AUSTRALIA

Parliamentary Joint Committee on Law Enforcement

Impact of new and emerging information and communication technology

April 2019

ISBN 978-1-76010-951-6

Printed by the Senate Printing Unit, Parliament House, Canberra.

Joint Committee on Law Enforcement

Members

Mr Craig Kelly MP	LP, NSW (Chair)
Senator the Hon Lisa Singh	ALP, TAS (Deputy Chair)
Senator the Hon Eric Abetz	LP, TAS
Dr Anne Aly MP	ALP, WA
Senator Jane Hume	LP, VIC (from 10.9.18)
Senator the Hon Kristina Keneally	ALP, NSW (from 15.2.18)
Mr Llew O'Brien MP	NATS, QLD
Ms Clare O'Neil MP	ALP, VIC
Mr Jason Wood MP	LP, VIC

Former Members

Senator David Bushby	LP, TAS (from 17.10.17 to 5.2.18)
Senator the Hon Richard Colbeck	LP, TAS (from 12.2.18 – 10.9.18)
Senator the Hon Don Farrell	ALP, SA (from 23.11.16 – 15.2.18)
Senator Skye Kakoschke-Moore	NXT, SA (from 7.2.17 – 22.11.17)
Senator Barry O'Sullivan	NATS, QLD (from 3.10.17 – 12.2.18)

Secretariat

Ms Sophie Dunstone, Secretary
Mr Michael Sloane, Principal Research Officer (until 20.10.17)
Ms Cathy Nembu, Acting Principal Research Officer (until 21.1.19)
Dr Joy McCann, Senior Research Officer (until 21.3.19)
Mr Joshua Wrest, Senior Research Officer
Ms Jo-Anne Holmes, Administrative Officer (until 11.1.19)
Ms Sofia Moffett, Administrative Officer (from 14.1.19)

PO Box 6100
Parliament House
CANBERRA ACT 2600
Telephone: (02) 6277 3419
Email: le.committee@aph.gov.au
Internet: www.aph.gov.au/le_ctte

Table of contents

Definitions

5G	The next cellular communications standard in development to replace existing 4G technology. Most commonly associated with providing wireless internet services to electronic devices. 5G is predicted to be in common use by 2020.[1]
Artificial intelligence (AI)	The simulation of intelligence processes by machines, especially computer systems.
Australian Cybercrime Online Reporting Network (ACORN)	An Australian government initiative to provide information to the public on how to identify cybercrime and methods of mitigating the risk of being affected by common cybercrime.
Backdoor	A means to access a computer system or encrypted data that bypasses the system's customary security mechanisms.
Bitcoin	A digital currency and payment system underpinned by blockchain technology. Bitcoins can be used for online purchases, or converted into traditional currency.
Blockchain	A distributed database that maintains a continuously growing list of records, called blocks, secured from tampering and revision.
Botnet	'Backdoors' are a category of malware that enable a cybercriminal to remotely control an infected computer over a network. Such an infected computer is often called a robot or ‘bot’ computer. When several computers are infected with a backdoor and become bots, they can be simultaneously controlled from a single remote mechanism. These remotely controlled networks of bot computers are known as ‘botnets’.
Cloud computing	Provides for storing and potential processing of data offsite from a person's or entity's main premises.
Computer Network Operation (CNO)	A form of extraterritorial police activity used to investigate the 'dark web'.
Critical infrastructure	Critical systems, services and facilities underpinning the operation of society and the economy, such as electricity and transportation networks, water services, healthcare systems and banking.

[1] Department of Home Affairs (DHA), Australian Border Force (ABF) and Attorney-General's Department (AGD), *Submission 28*, pp. 3−4.

Cryptocurrency	A form of digital currency where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds.
Cybercrime	Cybercrime relates to criminal activities carried out by means of computers or via the internet. Cybercrime is also referred to as 'computer crime'. It encompasses a wide range of criminal activities encompassing: (a) crimes where computers or other ICTs are an integral part of an existing offence (such as online fraud or online child sex offences); and (b) crimes directed at computers or ICTs (such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software).[2]
Cyber security	Broadly encapsulates measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.[3]
Dark web	The dark web is made up of sites that are not indexed by search engines and are only accessible through specialty networks such as Tor. Often, the dark web is used by website operators who want to remain anonymous. The ‘dark web’ is a subset of the ‘deep web’.
Deep web	The part of the internet that is not indexed by search engines. Includes websites that are password-protected and pay walled, encrypted networks and databases, and dynamic data such as social media feeds. Also includes the dark web.
Digital currency	A digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status.
Digital evidence	Also called 'electronic evidence'. Any information stored or transmitted in digital form that a party to a court case may use at trial.[4]

[2] 'Cybercrime', Australian Criminal Intelligence Commission (ACIC), updated 17 July 2018, https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime (accessed 16 January 2019).

[3] Australian Government, *Australia's International Cyber Engagement Strategy*, Barton, ACT, 2017, p. 23.

[4] International Association of Prosecutors—Global Prosecutors E-Crime Network (GPEN), *Submission 19*, p. 4.

Encryption	The conversion of electronic plaintext data into unreadable cipher text using algorithms. Encryption protects the confidentially of data at rest and in transit. Both encryption and decryption are functions of cryptography.
End to end encryption	A method of secure communication where only the communicating users can read data transferred from one end system or device to another.
Going dark	A term often used by users of social media to describe situations where digital communications that appear to have ceased are moved from the public sphere into a private communication channel that prevents others from monitoring it.
Hacking	‘Hacking’ is a term with multiple meanings. It can refer to testing and exploring computer systems, highly skilled computer programming or the practice of accessing and altering other people’s computers. Hacking may be carried out with honest aims or with criminal intent.
Five Eyes Alliance	An intelligence alliance involving the United Kingdom, United States, Canada, Australia and New Zealand.
Information and communications technology (ICT)	Any device that can process, store or communicate electronic information.
Internet	The global system of interconnected computer networks that use standardised communication protocols to link devices and provide a variety of information and communication facilities.
Internet of Things (IoT)	A term to describe the way in which the internet is transforming the way in which people work, live and play by combining internet connectivity and data analytic capabilities with consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects.[5]
Internet Protocol (IP)	The technology that allows computers and other electronic devices to connect to the internet.
Malware	Malware is a general term used for software designed to damage or subvert a computer or information system.

[5] 'The Internet of Things (IoT): An Overview', Internet Society, https://www.internetsociety.org/resources/doc/2015/iot-overview?gclid=EAIaIQobChMI9Zqf0siC4AIVFR4rCh3hPwVVEAAYAyAAEgL_gPD_BwE (accessed 23 January 2019).

Mesh network	A wireless mesh network combining multiple routers into a single and larger local network.
Mutual Legal Assistance Treaty (MLAT)	An agreement between governments to facilitate the exchange of information relevant to an investigation in at least one of those countries.
Network Investigation Technique (NIT)	A form of extraterritorial police activity used to investigate the 'dark web'.
Silk Road	A now defunct illicit marketplace located on the dark web.
Technology-enabled crime	The use of computers or other ICTs to commit or facilitate the commission of traditional crimes.[6]
Telephone interception (TI)	TI 'consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication'.[7]
The Onion Router (Tor)	Free software used to anonymise access to the internet by routing data through multiple anonymised networks, allowing users to mask their usage and location. It is the most commonly used means to access the dark web.
Virtual Private Network (VPN)	An encrypted communication that creates a safe connection between a device and a network over a less secure network.

[6] 'Cyber crime', Australian Federal Police, https://www.afp.gov.au/what-we-do/crime-types/cyber-crime (accessed 21 January 2019).

[7] *Telecommunications (Interception and Access) Act 1979 (Cth)*, section 6(1).

Recommendations

Recommendation 1

3.86 The committee recommends that the National Cybercrime Working Group examines and reports on the merits of the following initiatives as part of its work developing a new National Plan to Combat Cybercrime:

- **a national statutory framework for Delayed Notification Search Warrants for serious crime and corruption offences;**
- **a framework for an Indicators and Warning system, to sit within the ACIC, aimed at identifying disruptive changes in the global illicit supply chains that impact on Australia's market;**
- **an independent entity to review current case categorisation and prioritisation models used by agencies within the Home Affairs Portfolio; and**
- **a review of how existing law enforcement strategies to tackle activities facilitated by the dark web, such as that used to close Silk Road, can be enhanced for wider application.**

Recommendation 2

4.52 The committee recommends that the Australian government considers establishing a task force comprising information and communications technology (ICT), legal, law enforcement and security experts, including from academia, to:

- **monitor the development, and examine and advise on the impact of new and emerging ICTs on Australian law enforcement;**
- **identify specific gaps and vulnerabilities in the current legislative and regulatory frameworks that may be limiting the ability of Australian law enforcement agencies to investigate, disrupt or otherwise deal with cybercrime, including encryption services and encrypted devices;**
- **consult and advise on the balance between investigatory powers to tackle cybercrime and their impact on civil rights and liberties;**
- **report to the Australian government at regular intervals on the appropriateness of current legislative and regulatory frameworks; and**
- **recommend any changes that may be necessary to ensure that law enforcement agencies are keeping pace with and capable of tackling new cyber challenges as they arise.**

Recommendation 3

5.97 The committee recommends that the Australian government evaluates the current Mutual Legal Assistance Treaty process and identifies:

- **how the process might be modified to better suit the investigation of cybercrimes and the information and communications technology challenges facing law enforcement; and**
- **opportunities to implement those modifications with treaty partners.**

Recommendation 4

5.101 The committee recommends that the Australian government explores a range of approaches for improving the information and communications technology (ICT) skills and capabilities of the law enforcement workforce, including:

- **engaging volunteer experts, similar to the United Kingdom (UK) National Crime Agency Specials program;**
- **establishing 'single points of contact' within law enforcement agencies, similar to the approach adopted in the UK;**
- **implementing a single Commonwealth-led cooperative entity, providing expert cybercrime investigative support services to government, national security and law enforcement agencies; and**
- **establishing ICT cadetship programs for the recruitment of talented university students.**

Recommendation 5

5.105 The committee recommends that the Australian government explores suggestions from law enforcement agencies and cybersecurity experts for improving information and communications technology (ICT) capabilities and resources, including:

- **dedicated agency funding with sufficient flexibility to enable law enforcement agencies to respond to the escalating challenges of cybercrime; and**
- **improving the model of ICT procurement and project management to promote new and emerging ICT for operational purposes.**

Recommendation 6

5.109 The committee recommends the Australian government considers the use of hybrid storage strategies, artificial intelligence and other advanced techniques for sorting, filtering and analysing large volumes of data.

