European Parliament, which was established after the massive leakage of offshore financial information in the Panama Papers, suggested that lawyers, accountants and consultants had played a prominent role in 'design[ing] offshore structures and networks for their clients' which had the effect of facilitating money laundering, tax avoidance and tax evasion (PANA Committee 2017: 27). The PANA Committee did not critique the culpability of lawyers, and particularly where they were

placed along a 'continuum of culpability'—actual knowledge of the criminality, suspicion of criminality, or unknowing participation in the criminality (Smith 2013: 38; Victorian Law Reform Commission 2016: 36–43). However, the PANA Committee implicitly suggested that, whatever the culpability of the professional behaviour, self-regulation of the legal profession had failed in the prevention of money laundering. The PANA Committee's report found that lawyers in the EU had filed a low number of suspicious transaction reports (often in response to media reports), they were not subject to active supervision by their professional associations, and the risk of being debarred for misconduct was so low that there was no effective AML regulation of lawyers (PANA Committee 2017: 121–2). The European Parliament, in response to the PANA Committee report, recommended that the legal profession should be more closely monitored for AML purposes, be held 'legally co-responsible' when creating tax evasion and money laundering schemes for their clients, and 'systematically be liable for both penal sanctions and disciplinary measures' when participating in such schemes (European Parliament 2017).

Conclusion

There is an ongoing debate in Australia as to whether there should be comprehensive AML regulation of lawyers and other professional groups, with the Australian Government still considering this issue. At this stage, lobbying by the Law Council of Australia appears to have staved off increased AML regulation of lawyers in Australia. Although there are signs that AUSTRAC has become more aggressive in its AML enforcement stance by taking action against one of the leading banks in Australia, questions remain as to how the Australian Government may make more effective its use of AML regulatory tools to combat organised crime. The recent independent review of Australian intelligence agencies (PM&C 2017), and the creation of the Department of Home Affairs that brings together Commonwealth intelligence, security and law enforcement agencies in one administrative department, may see further attention being placed on this question in the years ahead.

References

URLs correct as at February 2018

American Bar Association (ABA) 2013. *Formal opinion 463: Client due diligence, money laundering and terrorist financing, Standing Committee on Ethics and Professional Responsibility, May 23*. Washington DC: ABA

Attorney-General's Department (AGD) 2016. *Report on the statutory review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations*. Canberra: AGD

Attorney-General's Department (AGD) 2015. *Consultation paper, Legal practitioners and conveyancers: A model for regulation under Australia's anti-money laundering and counter-terrorism financing regime*. Canberra: AGD

AUSTRAC 2017. *Annual report 2016–2017*. Canberra: AUSTRAC

AUSTRAC 2015. *Strategic analysis brief: Money laundering through legal practitioners*. Canberra: AUSTRAC

Australian Crime Commission (ACC) 2015. *Organised crime in Australia 2015*. Canberra: ACC

Australian Criminal Intelligence Commission (ACIC) 2016. *Organised Crime in Australia 2017*. Canberra: ACIC

Braithwaite J 2002. *Restorative justice and responsive regulation*. New York: Oxford University Press

Chaikin DA 2013. *Financial crime risks, globalisation and the professions*. North Melbourne: Australian Scholarly Publishing

Choo K-KR, Smith RG, Walters J & Bricknell S 2013. *Perceptions of money laundering and financing of terrorism in a sample of the Australian legal profession*. Research and public policy series no. 122(1). Canberra: Australian Institute of Criminology

Cummings LP & Stephnowsky PT 2010. *My brother's keeper: An empirical study of attorney facilitation of money laundering through commercial transactions*. University of Maryland Legal Studies Research Paper No 2010-32. http://dx.doi.org/10.2139/ssrn.1658604

Department of Prime Minister and Cabinet (PM&C) 2017. *Independent intelligence review*. Canberra: PM&C

European Parliament 2017. *Recommendation of 13 December 2017 to the Council and the Commission following the inquiry into money laundering, tax avoidance and tax evasion, P8_TA-PROV (2017) 0491*. Brussels: European Parliament