Recommendation 7

5.111 The committee recommends that the Australian government takes the following into account when developing any future strategies for biometric data and facial recognition systems:

- **the development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security;**
- **the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities; and**
- **publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.**

Recommendation 8

5.114 The committee recommends that the Australian government reviews current consumer protection laws and regulations in relation to internet-enabled devices and identifies changes that may be required to provide adequate and timely consumer protection in relation to the risks they pose.

Recommendation 9

5.118 The committee recommends that Australian governments review legal mechanisms intended to protect victims, such as Apprehended Violence Orders, to ensure that they offer adequate protection to victims of crime facilitated by internet-enabled devices.

Recommendation 10

5.119 The committee recommends that the Australian government develops education materials to inform law enforcement agencies and personnel about new and emerging information and communications technologies that offenders may use to facilitate family and domestic abuse, and to provide guidance on appropriate strategies for responding to such situations.

Recommendation 11

5.122 The committee recommends that the Australian government develops and implements an Internet of Things (IoT) public awareness campaign that:

- **raises awareness about the potential vulnerabilities of internet-enabled devices and the IoT; and**

- **provides guidance to consumers about how to protect their privacy when using internet-enabled devices or the IoT, and information about how to access online help.**

Recommendation 12

6.50 The committee recommends that the National Plan includes, as a key priority area, ways to better coordinate intelligence gathering, data analytics, data management and investigative support services across Australian jurisdictions and agencies in order to ensure that law enforcement in Australia is able to keep pace with the rapid pace of technological change in digital communications.

Recommendation 13

6.53 The committee recommends that the Australian government considers implementing the INdata Cooperative Research Centre to address the common big data and information data sharing needs of law enforcement agencies and explores other opportunities for improving information and intelligence-sharing between law enforcement agencies in all Australian jurisdictions.

Recommendation 14

6.57 The committee recommends that the Australian government considers reviewing the *Telecommunications (Interception and Access) Act 1979* and *Surveillance Devices Act 2004* and amending them as necessary to ensure that they are technology neutral and an effective legal mechanism for meeting the telecommunications interception needs of law enforcement agencies.

Recommendation 15

6.59 The committee recommends that the Australian government explores opportunities for greater engagement and partnerships with the private sector to facilitate the exchange of information and communications technology expertise and the development of novel approaches to tackling cybercrime.

Chapter 1

Introduction

Referral and conduct of the inquiry

1.1 On 18 October 2017, the Parliamentary Joint Committee on Law Enforcement initiated an inquiry into the impact of new and emerging information and communications technology on law enforcement.

1.2 Pursuant to subsection 7(1) of the *Parliamentary Joint Committee on Law Enforcement Act 2010*, the committee examined the impact of new and emerging information and communications technology (ICT) with particular reference to:

(a) challenges facing Australian law enforcement agencies arising from new and emerging ICT;

(b) the ICT capabilities of Australian law enforcement agencies;

(c) engagement by Australian law enforcement agencies in our region;

(d) the role and use of the dark web;

(e) the role and use of encryption, encryption services and encrypted devices; and

(f) other relevant matters.

1.3 The committee invited submissions from interested organisations, individuals and government bodies. The committee received 35 submissions. A list of public submissions, together with other information authorised for publication is provided at Appendix 1.

1.4 The committee held public hearings in Canberra on 29 March 2018 and 11 May 2018. The witnesses who appeared at the public hearings are listed at Appendix 2.

1.5 The committee thanks the organisations and individuals that made written submissions, and those who gave evidence at the public hearings.

Structure and scope of this report

1.6 This report is divided into six chapters.

1.7 This chapter broadly considers the new and emerging ICT landscape and provides an overview of some key ICTs.

1.8 Chapter 2 discusses the coordination of international and Australian law enforcement and key issues to be considered in addressing cybercrime across jurisdictions.

1.9 Chapter 3 considers the nature and uses of the 'dark web', including encryption, and the challenges it poses for law enforcement.

1.10 Chapter 4 examines recent legislative reforms in relation to new and emerging ICTs, including the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

1.11 Chapter 5 discusses operational challenges as well as the workforce and ICT vulnerabilities that affect Australian law enforcement's capabilities.

1.12 Chapter 6 considers strategic responses and opportunities both internationally and within Australia.

Related inquiries and recent legislation[1]

1.13 The following related inquiries were commenced during the course of this inquiry and they are referred to, where relevant, throughout this report.

- Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) (commenced 6 December 2018);
- PJCIS Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (ongoing);
- Joint Select Committee on Trade and Investment Growth inquiry into Trade and the Digital Economy (completed September 2018)[2]; and
- Senate Finance and Public Administration References Committee inquiry into Digital Delivery of Government Services (completed June 2018)[3].

1.14 The PJCIS recommended that the Parliament pass the TOLA Bill and that, once passed by the Parliament, the PJCIS should undertake a review of the new legislation. The TOLA Bill passed both Houses on 6 December 2018.[4]

1.15 The PJCIS commenced its Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* with specific reference to

[1] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*, October 2017, p. 33, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf (accessed 28 March 2019).

[2] Joint Standing Committee on Trade and Investment Growth, *Trade and the Digital Economy*, 20 September 2018.

[3] Senate Finance and Public Administration References Committee, *Digital Delivery of Government Services*, 27 June 2018.

[4] Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, December 2018, Recommendation 1, p. 3 and Recommendation 16, p. 8.

Government amendments introduced and passed on 6 December 2018. The Senate referral requires the PJCIS to report by 3 April 2019.[5]

ICT landscape

1.16 ICT and the internet have become central features of Australia's economy and way of life. Globalisation combined with technological advances means that people are now interconnected by internet technology as never before.

1.17 For example, a study by the global research organisation Software.org: the BSA Foundation has estimated that, by 2020, an estimated 50 billion devices will be connected to the internet.[6]

1.18 According to the Australian Bureau of Statistics (ABS), in 2016–17 86 per cent of Australian households had access to the internet; the mean number of devices used to access the internet at home per household was 6.2.[7] In the three months ended 30 June 2018, the total volume of data downloaded in Australia was 3.8 million Terabytes, a 28.1 per cent increase compared with the three months ended June 2017. As at 30 June 2018, there were approximately 27.0 million mobile handset subscribers in Australia, with 246 765 Terabytes of data downloaded to these devices in the three months ending 30 June 2018.[8] The three most popular online activities for Australians in 2016–17 were banking, entertainment and social networking, followed by online shopping.[9]

1.19 New and emerging ICTs offer significant benefits for governments, business, the private sector and individuals. They also offer law enforcement agencies the potential for improved investigative and operational outcomes.[10]

1.20 *Australia's Tech Future*, the Australian government's Digital Economy Strategy launched in December 2018, noted that improvements to existing industries

[5] PJCIS, Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* with specific reference to Government amendments introduced and passed on 6 December 2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct (accessed 16 January 2019).

[6] Software.org: the BSA Foundation, cited in 'IoT devices to reach 50 billion by 2020: Report', BGR, 14 July 2017, https://www.bgr.in/news/iot-devices-to-reach-50-billion-by-2020-report/ (accessed 24 January 2019).

[7] Australian Bureau of Statistics (ABS), *8146.0 – Household Use of Information Technology, Australia, 2016–17*, available: http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0 (accessed 6 March 2019).

[8] ABS, *8153.0 – Internet Activity, Australia, June 2018*, available: https://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/ (accessed 6 March 2019).

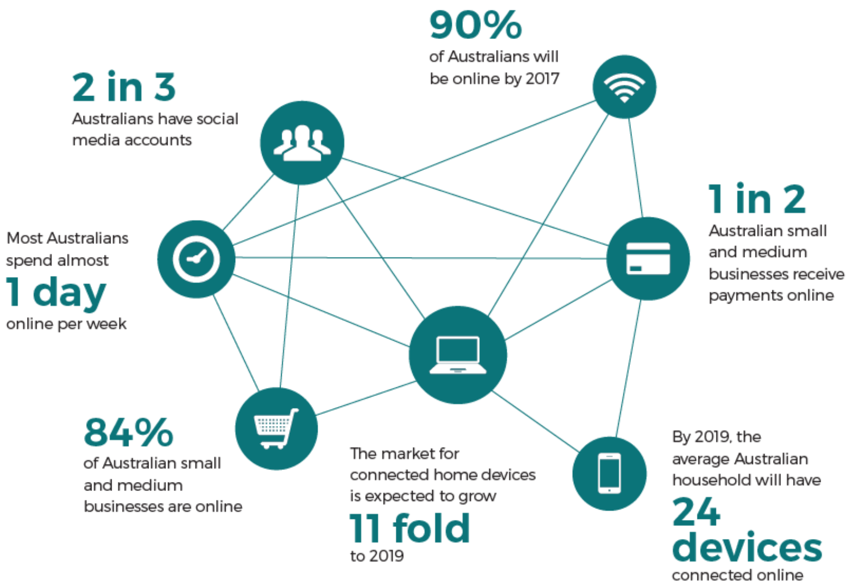
[9] ABS, *8146.0 – Household Use of Information Technology, Australia, 2016–17*, available: http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0 (accessed 6 March 2019).

[10] Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF), *Submission 28*, p. 9.

and growth of new ones could be worth $315 billion to the Australian economy over the next decade.[11]

1.21 This interconnectivity has changed the way people exchange information and conduct business (see Figure 1).

Figure 1: How Australians are connected online[12]


90%
of Australians will be online by 2017
2 in 3
Australians have social media accounts
1 in 2
Australian small and medium businesses receive payments online
Most Australians spend almost
1 day
online per week
84%
of Australian small and medium businesses are online
The market for connected home devices is expected to grow
11 fold
to 2019
By 2019, the average Australian household will have
24 devices
connected online

Cybercrime

1.22 Cybercrime relates to criminal activities carried out by means of computers or via the internet. It includes both crimes where computers or other ICTs are an integral part of an existing offence (such as online fraud or online child sex offences), as well as crimes directed at computers or ICTs (such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software).[13]

[11] Commonwealth of Australia, Department of Industry, Innovation and Science, *Australia's Tech Future: Delivering a strong, safe and inclusive digital economy*, 19 December 2018, p. 6, https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf (accessed 12 February 2019).

[12] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*, 2016, p. 14, https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf (accessed 5 December 2018).

[13] Australian Criminal Intelligence Commission (ACIC), *Cybercrime*, updated 17 July 2018, https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime (accessed 16 January 2019).

1.23 The International Association of Prosecutors—Global Prosecutors E-Crime Network (GPEN) remarked that ICT is constantly changing and that cybercrime 'is a crime without borders':

> With the speed of technological change, we can expect such innovations to be open to misuse by ICT criminals and therefore need to ensure that protection is factored in right from the beginning. The ability of governments to protect society against ICT crimes is of paramount importance.[14]

1.24 The increasing reliance of Australians on internet technology, together with the rapid development of new and emerging ICTs, is creating significant law enforcement challenges to Australia's national, state and territory jurisdictions, as well as to the Indo-Pacific region as a whole.

1.25 As the Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF) stated:

> The use of cyber elements for criminal purpose is growing, creating unprecedented risks for both individuals and businesses. For example, according to the Australian Cybercrime Online Reporting Network (ACORN), reports of ransomware attacks doubled between 2016 and 2017…Terrorists, child sex offenders, cyber criminals and organised crime syndicates are exploiting new technologies to communicate, commit and enable crimes. Technology is also increasingly used as an enabler of crime, with the majority of serious and organised crime using ICT for a variety of crime types. Technology is no longer limited to high tech crime types.[15]

Economic impact

1.26 The Cyber Security Research Centre (CSRC) highlighted the increasing economic impact of internet-enabled crime globally:

> The Internet has become a ubiquitous new vector for old threats and old crimes. Just as Cyberspace has become the Fifth Domain of Warfare, so Cybercrime is becoming one of the most profitable areas of criminal activity, impacting adversely on both individuals and the community as a whole. The global cost of cybercrime is expected to reach over $US6 trillion in the early 2020s.[16]

[14] International Association of Prosecutors—Global Prosecutors E-Crime Network (GPEN), *Submission 19*, p. 2.

[15] DHA, AGD and ABF, *Submission 28*, pp. 6 and 9.

[16] Cyber Security Research Centre (CSRC), *Submission 8*, p. 1.

1.27 Australia's relative wealth and high use of social media, online banking and online government services have made it an attractive target for criminal syndicates.[17] DHA noted the increasing economic cost of cybercrime to Australia:

> Cybercrime now operates on an industrial scale, driven by the global commercialisation of cybercrime, the ability of sophisticated cyber criminals to adapt to technological advancements, and the rapid pace of technological change. With the prolific global rise of cybercrime, estimates suggest that it costs Australians between $1 billion to $17 billion annually.[18]

New and emerging ICTs

1.28 As noted above, the rapid development of new ICTs offers law enforcement agencies the opportunity to undertake criminal investigations in new and more effective ways. However, new and emerging ICTs also present particular challenges to the capabilities of law enforcement agencies in combating cybercrime.

Internet Protocol version 6 (IPv6)

1.29 Internet Protocol version 6 (IPv6) is being implemented across the internet. It includes a 'native IP security system' that automatically encrypts network communications content. It also allows for a significant increase in the number of IP addresses available. Both of these issues are of concern to law enforcement agencies. A single internet user may have multiple IP addresses, whereas currently 'domestic IP providers must maintain records linking IP addresses and a subscriber for a session'. IPv6 will therefore make record-keeping more complicated.[19]

5G and 7G networks

1.30 The 5G network will give users greater anonymity, enabling data to be obtained by a single device from multiple sources such as WiFi, network towers and satellite simultaneously. It will replace the unique identifier associated with an electronic device with a temporary identifier, which destructs once a connection is made with a network tower.[20]

1.31 Law enforcement agencies are currently able to use the unique identifier in 4G technology to attribute a device to an individual. However, according to the Australian Criminal Intelligence Commission (ACIC) and Australian Institute of Criminology (AIC), 5G technology 'will obfuscate this' as fewer communications data will cross

[17] ACIC, *Connect, Discover, Understand, Respond: 2016−17 Annual Report*, Canberra, 2017, p. 118, https://acic.govcms.gov.au/sites/g/files/net1491/f/acic_2016-17_annual_report.pdf?v=1508387578 (accessed 29 January 2019).

[18] DHA, AGD and ABF, *Submission 28*, p. 6.

[19] DHA, AGD and ABF, *Submission 28*, p. 10.

[20] ACIC and Australian Institute of Criminology (AIC), *Submission 29*, p. 7.

over a point on the provider network, rendering current practices of intercepting communications void:

> A key issue with the introduction of 5G technology is that to provide lawful access, communications providers will need to assist law enforcement agencies to reconstruct data sessions from multiple sources to allow access to a single communication event...the impost and burden on both communications providers and law enforcement agencies to achieve lawful interception will be unprecedented [21]

1.32 The Wireless Internet Service Provider Association of Australia (WISPAU) discussed plans by overseas satellite services to launch more than 10 000 satellites as part of the implementation of global seventh generation (7G) networks by 2025. These 'Low Earth Orbit Satellite broadband services' will provide 100 per cent coverage for voice and broadband services across the globe. However, they may remove control of the Australian communications network from Australia.[22]

Mesh networks

1.33 A mesh network is a network of interlocked routers called nodes or points. Mesh networks allow devices in the network to have a strong Wi-Fi signal regardless of their location or direct connection to the internet. For example, a mesh network may involve a person's personal router being 'meshed' with the networks of surrounding neighbours, allowing that person to access the internet through their neighbour's connection in the event of an outage or other adverse circumstance. The primary network technology may be Wi-Fi, while some other devices can be connected with one another via Bluetooth, or a mixture of new wireless technologies.[23]

1.34 DHA, AGD and ABF submitted that mesh network technologies are likely to pose significant problems for law enforcement agencies involved in investigating offences conducted outside of standard carrier networks:

> Commercial mesh products are still within their developmental stages, however personal mesh networks between smart phones, watches and other devices are increasingly prevalent. Future adoption of mesh network technologies makes it imperative for legislation to enable law enforcement agencies to investigate offences over more than just carrier networks. These technologies raise questions about traceability and attribution that underpin current interception frameworks. For example, it may appear that the owner of the router directly connected to the internet sent a communication, rather than the actual sender. Additionally, mesh networks will not typically establish one direct path for a communication to travel over. Mesh networks

[21] ACIC and AIC, *Submission 29*, p. 7.

[22] Wireless Internet Service Provider Association of Australia (WISPAU), *Submission 17*, p. 3.

[23] DHA, AGD and ABF, *Submission 28*, p. 11.

> self-configure and will establish the most efficient route for a communication to travel over at a given time.[24]

Virtual Private Network (VPN)

1.35 A Virtual Private Network (VPN) encrypts information sent and received by a device so that the information cannot be intercepted and decoded, thereby creating a safe connection between a device and a network over a less secure network such as the public internet. VPN technology is widely used in corporate environments enabling, for example, an employee to work outside the office whilst being securely connected to the corporate network.[25]

1.36 VPNs have also become increasingly available to and used by private individuals, to protect identity and privacy, as well as circumvent geo-blocking[26] and "bandwidth throttling".[27] [28]

Drone technology

1.37 Drone technology is evolving, from single drone activity to models that can support 'Eusocial' behaviours whereby drones are to perform complex tasks in a coordinated fashion.[29] Drones have a wide range of applications, including delivery of various items, mapping, land management, surveillance and monitoring.[30]

1.38 Such technology offers significant advantages for emergency response scenarios and reduces the risk to responders. However, as Dr John Coyne noted, the evolution of this technology is likely to result in drones that are able to complete pre-programmed actions without human interaction, and the associated risk of hijacking for terrorist purposes.[31]

[24] DHA, AGD and ABF, *Submission 28*, p. 11.

[25] CISCO, *What is a VPN? – Virtual Private Network*, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (accessed 19 February 2019).

[26] Geo-blocking is used on websites to prevent shoppers in some countries from being able to buy products and services for cheaper overseas prices.

[27] Bandwidth throttling is when an internet service provider detects and de-prioritises certain types of internet traffic.

[28] Choice, *How to find the best VPN service*, https://www.choice.com.au/electronics-and-technology/internet/connecting-to-the-internet/buying-guides/vpn-services (accessed 6 March 2019).

[29] Dr John Coyne, *Submission 4*, p. 2.

[30] For a summary of the many ways in which drones are used see Senate Rural and Regional Affairs and Transport References Committee, *Current and future regulatory requirements that impact on the safe commercial and recreational use of Remotely Piloted Aircraft Systems (RPAS), Unmanned Aerial Systems (UAS) and associated systems*, July 2018, pp. 4–6.

[31] Dr John Coyne, *Submission 4*, p. 2.

1.39 All drone operators, including law enforcement agencies, are subject to the Civil Aviation Safety Authority legislation. However, the widespread public use and accessibility of drone technology has created a significant threat to public safety.

1.40 Current Australian legislation prevents law enforcement agencies from using signal interference devices and signal jammers to intercept a drone in flight, despite the availability of technologies that can safely disable the threat.[32] According to the Western Australia Police Force, a legislative review is required to determine whether law enforcement agencies should be able to utilise these technologies for policing purposes.[33]

Artificial intelligence

1.41 As with drone technology, the rapid development of artificial intelligence (AI) technologies is expected to have significant implications for future law enforcement.