Financial Action Task Force (FATF) 2015. *Anti-money laundering and counter-terrorist financing measures - Australia, Fourth Round Mutual Evaluation Report. Sydney: FATF http://www.fatf-gafi.org/topics/mutualevaluations/documents/mer-australia-2015.html*

Financial Action Task Force 2012. FATF mandate 2012–2020. Paris: FATF

Financial Action Task Force 2008. *Risk-based approach guidance for legal professionals*. Paris: FATF

Government Accountability Office (GAO) 2016. *Financial institutions: Fines, penalties and forfeitures for violations of financial crimes and sanctions requirements*. GAO-16-297. Washington DC: GAO

Hudson Jr DL 2013. ABA endorses guidance for lawyers on fighting money laundering and terrorist financing. *American Bar Association Journal* 99 (Sept): 64–5

International Bar Association (IBA) 2011. *Risks and threats of corruption and the legal profession: Survey 2010. London: IBA*

Law Council of Australia (LCA) 2017. Response to Attorney General's Department consultation paper, legal *practitioners and conveyancers: A model for regulation under Australia's anti-money laundering and counter-terrorism financing regime*. Canberra: LCA

Moscow JW 2002. *Money laundering: A view from North America*. Address to the Financial Markets Group, London School of Economics, June. http://www2.lse.ac.uk/fmg/documents/specialPapers/2002/sp141.pdf

PANA Committee 2017. *Report of the committee of inquiry to investigate alleged contraventions and maladministration in the application of Union Law in relation to money laundering, tax avoidance and tax evasion. 2017/2013 (INI)*. Brussels: European Parliament

Reuter P & Truman EM 2004. *Chasing dirty money: The fight against money laundering*, Washington DC: Peterson Institute for International Economics

Shepherd KL 2009. Guardians at the gate: The gatekeeper initiative and the risk-based approach for transactional lawyers. *Real Property, Trust and Estate Law Journal* 43: 607–71

Smith RG *2013.* Anti-money laundering: The accounting and legal professions, in Chaikin D (ed), *Financial crime risks, globalisation and the professions*. North Melbourne: Australian Scholarly Publishing: 28–40

Victorian Law Reform Commission 2016. *Use of regulatory regimes in preventing the infiltration of organised crime into lawful occupations and industries*. Melbourne: Victorian Law Reform Commission.

Walters J, Chadwick H, Choo K-KR & Smith RG 2013. *Industry perspectives on money laundering and financing of terrorism risks in non-financial sector businesses and professions*. Research and public policy series no. 122. Canberra: Australian Institute of Criminology.

Chapter 15: Third party co-production of cybersecurity

Lennon YC Chang, Lena Y Zhong and Peter Grabosky

Governmental agencies of social control are neither omnipresent nor omnipotent, and this has created a demand for supplementary policing and security services. As a consequence, the past half-century has seen widespread enthusiasm for citizen 'co-production' of policing services in the terrestrial world, typified by such institutions as Neighbourhood Watch, and the 'responsibilisation' of ordinary members of the public (Bennett, Holloway & Farrington 2008; Garland 1994). While much of this activity is actively encouraged by law enforcement agencies, circumstances have arisen in which citizen co-production has resulted in adverse and unintended consequences. Other forms of citizen crime control activity have occurred beyond state auspices, some in blatant defiance of the law. The long history of lynching and vigilante activity in the United States is but one example (Brown 1969; Garland 2005). As Donald Black (1976) observed, law varies inversely with other social control.

Co-production is by no means confined to terra firma. Since the dawn of the digital age, the insecurities of cyberspace have become increasingly apparent. Moreover, the resources and capacities of states to patrol cyberspace are, arguably, even more constrained than those available in the terrestrial world (Broadhurst & Chang 2012). The prevailing cybersecurity shortfall has been met with a variety of co-production efforts by individuals or by collectives of varying degrees of organisation and coordination. As is the case with the terrestrial analogue, not all of this activity is welcome, nor are the actors always accountable for their conduct.

Although the concept of security co-production has been widely examined in the terrestrial world, there is still limited research addressing co-production of cybersecurity. This chapter aims to alleviate this imbalance by categorising examples of citizen co-production in cybersecurity and differentiating those which appear successful from those which are counterproductive. It will conclude by offering some principles by which co-production might be constructively undertaken.

Citizen responses to cybercrime

Private citizens encounter illegal online activity on a regular basis. Most, if not all, readers will have received an advance fee fraud solicitation or a 'phishing' overture under the guise of a message from a financial institution requesting confirmation of their password and account number. Today, the volume of illegal activity in cyberspace generates more business than governments can handle (Ellyatt 2016). Many individuals and organisations are aware of the lack of state capacity and have sought to fill this vacuum. Not all of this non-state response to cybercrime occurs within the boundaries of the law. One may therefore ask, what are the limits of citizen co-production in cyberspace?

Private citizens, commercial entities and non-profit organisations alike may all be in a position to identify apparent incidents of online illegality and to report them to the authorities. Some may be able and willing to investigate and report the incident as well (Chang 2012). These responses may be motivated by self-interest, by concern for the wider public good or by some combination of the two. In some circumstances, the response may be entirely legal; in others, it may not. The categories differentiate conceptually between unilateral co-production activity and that in which states may be involved as sponsors, coordinators or facilitators.

Identification/investigation of illegality occurring against one's own resources

One of the first 'private investigators' of cybercrime was Clifford Stoll. Back in the 1980s, when he was working as an astronomer at the Lawrence Berkeley Laboratories, Stoll was asked to reconcile a small discrepancy in the accounts of the labs' computer centre. In the course of his investigation, it became apparent to him that someone had obtained unauthorised access to the labs' computer system. When he brought this to the attention of law enforcement agencies, they were initially uninterested. Only when he found that the intruder was a German national seeking access to other defence-related computer systems in the United States did government authorities become involved (Stoll 1989).

Since then, private individuals and institutions have been frequently involved in investigations of alleged cybercrimes and in repairing the damage caused, especially when their own systems have been compromised and/or when their own expertise can make a material contribution to the investigative effort (Shimomura & Markoff 1996). In some cases, matters may be referred to a law enforcement agency. In others, the victim may simply seek to stop the intrusion or to mitigate its impact by engineering a 'fix' or 'patch' or by reinstalling the computer's operating system and enhancing system security.

Identification/investigation of illegality occurring in a public (publicly accessible) place

Some citizens patrol the public areas of cyberspace, looking for indicia of illegality. Alternatively, they can encounter crime by happenstance, in the course of 'surfing the web' or in an internet chatroom. For example, Thompson (2009) notes that volunteer groups monitor botnets and maintain blacklists of spam (see www.spamhaus.org). Similar cases can regularly be seen in the Greater China region (Chang & Leung 2015). It is called 'renrou sousou' in Chinese, literally human flesh search or internet vigilantism (netilantism). While some might participate in the netilantism for fun, Chang and Poon (2017) argue that netilantes (internet vigilantes) possess the highest level of self-efficacy in the cyberworld, perceive the criminal justice system as ineffective and perceive netilantism as achieving social justice effectively.

Invited/parallel co-production

Citizens may also be encouraged or invited by governments to engage in hacking activity or other online activities in furtherance of public policy—or states may simply monitor private co-production activities. In the People's Republic of China, some netizens are 'hired' by local and central governments to write commentaries and create blogs and other online platforms to shape or sway public opinion. These hired commentators are called the '50 Cents Party' because they supposedly earn 50 cents Renminbi for every post. It was estimated that, in 2014, there were between 250,000 and 300,000 'members' of this 'party' (Sterbenz 2014). Invited co-production can also be seen in laws and regulations which encourage the reporting of computer incidents. Such information can then be analysed and disseminated to other institutions as a pre-warning scheme (Chang 2012).

Mandated co-production

Private organisations or individual citizens may be commanded by law to assist in law enforcement or criminal investigation (Ayling, Grabosky & Shearing 2009). In most jurisdictions, banks and other financial institutions have a legal obligation to report transactions over a certain threshold or those of a suspicious nature to specified government authorities. Members of certain professions, such as doctors, nurses, teachers and social workers, are required to report suspected cases of child abuse and/or neglect.