1.42 Mr Matthew Loeb, Chief Executive Officer, ISACA, noted that AI is one of the most dangerous technological capabilities to emerge because, while it can be used to identify perpetrators, it can also be used to accelerate the rate of cyberattacks and present them in ways that might not be recognisable to law enforcement personnel.[34]

1.43 However, as Mr Loeb also noted, AI offers technological advantages to law enforcement. For example, AI is being used in the United States to improve the timeliness of investigations such as video search:

> Artificial intelligence can be used to identify certain instances. It can be used to identify faces. It can be used to identify tattoos on bodies. It can even be used in the redaction of non-relevant images in the video. We're starting to see implementations of that in a limited fashion. Again, the challenge of that is having the people employed in these law enforcement agencies being up to the capabilities to actually leverage that and understand how to use that.[35]

1.44 Dr Coyne noted that contemporary approaches to software development will not be adequate to deal with new AI capabilities:

> To support new capabilities we may see a move to intelligent systems that are decoupled from underlying infrastructure. In this construct, AI may

[32] The *Customs (Prohibited Imports) Regulations 1956* prohibits the importation of signal jammers and drone jammers into Australia unless subject to an exemption.

[33] Western Australia Police Force, *Submission 31*, p. 3.

[34] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 13.

[35] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 11.

> exist across multiple pieces of hardware rather than being developed in a single stand alone or networked piece of hardware infrastructure.[36]

Material manipulation

1.45 New and emerging technologies such as digital manufacturing, gene editing, nanotechnology and synthetic biology are being developed that enable users to digitise, manipulate and reproduce every aspect of the material and biological environment. This has the potential to undermine traditional law enforcement investigative tools. Digital manufacturing (3D printing) technology, for example, is developing rapidly and is becoming more reliable and accessible.[37]

The Internet of Things

1.46 The Internet of Things (IoT) is the name given to the networking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators and network connectivity enabling them to collect and exchange data.[38]

1.47 The IoT reflects the way in which the internet is transforming everyday life and work by combining internet connectivity and data analytic capabilities with consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects.[39] By 2020, it is predicted that around 25 billion such objects will be connected to the internet, which has the potential to generate up to $11.1 trillion a year by 2025.[40]

[36] Dr John Coyne, *Submission 4*, p. 3.

[37] See for example, Bob Yirke, *A small chemical reactor made via 3-D printing allows for making drugs on-demand*, 19 January 2018, https://techxplore.com/news/2018-01-small-chemical-reactor-d-drugs.html (accessed 25 March 2019); David Morris, *Army Unveils 3-D Printed Grenade Launcher*, 11 March 2017, http://fortune.com/2017/03/11/3d-printed-grenade-launcher/ (accessed 25 March 2019).

[38] Internet Society, *The Internet of Things: An Overview*, 15 October 2015, p. 4, https://www.internetsociety.org/resources/doc/2015/iot-overview?gclid=EAIaIQobChMI9Zqf0siC4AIVFR4rCh3hPwVVEAAYAyAAEgL_gPD_BwE (accessed 23 January 2019).

[39] Internet Society, *The Internet of Things: An Overview*, 15 October 2015, (accessed 23 January 2019).

[40] ACIC and AIC, *Submission 29*, p. 7; Software.org: the BSA Foundation, cited in BGR, *IoT devices to reach 50 billion by 2020: Report*, 14 July 2017, https://www.bgr.in/news/iot-devices-to-reach-50-billion-by-2020-report/ (accessed 24 January 2019).

Chapter 2

Coordinating law enforcement across jurisdictions

2.1 Cybercrime is a global challenge, and any effective response requires close coordination between law enforcement agencies across multiple international jurisdictions. As the International Association of Prosecutors—Global Prosecutors E-Crime Network (GPEN) stated, the central problem for law enforcement relates to the problem of jurisdiction and the borderless nature of the internet:

> Nearly every cybercrime will involve more than one jurisdiction and therefore require some form of international cooperation. In cybercrime cases you can have parallel or competing jurisdictions. There is the need for clarity regarding jurisdiction some countries have domestic laws with extrajurisdictional effect; and will limit the assistance they will give to another country on a matter if they have a jurisdictional claim or interest. If you look also at the different legal, investigative and prosecution systems and the fact that some countries will not extradite their own nationals. It can become very complicated and you can understand why countries require rules on negotiating jurisdiction.[1]

2.2 This borderless nature of cybercrime means that no country can fully protect itself against cybercrime without the help of law enforcement in other countries. It is therefore necessary for all countries to have law enforcement agencies, prosecutors and judges who understand the nature of cybercrime and are able to cooperate on investigations and prosecutions of these crimes. As GPEN noted:

> ICT criminals typically hide in countries that are less developed, where the law enforcement personnel, prosecutors and judges are less efficient in the investigation and prosecution of ICT offences.[2]

International law enforcement arrangements

2.3 Australia is party to several inter-jurisdictional treaties, alliances and other mechanisms that aim to facilitate international cooperation in relation to the investigation of criminal activity enabled by new and emerging technologies.

Council of Europe Convention on Cybercrime (Budapest Convention)

2.4 Council of Europe Convention on Cybercrime (Budapest Convention) is the leading, binding international instrument directed at cybercrime. It sets out offences that criminalise ICT-offending, and encourages effective international cooperation which is needed not only between governments but also with industry. The Australian

[1] International Association of Prosecutors—Global Prosecutors E-Crime Network (GPEN), *Submission 19*, p. 3.

[2] GPEN, *Submission 19*, p. 3.

government announced in 2010 that it would take steps to accede to the Budapest Convention. It came into force in Australia on 1 March 2013.[3]

2.5 Australia's accession to the Budapest Convention helps to improve the ability of Australian law enforcement agencies to work effectively with their overseas counterparts. The Budapest Convention aims to:

- harmonise domestic legal frameworks on cybercrime;
- provide for domestic powers to investigate and prosecute cybercrime; and
- establish an effective regime of international legal cooperation.[4]

2.6 Ms Esther George, Lead Cybercrime Consultant, International Association of Prosecutors, noted how many non-European countries, including Australia, have now adopted the Budapest Convention, increasing its effectiveness in establishing principles for cybercrime offences:

> …the Council of Europe cybercrime convention, which, although it began in Europe, has actually spread and taken over quite a few countries. They have about 56 countries as signatories now, and that includes Australia, US, Turkey, Chile, Costa Rica, Dominican Republic, Israel, Japan, Mauritius, Senegal, Sierra Leone, Tonga and the Philippines. I understand that Tunisia has recently been invited to join….The reason that I think this convention is very good is not just because I'm a Council of Europe expert…but also because the Council of Europe convention is the only treaty you have that actually deals with [it]. It's been around since 2001 and it covers what I think are the main pillars that need to be covered. It sets out the offences, and you've got countries that have not signed up to the convention that actually have taken on board the principles in their legislation and they've actually criminalised the offences…. It brings back the idea that what you need for international cooperation is for every country to criminalise the same offences.[5]

Mutual Legal Assistance Treaties

2.7 Mutual Legal Assistance Treaties (MLATs) are agreements between governments that facilitate the exchange of information relevant to an investigation occurring in at least one of those countries. They impact on the way that a user's data is shared with foreign governments for criminal investigations and prosecutions. MLATs are designed to facilitate cooperation in addressing serious cases of criminal

[3] Government response, House of Representatives Standing Committee on Communications, *Report on the Inquiry into Cyber Crime*, p. 13, https://www.aph.gov.au/PARLIAMENTARY_BUSINESS/COMMITTEES/HOUSE_OF_REPRESENTATIVES_COMMITTEES?url=coms/reports.htm (accessed 4 December 2018).

[4] Department of Home Affairs (DHA), 'Cybercrime', https://archive.homeaffairs.gov.au/about/crime/cybercrime (accessed 5 December 2018).

[5] Ms Esther George, Lead Cybercrime Consultant, International Association of Prosecutors, *Committee Hansard*, 29 March 2018, p. 41.

activity including cybercrime. This international standardised process allows a court or judge to review each request before data is accessed.[6]

2.8 MLATs present a number of challenges to law enforcement agencies; some of these challenges are discussed in subsequent chapters.

Five Eyes Alliance

2.9 The Five Eyes Alliance is an intelligence alliance involving the United Kingdom, United States, Canada, Australia and New Zealand. It was formally founded on 5 March 1946 as a multilateral post-war agreement for cooperation in signals intelligence known as the UKUSA Agreement, and subsequently expanded to include Canada (1948) and Australia and New Zealand (1956). After more than 70 years, its scope continues to expand in response to security concerns associated with the emergence of new technologies.[7]

Australian law enforcement policy framework

2.10 In Australia, there has been a concerted national effort to develop a coordinated response to cybercrime, including the implementation of a high level policy framework to guide government, including law enforcement, contributions to a safer and more secure online environment.[8]

National Plan to Combat Cybercrime

2.11 In 2013 the Australian government released the first *National Plan to Combat Cybercrime*.[9] The National Plan provides a coordinated national response across jurisdictions, based on six key principles (see Figure 2).