Similar requirements may also exist in relation to cybercrime, including matters relating to national security. In many jurisdictions, critical infrastructure related institutions, such as banks and telecommunication companies, are required by law and regulation to report computer incidents to government authorities. Internet service providers (ISPs) may be required to retain metadata (details of the origin and destination of all communications), in case it might be needed in the course of a criminal investigation. ISPs and computer repair technicians who become aware of child pornography on a customer's system may be required to report this to the authorities in their jurisdiction. Mandatory reporting of suspected terrestrial criminality raises the issues of system capacity; there may be more cases than an investigative agency can reasonably cope with, given its available resources.

Covert investigations

Private actors may engage in covert investigations of a passive or active nature. Deceptive practices, often entailing entrapment, may be undertaken in order to identify offenders. This can involve the creation of 'honeypots' or decoy sites to target prospective offenders (Tuovinen & Röning 2007). These have been shown to be effective lures in the domain of online child exploitation (Jayawardena & Broadhurst 2007). It can also involve more active engagement with prospective offenders, in order to lure them into incriminating situations. A number of citizens' organisations work with police to identify online pedophiles. Huey, Nhan and Broll (2013) reported a case of an English grandmother who came across a participant in an online forum who was encouraging others to commit suicide. Posing as a person with suicidal thoughts, she engaged the person online and provided his contact details to the police in St Paul, Minnesota, where he resided. Police investigations led to criminal charges, and the suspect was convicted of aiding the suicide of two individuals.

There are also private investigations which may not necessarily lead to police investigation. Private investigators, such as Predator Hunting (http://huntingapredator.com/) and Letzgo Hunting (http://letzgohunting.co.uk), use their own methods to punish online pedophiles, mainly by naming and public shaming. Information about the alleged offender, including the profile, the text of the online conversation and voice recordings, were posted on the website Predator Hunting as well as on YouTube.

Downside risks of co-production of security against cybercrime

Mistake

Grabosky (1992) noted that terrestrial vigilantes were often mobilised to achieve deplorable ends, and their sanctions were irrevocable. Irrevocability may also characterise counter-hacking cases. One of the great barriers to effective counter-hacking is the difficulty of attribution, in other words, determining the source of an attack. Ideally, one should be certain of the location of the offending machine, the identity of its owner and the person actually responsible for the offending conduct. However, precise attribution is easier said than done. To cite but one example, Carr (2012) observed that a distributed denial of serviceattack on servers in South Korea in July 2009, suspected of originating in North Korea, was traced to Miami, Florida. If the South Korean government launched retaliation against the proximate source of the attack, it would cause damage to the company which owns the server in Florida, instead of the real attacker. Skilled hackers can mask their activities by 'impersonating' another system, using 'spoofing' skills or simply using the Tor network to facilitate anonymous communication. Hackers can also sequence their activity through a chain of otherwise 'innocent' computers that have been commandeered for the purpose.

Collateral damage

An indiscriminate response to a distributed denial of service attack may inadvertently disable an intermediate computer (or zombie) that was used in the attack. Depending on the zombie's location and normal function, its disabling may disrupt systems supporting government, critical infrastructure or other important services (Karnow 2005: 93). Counter-attacks can also go astray because of the vagaries of the internet. As packets of information travel from computer A to computer B, they may pass through a large number of intermediate locations, which may vary significantly in terms of robustness. Allison (2003) relates how a British teenager, allegedly intending to harass a chatroom user in the United States, inadvertently disrupted computer systems at the Port of Houston, Texas.

Apparent condonation encourages emulation

Vigilantes take justice into their own hands and believe that they are entitled to punish criminals by illegal means. However, if the state condones, or fails to take action against, illegal behaviour on the part of its citizens, even when such activity is undertaken in furtherance of crime control, it sends a questionable message to the public. Citizens are implicitly encouraged to take the law into their own hands. Some might be tempted to conclude that committing a crime is acceptable, or that the end justifies extreme means.

Erosion of legitimacy

State tolerance of private illegality may further erode the state's own legitimacy. It may be seen as taking on an aura of criminality in its own right, and any moral authority it may have commanded is at risk of dilution. Most private investigation or vigilantism commences when people believe that the government is incapable of dealing with the problem. Therefore, they choose to use their own methods to achieve justice. This is especially obvious in cases related to online child-predators. When some of these investigations end up as co-productions with official security and crime investigation authorities, they imply that governments were not able to deal with the problem. In such circumstances, states subtly invite or tolerate vigilante activity.