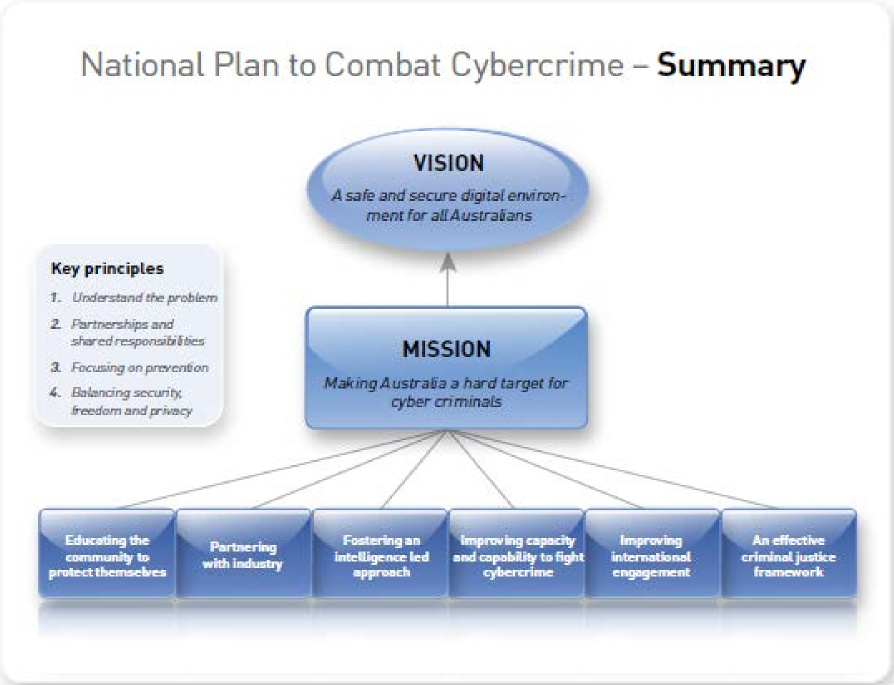
[6] Access Now, *Mutual Legal Assistance Treaties*, https://www.mlat.info/ (accessed 18 February 2019).

[7] JV Tossini, 'The Five Eyes—The Intelligence Alliance of the Anglosphere', *ukdj*, 14 November 2017, https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/ (accessed 20 December 2018). See Chapter 4 for discussion of the Five Eyes Alliance Statement of Principles in relation to encryption.

[8] DHA, Attorney-General's Department (AGD) and Australian Border Force (ABF), *Submission 28*, p. 6.

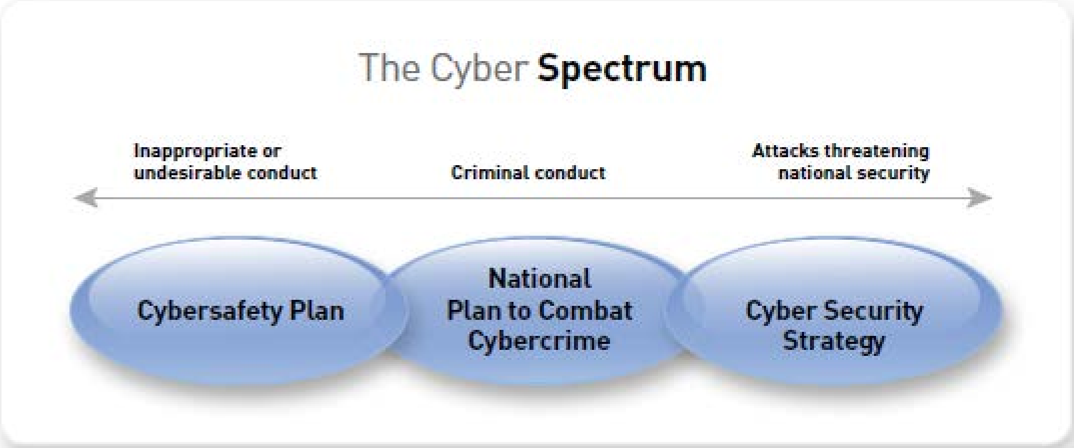
[9] ISACA, *Submission 13*, [p. 2].

Figure 2: Overview of National Plan to Combat Cybercrime


National Plan to Combat Cybercrime – Summary
VISION
A safe and secure digital environment for all Australians
Key principles
1. Understand the problem
2. Partnerships and shared responsibilities
3. Focusing on prevention
4. Balancing security, freedom and privacy
MISSION
Making Australia a hard target for cyber criminals
Educating the community to protect themselves
Partnering with industry
Fostering an intelligence led approach
Improving capacity and capability to fight cybercrime
Improving international engagement
An effective criminal justice framework

2.12 The Plan notes that cybercrimes are part of a 'cyber spectrum' of activities ranging from broader social and personal risks associated with the use of the internet and computers on the one hand, to attacks that threaten national security on the other. The Plan focuses on the centre of this spectrum: criminal conduct (see Figure 3).

Figure 3: The Cyber Spectrum[10]


The Cyber Spectrum
Inappropriate or undesirable conduct
Criminal conduct
Attacks threatening national security
Cybersafety Plan
National Plan to Combat Cybercrime
Cyber Security Strategy

[10] AGD, *National Plan to Combat Cybercrime*, 2013, p. 6.

Australia's Cyber Security Strategy

2.13 In 2016 the Prime Minister launched *Australia's Cyber Security Strategy* as a 'roadmap for creating a "cyber smart nation"'. The Strategy sets out the Australian government's philosophy and program for 'meeting the dual challenges of the digital age—advancing and protecting our interests' online between 2016 and 2020.[11]

2.14 It recognises that Australia needs to innovate and diversify its economy, and embrace 'disruptive technologies' that open up new possibilities for innovation and growth.[12]

2.15 The Strategy recognises that digital technologies bring risks, and that strong cyber security is a 'fundamental element of our growth and prosperity in a global economy' and vital to national security requiring partnerships between governments, the private sector and the community:[13]

> As people and systems become increasingly interconnected, the quantity and value of information held online has increased. So have efforts to steal and exploit that information. Cyberspace, and the dynamic opportunities it offers, is under persistent threat.[14]

2.16 The objectives of the Strategy include:

- the creation of jointly operated cyber threat sharing centres and an online threat sharing portal;
- partnering internationally to prevent cybercrime and other malicious/nefarious cyber activity; and
- helping to build capacity and awareness within Australia's public and private sectors by developing a highly-skilled workforce and raising citizens' awareness of the risks and benefits of the cyber realm.[15]

2.17 The Strategy includes a commitment to increasing the capabilities of the Australian Cyber Security Centre (ACSC); a new multi-use facility for the ACSC; additional funding for the Australian Federal Police (AFP) and Australian Criminal Intelligence Commission (ACIC); and engaging our regional partners to shut down

[11] Commonwealth of Australia, Department of Prime Minister and Cabinet, *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*, 2016, p. 2, https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf (accessed 5 December 2018).

[12] ISACA, *Submission 13*, [p. 2].

[13] Commonwealth of Australia, Department of Prime Minister and Cabinet, *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*, 2016, p. 5.

[14] Commonwealth of Australia, Department of Prime Minister and Cabinet, *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*, 2016, p. 15.

[15] ISACA, *Submission 13*, [pp. 2−3].

'safe havens' for cyber criminals.[16] It also recognises the importance of government working with the business sector to address cyber threats.[17] The Strategy also outlines a number of cyber security initiatives that have been implemented in relation to building strong cyber defences (see Figure 4).

2.18 Mr Andrew Colvin, Commissioner, AFP has remarked that the Strategy requires constant monitoring in order to keep pace with the changing cyber security environment:

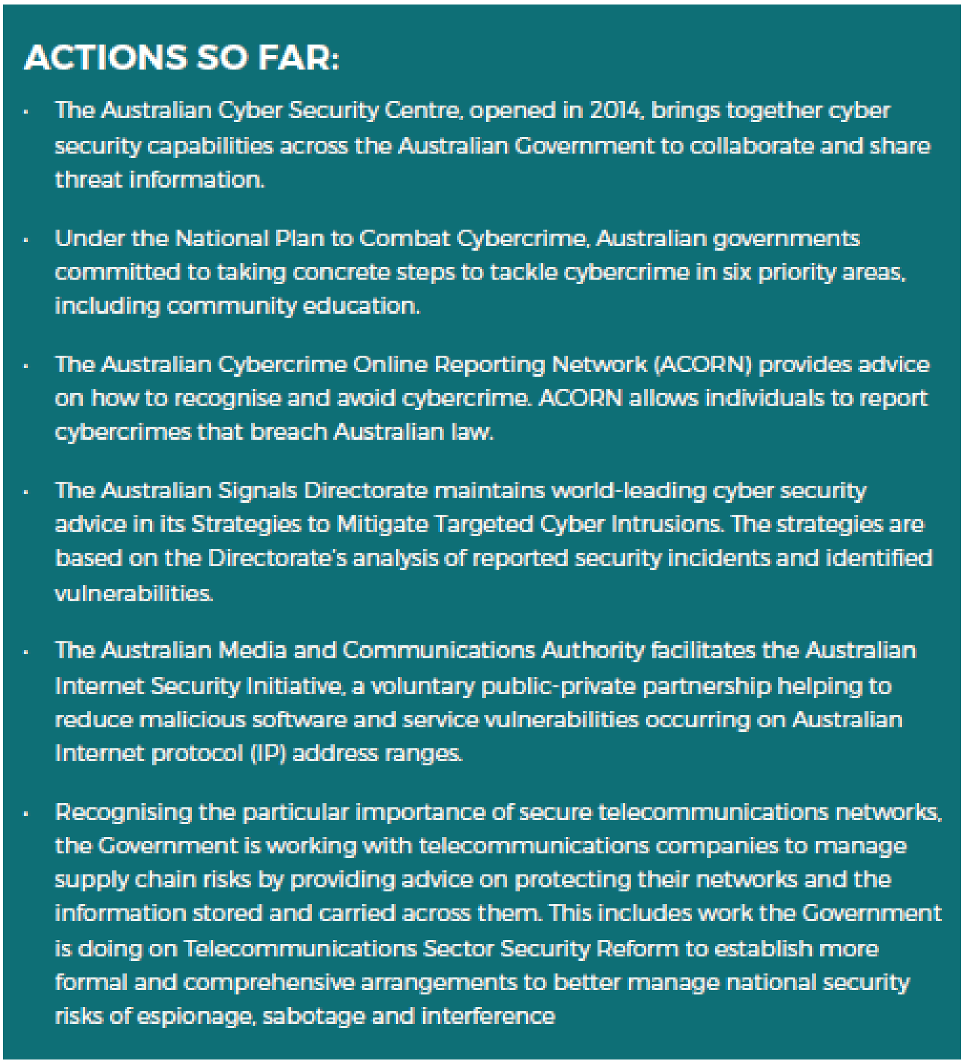
> The government is constantly reviewing that strategy, and that's because, in cybercrime, of all the crimes we deal with, two years ago is a very long time and things have changed enormously, both in the threat actors that we are dealing with but also in the technologies—the targets that they're attacking.[18]

[16] DHA, AGD and ABF, *Submission 28*, p. 7; see also Mr Hamish Hansford, First Assistant Secretary, National Security and Law Enforcement Policy, DHA, *Committee Hansard*, 11 May 2018, p. 48.