Lack of accountability by unilateral actors

The term 'electronic frontier' brings to mind the practices of informal justice in the 'Wild West' of nineteenth century America (and in other pre-industrial societies), where disputes were settled by duelling, and criminal acts were met with reciprocity. The 'law of the gun' often led to personal values and private interests trumping objective justice. We have seen that there are similar private actors engaging in cybercrime unilaterally, in order to protect their own interests. Rather than place themselves at legal risk, some have sought indemnification by means of a 'licence to hack' under the laws of self-defence or nuisance abatement (Karnow 2005). However, co-producers of cybersecurity may feel free to advance their own priorities, even when these personal priorities may be inconsistent with public policy. Those who object strongly to some practice that is legally permissible may be inclined to act on their beliefs to the extent of engaging in criminality.

Those who embrace the principle that all information should be free will be tempted to punish those who have a proprietary interest in such information. Individuals who deem certain institutions to be impediments to justice are not always troubled by legal niceties. The group known as Anonymous attacked not only websites hosting illicit images of children, but also those of the US Department of Justice. Terrestrial analogues are too numerous to canvass in this essay. From the Great Proletarian Cultural Revolution in China to the culture of lynching in the United States, self-help has subverted the rule of law.

Interference with ongoing law enforcement operations

Another significant risk is that citizen co-production can contribute to the failure of a criminal investigation. In those jurisdictions where the rule of law matters, a proper criminal investigation entails very exacting procedures. Incompetent private sleuths may contaminate a crime scene and corrupt electronic evidence. An obtrusive citizen-investigator may inadvertently alert an offender to the fact that he or she is being 'followed'. Or they may simply make life difficult for the police by getting underfoot. Michaels (2010) notes that vigilante disabling of extremist websites has occasionally disrupted intelligence collection by state agencies who were engaged in careful monitoring of the sites prior to their takedown. This problem is not unique to citizen co-production. In places where jurisdictional authority overlaps, different law enforcement agencies may get in each other's way.

Further erosion of privacy

Gary Marx (2016) noted the refinement and the proliferation of surveillance technology and the increasing potential for serious violations of rights to privacy. In particular, he warned of the risks associated with the proliferation of technologies of surveillance (eg miniature cameras, bugs, tape recorders and computer databases). He argued that such modern technologies have served to 'democratize surveillance' and enabled private citizens to easily engage in eavesdropping behaviours (either legally or illegally) once undertaken solely by state authorities (Marx 2016). Since then, the capacity of such technology has increased, while the cost has decreased even further. Vision recorded on a mobile phone can now be disseminated around the world instantly and at negligible cost. The risks to individual privacy are without precedent in the modern era (Ong 2012), as CCTV camera images from all over the world can be broadcast live at www.anqiaoqiao.com, a domain maintained in China. As was the case with private terrestrial surveillance a century ago, the democratisation of digital surveillance may invite otherwise passive citizens to become righteous intruders. In addition, it may increase public tolerance for even more intensive surveillance by state agencies (Fronc 2009).

Concluding remarks: principles and safeguards

What orderings are most appropriate to bring about responsible co-production of cyberspace security? One might begin by suggesting that states should emphasise prevention and defence by citizens rather than vigilante pursuit of law-breakers. States should build platforms for information sharing. This co-production of security is already happening between government and big IT companies such as Microsoft, but there is less co-production with individual

vigilantes or vigilant groups such as Duri.net or Predator Hunting. Once the information is received, law enforcement agencies should work together with vigilant netizens, build trust and gain the confidence of netizens by arresting criminals. That is, for example, the Russian Government should collaborate with Duri.net to arrest child-predators rather than leaving them vulnerable to physical abuse by vigilantes. Once justice is realised, it may reduce the incentive to break the law in order to enforce it.

As Donald Black (1983) illustrates, the crime of self-help is usually treated leniently or with impunity. Vigilantes' behaviour tends to be punished less than that of the offender. Internet vigilantes might not be afraid of being punished by the law. As there will be no complaint, they believe that they have the right to do what they are doing and that the state will not take action against them. Even if there is a complaint, the individual cyber vigilante's behaviour seems tolerable when it comes to public shaming and naming online of paedophiles and drug dealers. Paradoxically, these collective individual behaviours often amount to more severe and longer lasting sanctions against the criminals than the law would have imposed if enforced.