[17] Commonwealth of Australia, Department of Prime Minister and Cabinet, *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*, 2016 p. 6.

[18] Mr Andrew Colvin, Commissioner, Australian Federal Police (AFP), *Committee Hansard*, 22 February 2019, pp. 5–6.

Figure 4: Australian cyber security initiatives as at 2016[19]



ACTIONS SO FAR:

- The Australian Cyber Security Centre, opened in 2014, brings together cyber security capabilities across the Australian Government to collaborate and share threat information.
- Under the National Plan to Combat Cybercrime, Australian governments committed to taking concrete steps to tackle cybercrime in six priority areas, including community education.
- The Australian Cybercrime Online Reporting Network (ACORN) provides advice on how to recognise and avoid cybercrime. ACORN allows individuals to report cybercrimes that breach Australian law.
- The Australian Signals Directorate maintains world-leading cyber security advice in its Strategies to Mitigate Targeted Cyber Intrusions. The strategies are based on the Directorate's analysis of reported security incidents and identified vulnerabilities.
- The Australian Media and Communications Authority facilitates the Australian Internet Security Initiative, a voluntary public-private partnership helping to reduce malicious software and service vulnerabilities occurring on Australian Internet protocol (IP) address ranges.
- Recognising the particular importance of secure telecommunications networks, the Government is working with telecommunications companies to manage supply chain risks by providing advice on protecting their networks and the information stored and carried across them. This includes work the Government is doing on Telecommunications Sector Security Reform to establish more formal and comprehensive arrangements to better manage national security risks of espionage, sabotage and interference

A new National Plan to Combat Cybercrime

2.19 On 19 May 2017, the Council of Australian Governments Law, Crime and Community Safety Council, comprising ministers with responsibilities for law and justice, police and emergency management, agreed to develop a new *National Plan to Combat Cybercrime* 'to ensure a strong national approach to tackling the increasing risks to business and individuals posed by cybercrime'.[20]

2.20 The National Cybercrime Working Group, comprising representatives from state and territory police and justice agencies, the ACIC and the Australia New

[19] Commonwealth of Australia, Department of Prime Minister and Cabinet, *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*, 2016, p. 29.

[20] Law, Crime and Community Safety Council, *Communiqué*, 19 May 2017, https://www.ag.gov.au/About/CommitteesandCouncils/Law-Crime-and-Community-Safety-Council/Documents/19-May-LCCSC-Communique.pdf (accessed 20 December 2018).

Zealand Policing Advisory Agency, is currently overseeing the development of the new Plan.[21]

Australia's International Cyber Engagement Strategy[22]

2.21 In October 2017, the Australian government released *Australia's International Cyber Engagement Strategy* aimed at fostering relationships between Australia and Asia-Pacific nations, such as China, New Zealand, South Korea and India, and improving connectivity, collaboration, and access throughout the region, especially in areas such as cyber security and internet governance.[23]

2.22 The Strategy has led to the formation of the Asia Pacific Computer Emergency Response Team (APCERT), a combination of CERTs from several nations that monitor and protect cyberspace in the region. It is also anticipated that overall regional cyber security capability will be strengthened as a result of the establishment of the Pacific Cyber Security Operational Network (PaCSON) to provide operational points of contact.[24]

Australian law enforcement agencies

2.23 Within Australia, responsibility for dealing with the different forms of cybercrime is shared between national, state and territory law enforcement and security agencies.[25]

Department of Home Affairs

2.24 The government established the portfolio of Home Affairs in December 2017. It includes the ACIC, AFP, Australian Signals Directorate (ASD), Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian Border Force (ABF), and Australian Security Intelligence Organisation (ASIO), representing an amalgamation of national security, emergency management and criminal justice

[21] DHA, *Cybercrime*, https://archive.homeaffairs.gov.au/about/crime/cybercrime (accessed 5 December 2018).

[22] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Security Strategy*, October 2017, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf (accessed 28 March 2019).

[23] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*, 2017, p. 32.

[24] ISACA, *Submission 13*, [p. 4].

[25] DHA, 'Cybercrime', https://archive.homeaffairs.gov.au/about/crime/cybercrime (accessed 5 December 2018).

functions from across government.[26] The portfolio also encompasses the Commonwealth Ombudsman which remains an independent statutory authority.[27]

2.25 The Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF) stated that strong cyber security is 'fundamental to our economic growth and is vital for our national security'. They noted that the Home Affairs portfolio established in December 2017 is designed to be a central policy agency providing coordinated strategy and policy leadership.

> Strong oversight and accountability is important to give the public confidence that our agencies not only safeguard our nation's security, but do so respecting the rights and liberties of all Australians.[28]

Australian Commission for Law Enforcement Integrity

2.26 The Australian Commission for Law Enforcement Integrity (ACLEI) is a statutory authority established by the *Law Enforcement Integrity Commissioner Act 2006* (the LEIC Act).

2.27 ACLEI is the only Commonwealth agency dedicated to the prevention, detection and investigation of corrupt conduct. It forms part of the Australian government's anti-corruption framework, focusing on agencies with law enforcement functions operating within a high-corruption risk environment.[29]

> Much of the information gathered by ACLEI occurs covertly—including through lawful access to digital records, and by using electronic surveillance capabilities. Often, ACLEI uses covertly-obtained material as a basis to collect additional information using its other investigatory tools—such as by issuing a summons for a person to attend a private hearing to give evidence, or corroborating information in another way (including by issuing notices to produce documents, or by conducting a search of premises under warrant).[30]

2.28 ACLEI works closely with other agencies subject to the Integrity Commissioner's jurisdiction to share information and insights to identify

[26] DHA, AGD and ABF, *Submission 28*, p. 6.

[27] DHA, AGD and ABF, *Submission 28*, p. 8.

[28] DHA, AGD and ABF, *Submission 28*, p. 8.

[29] Australian Commission for Law Enforcement Integrity (ACLEI), *Submission 1*, p. 1. The *Law Enforcement Integrity Commissioner Act 2006* (the LEIC Act) gives the Integrity Commissioner power to examine witnesses on oath in coercive hearings. Agencies subject to the Integrity Commissioner's jurisdiction include the ACIC; the former Crim Trac Agency and the former National Crime Authority; the Australian Federal Police; Australian Transaction Reports and Analysis Centre; Department of Immigration and Border Protection/DHA; prescribed aspects of the Department of Agriculture and Water Resources; and other agencies with law enforcement functions.

[30] ACLEI, *Submission 1*, p. 1.

vulnerabilities in the agencies' practices and procedures and help strengthen anti-corruption policies and arrangements. It also publishes case studies, investigation reports and articles on its website to assist corruption prevention practitioners.[31]

Australian Criminal Intelligence Commission

2.29 The ACIC is Australia's national criminal intelligence agency. It commenced operations on 1 July 2016, bringing together the Australian Crime Commission (ACC) and CrimTrac to form Australia's national criminal intelligence agency equipped with intelligence, investigative and information delivery functions.

2.30 The ACIC 'works with partners on the serious and organised crime threats of most harm to Australians and the national interest'.[32] One of the agency's key priorities is to explore the future of crime and justice, including the emergence of new technologies and potential impacts.[33]

2.31 The ACIC is the system administrator responsible for the operation of the Australian Cybercrime Online Reporting Network (ACORN). In 2018−19, the Australian government allocated $59.1 million to the ACIC to develop the National Criminal Intelligence System (NCIS) as a whole of government capability to share criminal information and intelligence. The NCIS is discussed further in Chapter 6.

Australian Cyber Security Centre

2.32 The Australian Cyber Security Centre (ACSC), established by the Australian government in November 2014, brings together law enforcement and security agencies from across the nation and leads the Australian government's efforts to improve cyber security.

2.33 ACSC is located within the ASD. Its role is to continuously monitor cyber threats across the globe, and provide advice and information about how Australians can protect themselves and their businesses online.

2.34 ACSC also works with government, business and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats through a national network of Joint Cyber Security Centres.[34]

[31] ACLEI, *Submission 1*, p. 7. The agencies subject to the Integrity Commissioner's jurisdiction include the Australian Criminal Intelligence Commission (ACIC); AFP; Australian Transaction Reports and Analysis Centre (AUSTRAC); DHA, including Australian Border Force); prescribed aspects of the Department of Agriculture and Resources; and any other Australian government agency prescribed by regulation under the *Law Enforcement Integrity Commissioner Act 2006*.

[32] ACIC and Australian Institute of Criminology (AIC), *Submission 29*, p. 3.

[33] ACIC and AIC, *Submission 29*, p. 3.

[34] Australian Cyber Security Centre, https://cyber.gov.au/about-this-site/about-acsc/ (accessed 20 February 2019).

2.35 The Computer Emergency Response Team (CERT), based in the ACSC, was launched in 2010 to provide Australian businesses, Australia's critical infrastructure and other systems of national interest (rather than individuals or small businesses) with advice and support in mitigating cyber threats.[35]

Australian Federal Police

2.36 The AFP plays a pivotal role in enforcing federal criminal law and protecting the Australian national interests from crime by operating in the evolving digital and law enforcement landscape.

2.37 The AFP Corporate Plan 2017–18 lists a key focus of the AFP's capability development in continuously building on the ability to strengthen information on demand as well as detect, prevent and predict serious crime through deep data exploration. Other key focuses identified in the Corporate Plan include the ongoing partnerships with industry to invest in innovation to combat serious and organised crime.[36]

Australian Signals Directorate

2.38 The single biggest concentration of national cyber expertise lies within the ASD. The Cyber Security Research Centre (CSRC) noted that the central role and expertise of the ASD will be critical in future in ensuring an effective cooperative national effort on cybercrime.[37]

Australian Transaction Reports and Analysis Centre

2.39 The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's financial intelligence unit and anti-money laundering and counter-terrorism financing regulator. Its purpose is to protect the integrity of Australia's financial system and contribute to the administration of justice through its expertise in countering money laundering and the financing of terrorism:

> AUSTRAC works closely with law enforcement and national security intelligence agencies, primarily on counter-terrorism and counter-terrorism financing matters, as well as other national security priorities. AUSTRAC's intelligence has played an important role in identifying new suspects linked to terrorism in Australia and overseas, and has improved Australia's

[35] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy*, 2016, pp. 2−3.