Obviously the state and its officials would be well advised to avoid words or deeds that appear to condone or to encourage extralegal activity, even when the motives for such activity may be laudable. One might imagine a legal framework that reinforces this principle: Shah (2005) suggests that evidence derived from illegal private searches be inadmissible in the United States. The legal basis for hacking in self-defence is problematic (Thompson 2009; Kesan & Hayes 2011). Cybercrime laws tend to be broad in scope and devoid of exceptions and qualifications. This is perhaps as it should be.

When the state engages with private actors, the engagement should be achieved within strict guidelines and procedures. This can entail formal agreements or a contractual framework (Gabbatt 2010). Where there is a risk of misconduct, co-producers may be required to undergo a degree of training (Winters 2009). We suggest that education on law and ethics should be provided to netizens. In any event, states should not shrink from the obligation to reaffirm the rule of law.

In the contemporary terrestrial world, examples of overzealous investigation and prosecution by officers of the state are all too common. One need hardly suggest that private actors, too, may become overzealous in the protection of their interests, to advance their ideology or to exact vengeance.

But where state capacity to control cybercrime is limited, the socially and economically marginalised may suffer, directly or indirectly, no less than the privileged among us. A degree of citizen involvement in securing cyberspace can thus be useful. Successful co-production of cyber security has been demonstrated in this article, but the potential for overzealous reactions by the citizenry, which may be more self-serving than public regarding, is very real. Collective actions by netizens might impose more severe sanctions on the criminal than would the law. The globalisation of cybercrime and the increasing penetration of digital technologies into Asia may see the 'Wild East' join, if not eclipse, the 'Wild West' as a source of online criminality. Regardless of location, it is important to establish criteria for evaluating the appropriateness of citizen co-production in cybersecurity, no less than in terrestrial security.

Although crime can serve as a kind of social control, to condone criminal activity, even in furtherance of truly worthy ends, weakens the rule of law to some extent. One hesitates to suggest that 'noble cause' is universally wrong. But it should not be uncritically embraced as a solution to limited state capacity.

Responsible co-production within the bounds of the law should be encouraged, but activities of private citizens/netizens should be closely circumscribed. The closer that private activity gets to the limits of legality, the greater the risks to the state itself. One might also consider the costs of encouraging a nation of spies and informers, much less those who lure their fellow citizens into compromising situations for the purpose of shaming or of mobilising the law. The suggestion that 'privacy is dead' (Rauhofer 2008) heralds a society where speech, movement and social interaction may be irrevocably chilled.

Acknowledgements

This chapter is a condensed version of the lead author's previously published article written with co-authors Lena Y Zhong and Peter N Grabosky: (2018) 'Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime', Regulation & Governance. 12: 101–14. It is published with permission of the previous publisher.

References

URLs correct as at February 2018

Allison R 2003. Hacker attack left port in chaos: Busiest US port hit after Dorset teenager allegedly launched electronic sabotage against chatroom user. *The Guardian*, 7 October., http://www.guardian.co.uk/technology/2003/oct/07/usnews.uknews

Ayling J, Grabosky P & Shearing C 2009. *Lengthening the arm of the law: Enhancing police resources in the twenty-first century*. Cambridge: Cambridge University Press

Bennett T, Holloway K & Farrington D 2008. *The effectiveness of neighborhood watch. Campbell Collaboration Systematic Review*. Oslo: the Campbell Collaboration

Black D 1983. Crime as social control. *American Sociological Review* 48(1): 34–45

Black D 1976. *The behavior of law*. New York: Academic Press

Broadhurst R & Chang LYC 2012. Cybercrime in Asia: trends and challenges, in Hebenton B, Shou SY & Liu J (eds), *Asian handbook of criminology*. New York: Springer: 49–64

Brown RM 1969. The American vigilante tradition, in Graham HD & Gurr TR (eds), *The history of violence in America*. New York: Bantam: 154–226