[36] ISACA, *Submission 13*, [p. 2].

[37] Cyber Security Research Centre (CSRC), *Submission 8*, p. 11. The CSRC is a public, not-for-profit company through which the Cyber Security Cooperative Research Centre operates. See Cyber Security Cooperative Research Centre, https://www.cybersecuritycrc.org.au/ (accessed 31 January 2019).

understanding of high-risk funds flows to Syria, Iraq and surrounding countries.[38]

Other agencies

2.40 Other Australian government agencies with existing cybercrime and cyber security responsibilities also include:

- the Australian Digital Health Agency, which is responsible for the Australian government's digital health program, and Digital Health Cyber Security Centre;
- the Australian Taxation Office and Department of Social Services, which work to ensure a more secure cyber environment for Australians;
- the Australian Secret Intelligence Service (ASIS), which is responsible for counter-intelligence activities overseas; and
- the Australian Security Intelligence Organisation (ASIO), which is part of the Home Affairs portfolio and responsible for issues relating to cyber espionage in Australia.[39]

2.41 The Office of the eSafety Commissioner was established in July 2015.[40] The role of the office is to promote online safety for all Australians by coordinating online safety efforts of government, industry and the not-for-profit community. The office has 'a broad remit' including:

- a complaints service for young Australians who experience serious cyberbullying
- identifying and removing illegal online content
- tackling image-based abuse.

The Office also provides audience-specific content to help educate all Australians about online safety including young people, women, teachers, parents, seniors and community groups.[41]

[38] AUSTRAC, *Submission 30*, p. 4.

[39] See Appendix 4 for a list of Australian government agencies with existing cybercrime and cyber security responsibilities.

[40] Commonwealth of Australia, Department of Communications and the Arts, *Launch of the Office of the Children's eSafety Commissioner*, 9 October 2015, https://www.communications.gov.au/departmental-news/launch-office-children%E2%80%99s-esafety-commissioner (accessed 8 March 2019).

[41] Commonwealth of Australia, Office of the eSafety Commissioner, *Role of the office*, https://www.esafety.gov.au/about-the-office/role-of-the-office (accessed 8 March 2019).

Chapter 3

'Going dark'

3.1 The rapid development and proliferation of new and emerging information and communications technologies (ICTs) has resulted in a new investigative paradigm for law enforcement. These developments are increasingly testing Australia's legislative framework, much of which was established before the prevalence of mobile devices, foreign-based service providers and encrypted communications.

3.2 Many of the challenges facing law enforcement and intelligence agencies arise from the application of new and emerging ICTs in ways that enable criminal activities to go undetected—commonly described as 'going dark'. These include the 'dark web'; encryption; multiple data storage platforms; cryptocurrency; social media; and messaging apps.[1]

The dark web

3.3 The 'dark web', also referred to as the 'darknet', is that part of the internet that is hidden from the view of typical search engines such as Google and Yahoo, and is only accessible by means of additional networking protocols and special software.[2]

3.4 The dark web allows users and website operators to remain anonymous or untraceable. It is sometimes used to facilitate cybercrime through dark web markets where those using them can purchase stolen information or illicit goods.[3] Dr John Coyne explained:

> The internet is comprised of two parts: the part that is indexed by search engines and that which isn't (the deep web). A small portion of this deep web is comprised of what has become known as the 'dark web'. In these areas of the internet exist secure networks of various sizes. These networks, and their data, are protected by a range of technology including encryption. Within some of these dark web networks are buyers and sellers who combine to create dark markets: more often than not dealing in illicit commodities.[4]

Cybercrime threats and national security

3.5 Dark web communications are increasingly being used to facilitate cybercrime. Cybercrime threats include information theft, criminal sabotage and

[1] Australian Commission for Law Enforcement Integrity (ACLEI), *Submission 1*, p. 1.

[2] Cyber Security Research Centre (CSRC), *Submission 8*, p. 6; International Association of Prosecutors, Global Prosecutors E-Crime Network (GPEN), *Submission 19*, p. 4.

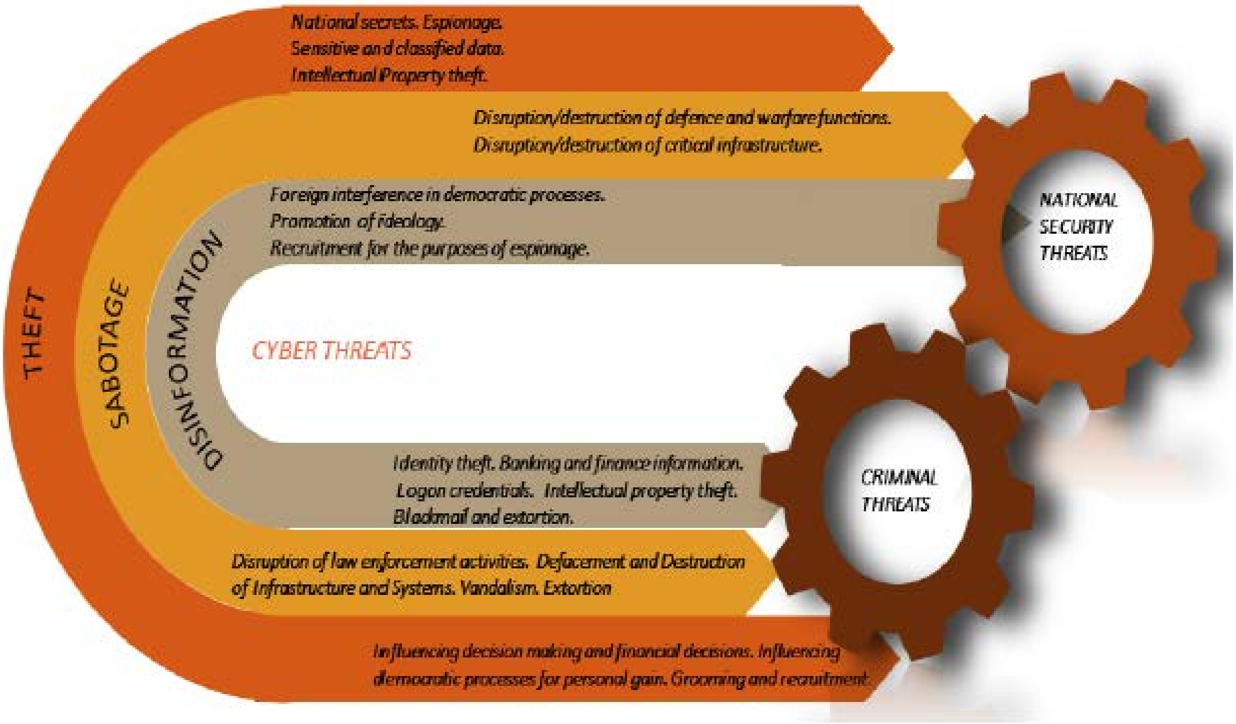
[3] CSRC, *Submission 8*, pp. 6–7.

[4] Dr John Coyne, *Submission 4*, pp. 7–8.

disinformation campaigns such as those that may affect the outcomes of democratic processes in a way that benefits the perpetrator. Cybercrime perpetrators may be individuals or companies, lone hackers, organised crime groups, terrorist cells or nation states.[5]

3.6 The Cyber Security Research Centre (CSRC) has illustrated how cybercrime is 'broadly parallel' to threats in the national security sector (see Figure 5).

Figure 5: Cybercrime threats and national security threats[6]


National secrets. Espionage.
Sensitive and classified data.
Intellectual Property theft.
Disruption/destruction of defence and warfare functions.
Disruption/destruction of critical infrastructure.
Foreign interference in democratic processes.
Promotion of ideology.
Recruitment for the purposes of espionage.
NATIONAL SECURITY THREATS
THEFT
SABOTAGE
DISINFORMATION
CYBER THREATS
Identity theft. Banking and finance information.
Logon credentials. Intellectual property theft.
Blackmail and extortion.
CRIMINAL THREATS
Disruption of law enforcement activities. Defacement and Destruction of Infrastructure and Systems. Vandalism. Extortion
Influencing decision making and financial decisions. Influencing democratic processes for personal gain. Grooming and recruitment.

3.7 National security threats and criminal activity exploit the internet in similar ways, and therefore need to be addressed using similar investigative tools and techniques. These tools can facilitate not only the investigation of cybercrime, but also other crimes not committed over the internet.[7]

3.8 A number of legislative reforms have been introduced in recent years in order to address law enforcement issues arising from these threats, including:

(a) A comprehensive set of offences to address cybercrime in the *Criminal Code Act 1995* based on model laws agreed across national, state and territory jurisdictions in 2001. The offences are consistent with those required by the Council of Europe Convention on Cybercrime, and are

[5] CSRC, *Submission 8*, p. 6.

[6] CSRC, *Submission 8*, p. 5.

[7] CSRC, *Submission 8*, p. 1.

drafted in technology-neutral terms to accommodate advances in technology.[8]

(b) In 2016, the Australian government responded to the potential challenges facing law enforcement investigation capabilities arising from new and emerging ICTs, by introducing the Data Retention regime through amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The amendments were designed to ensure that critical telecommunications metadata is retained by service provider companies for law enforcement purposes.[9]

(c) In April 2018, new legislation providing for digital currency exchange providers operating in Australia was implemented by the Australian Transaction Reports and Analysis Centre (AUSTRAC). The new laws covered, for the first time, regulation of service providers of cryptocurrencies including bitcoin.[10]

(d) On 6 December 2018, the Australian Parliament passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, to enhance cooperation between law enforcement and the ICT industry by introducing a new framework for industry assistance, including new powers to secure assistance from key companies in the communications supply chain both within and outside Australia.[11]

The new operational reality

3.9 The Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF), noted that the rapid development and increasing use of the dark web for criminal purposes is making it increasingly difficult for law enforcement agencies to undertake criminal investigations.[12]

[8] Department of Home Affairs (DHA), 'Cybercrime', https://archive.homeaffairs.gov.au/about/crime/cybercrime (accessed 20 December 2018).