Carr J 2012. *Inside cyber warfare, 2nd ed*. Sebastopol: O'Reilly Media

Chang LYC 2012. *Cybercrime in the greater China region: Regulatory response and crime prevention across the Taiwan Strait*. Cheltenham: Edward Elgar

Chang LYC & Leung KH 2015. An introduction to cyber-crowdsourcing (Human Flesh Search) in the Greater China Region, in Smith R, Chueng RY & Lau L (eds), *Cybercrime risks and responses: Eastern and western perspectives*. Hampshire: Palgrave Macmillan: 240–52

Chang LYC & Poon R 2017. Internet vigilantism: Attitudes and experiences of university students toward cyber crowdsourcing in Hong Kong. *International Journal of Offender Therapy and Comparative Criminology* 61(16): 1912–32

Ellyatt H 2016. *The 2016 trends in cybercrime that you need to know about*. CNBC, 28 September. https://www.cnbc.com/2016/09/28/the-2016-trends-in-cybercrime-that-you-need-to-know-about.html

Fronc J 2009. *New York undercover: Private surveillance in the progressive era*. Chicago: University of Chicago Press

Gabbatt A 2010. Google teams up with National Security Agency to tackle cyber attacks: Internet groups fear alliance means US government could access personal information. *The Guardian*, 5 February. http://www.guardian.co.uk/technology/2010/feb/05/google-national-security-agency-cyber-attack

Garland D 2005. Penal excess and surplus meaning: Public torture lynchings in twentieth-century America. *Law & Society Review* 39(4): 793–834

Garland D 1994. The limits of the sovereign state: Strategies of crime control in contemporary society. *British Journal of Criminology* 36(4): 445–71

Grabosky P 1992. Law enforcement and the citizen: Non-governmental participants in crime prevention and control. *Policing and Society* 2(4): 249–71

Huey L, Nhan J & Broll R 2013. Uppity civilians and 'cyber-vigilantes': The role of the general public in policing cyber crime. *Criminology and Criminal Justice* 13(1): 81–97

Jayawardena KP & Broadhurst R 2007. Online child sex solicitation: Exploring the feasibility of a research 'sting'. *International Journal of Cyber Criminology* 1(2): 228–48

Karnow C 2005. Launch on warning: Aggressive defense of computer systems. *Yale Journal of Law and Technology* 7(1): 87–102

Kesan JP & Hayes C 2011. *Self defense in cyberspace: Law and policy*. Illinois Public Law Research Paper No. 11–16. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1979857

Marx GT 2016. *Windows into the soul: Surveillance and society in an age of high technology*. Chicago: University of Chicago Press

Michaels J 2010. Deputizing homeland security. *Texas Law Review* 88: 1434–73

Ong R 2012. Online vigilante justice Chinese style and privacy in China. *Information and Communications Technology Law* 21(2): 127–45

Rauhofer J 2008. Privacy is dead, get over it! Information privacy and the dream of a risk-free society. *Information & Communications Technology Law* 17(3): 185–97

Shah M 2005. The case for a statutory suppression remedy to regulate illegal private party searches in cyberspace. *Columbia Law Review* 105(1): 250–78

Sterbenz C 2014. China hires as many as 300,000 Internet trolls to make the communist party look good. *Business Insider*, 18 October. http://www.businessinsider.com.au/chinas-50-cent-party-2014-10

Stoll C 1989. *The cuckoo's egg*. NY: Pocket Books

Shimomura T & Markoff J 1996. *Takedown*. NY: Hyperion

Thompson T 2009. Terrorizing the technological neighborhood watch: The alienation and deterrence of the 'white hats' under the CFAA. *Florida State University Law Review* 36: 537–84

Tuovinen L & Röning J 2007. Baits and beatings: vigilante justice in virtual communities, in Hinman L, Brey P, Floridi L, Grodzinsky F & Introna L (eds), Proceedings of CEPE 2007. The 7th international conference of computer ethics: Philosophical Enquiry. Enschede: Center for Telematics and Information Technology: 397–405

Winters C 2009. Cultivating a relationship that works: Cyber-vigilantism and the public versus private inquiry of cyber-predator stings. *University of Kansas Law Review* 57(2): 427–60

AIC reports

Research Report

Australia's national research and knowledge centre on crime and justice

aic.gov.au