[9] ACLEI, *Submission 1*, pp. 1−2. See also *Telecommunications (Interception and Access) Act 1979*, Part 5—1A—Data retention, https://www.legislation.gov.au/Details/C2018C00503 (accessed 20 December 2018).

[10] Australian Transaction Reports and Analysis Centre (AUSTRAC), *New Australian laws to regulate cryptocurrency providers*, 11 April 2018, http://www.austrac.gov.au/media/media-releases/new-australian-laws-regulate-cryptocurrency-providers (accessed 20 December 2018).

[11] This legislation is discussed in more detail in Chapter 4. See Parliament of Australia, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195 (accessed 12 December 2018). See Chapter 2 for further discussion about the Five Eyes Alliance.

[12] DHA, Attorney-General's Department (AGD) and Australian Border Force (ABF), *Submission 28*, pp. 6 and 9.

3.10 The 2013 *National Plan to Combat Cybercrime* summarised the problem for law enforcement:

> Online, criminals can commit crimes across multiple borders in an instant and can target a large number of victims simultaneously. Tools that have many legitimate uses, like high speed internet, peer to peer filesharing and sophisticated encryption methods, can also help criminals to carry out and conceal their activities. Despite these challenges, cybercrime is still a form of crime and requires a long term, sustained response from Australian governments.[13]

3.11 The Australian Securities and Investment Commission (ASIC) identified the specific challenges of the dark web to its surveillance capabilities as follows:

> (a) the ability to assume identities in order to 'gain trust' to access closed dark web forums (and committing resources to maintaining 'trust');
>
> (b) the protection of our systems and information (e.g. by being able to quarantine dark web access from our systems);
>
> (c) the obscuring of internet protocol addresses (that help with the location of 'threat actors') through the use of 'TOR nodes';
>
> (d) the immediate jurisdictional access to 'threat actors' who are largely operating outside Australia; and
>
> (e) lack of technological software and tools that have a specific focus on financial crimes, as typically the focus is on narcotics and terrorism.[14]

3.12 Dr Coyne explained that 'going dark' presents a major challenge to law enforcement because agencies still rely heavily on telephone interception capabilities:

> On one side is cybercrime, which everyone wants to talk about; it's very topical. On the other side is technology-enabled crime. In this case, one of the most significant challenges—the previous FBI director called it 'going dark'—is that our law-enforcement community, from the US to Australia to Canada to the UK, relies on telephone intercepts to undertake investigations. Our major, complex investigations require those.[15]

3.13 Dr Coyne cited the example involving Phantom Secure, a company that took BlackBerry devices and stripped out 'the cameras, microphones, GPS navigation and other features, and install[ed] encrypted messaging software, making them difficult for

[13] AGD, *National Plan to Combat Cybercrime*, 2013, p. 4, https://sherloc.unodc.org/cld/lessons-learned/aus/national_plan_to_combat_cybercrime.html?lng=en (accessed 19 December 2018).

[14] Australian Securities and Investment Commission (ASIC), *Submission 11*, p. 5.

[15] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 6.

law enforcement to crack'.[16] Of the 20,000 devices sold worldwide by Phantom Secure, approximately 10,000 were used in Australia by serious and organised crime groups to arrange criminal activities such as extortion, kidnapping, drug importations and contract killings.[17] In March 2018, the Chief Executive Officer of Phantom Secure was arrested and charged by the FBI 'with racketeering activity involving gambling, money laundering and drug trafficking'.[18]

3.14 Dr Coyne pointed to the operational impact of the dark web on law enforcement in the United States (US) context:

> Alleged criminal and terrorist targets are now using increasingly sophisticated encryption services which prevent law enforcement and police agencies from intercepting their communications. The interception intelligence sources are no longer shining a light on the covert activities of these targets.[19]

3.15 According to ISACA, the biggest threat of new and emerging ICTs is that they have the potential to 'negate the need for a "dark web"' by becoming mainstream:

> That is perhaps the most negative impact new and emerging ICTs could have on the dark web; the creation of Amazon- and Alibaba-esque companies as one-stop-shops for all things illicit, illegal, lethal and loathsome—on the same internet where the global community engages in digital commerce.[20]

3.16 DHA, AGD and ABF noted that the challenges for law enforcement agencies will be heightened by the introduction of the 5G network, with significant implications for the current telecommunications interception framework:

> Existing technologies that switch communications between Wi-Fi and cellular networks already present a problem for agencies—a significant amount of lawfully collected data is already incomplete. 5G will further exacerbate these intelligence gaps and make it harder for law enforcement to identify the appropriate access point to communications data. In order to gain the data from one communication platform, law enforcement may be required to intercept information from a number of sources.[21]

[16] Lucy McNally and John Stewart, 'Australian Federal Police seize Phantom Secure phones as part of global crackdown', *ABC News*, 16 March 2018, available: https://www.abc.net.au/news/2018-03-16/afp-seize-phones-as-part-of-phantom-secure-crackdown/9555652 (accessed 18 March 2019).

[17] Lucy McNally and John Stewart, 'Australian Federal Police seize Phantom Secure phones as part of global crackdown', *ABC News*, 16 March 2018.

[18] Lucy McNally and John Stewart, 'Australian Federal Police seize Phantom Secure phones as part of global crackdown', *ABC News*, 16 March 2018.

[19] Dr John Coyne, *Submission 4*, p. 4.

[20] ISACA, *Submission 13*, [p. 4].

[21] DHA, AGD and ABF, *Submission 28*, p. 10. See Chapter 1 for further explanation of the 5G network.

3.17 Dr Coyne offered a bleak assessment of the impact of 5G on the interception capabilities of law enforcement:

> Criminals are aware that the AFP, the New South Wales Police and the Victorian Police all use telephone intercepts and can access mobile phones. That problem is about to get significantly worse. When 5G technology comes in, it may spell the complete end of telephone intercepts across the globe.[22]

3.18 Mr Michael Phelan, APM, Chief Executive Officer, Australian Criminal Intelligence Commission (ACIC) and Director, Australian Institute of Criminology, stated 'when we move to systems like 5G—4G is problematic as it is—when identifiers don't exist for a device and they use dynamic IP addresses, it will make it even more difficult to use the metadata to track'.[23] Mr Phelan also advised the committee that:

> the [Department of Home Affairs] is doing a lot of work preparing for what we need to do in this space. It's an evolving issue. It's not lost upon anybody what we need to do for law enforcement to be able to continue to intercept. A lot of this is about public-private partnerships as well. It's about working with the technology companies, the carriers, so that we can come to mutual arrangements et cetera as to how these things will work. The goodwill on behalf of the carriers is enormous, particularly in Australia. They want to help but they have to keep their market edge as well with new products that are coming out.[24]

Extraterritorial and transnational policing

3.19 Privacy experts warned about the dangers of extraterritorial and transnational policing practices which, they argued, were not necessarily safeguarding human rights.

3.20 In 2017, for example, cybercrime researchers Ian Warren, Adam Molnar and Monique Mann drew attention to the use of 'poisoned watering holes' by Australian law enforcement. They argued that such strategies were 'creating troubling new standards in transnational policing', highlighting the need for new rules for digital

[22] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 6.

[23] Mr Michael Phelan, Chief Executive Officer, Australian Criminal Intelligence Commission (ACIC) and Director, Australian Institute of Criminology (AIC), *Committee Hansard*, 11 May 2018, p. 48.

[24] Mr Michael Phelan, Chief Executive Officer, ACIC & Director, AIC, *Committee Hansard*, 11 May 2018, p. 49.

evidence collection and exchange to assist prosecutions while preserving due process and human rights.[25]

3.21 Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia and Future Wise, submitted that policing the dark web increasingly involves extraterritorial police activity through a Computer Network Operation (CNO) or Network Investigation Technique (NIT) whereby law enforcement are collecting information from around the world by taking over illegal marketplaces that traffic in child exploitation material or drugs. They argued that there is limited regulatory guidance for their use, and expanding police powers for such investigations posed significant risks:[26]

> Without proper checks, police could have significantly expanded scope to search computers and this is creating troubling new standards in transnational policing. New rules for digital evidence collection and exchange must be developed to assist prosecutions while preserving due process and human rights.[27]

3.22 Drs Mann, Molnar, Warren and Daly stated that, whilst decisions to deploy CNO/NIT are frequently reviewed by law enforcement agencies, such decisions are rarely subject to judicial oversight or independent review until after a prosecution has begun.

3.23 They noted the debate over government sponsored use of malware, for example, whereby critics pointed out the extraterritorial effects of such operations while supporters argued that the shared concern internationally about dark web criminal activity means that there is unlikely to be resistance to law enforcement investigations.[28]

Law enforcement challenges

Encryption, encryption services and encrypted devices

3.24 Encryption and other anonymization tools and services are used to hide the identity of the user by separating identity from online activity, as well as securing

[25] I Warren, A Molnar and M Mann, 'Poisoned water holes: the legal dangers of dark web policing', *The Conversation*, 7 September 2017, https://www.news.com.au/technology/online/poisoned-water-holes-the-legal-dangers-of-dark-web-policing/news-story/285655e36981515e35e2290360f9e646 (accessed 20 December 2018).

[26] Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia, and Future Wise, *Submission 23*, p. 9.

[27] Dr Monique Mann et al, *Submission 23*, p. 9. See also discussion of law enforcement challenges in relation to big data in Chapter 5.

[28] Dr Monique Mann et al, *Submission 23*, p. 10.

access to the online content itself. Encryption is an essential contributor to the global economy and business competition in the twenty-first century.[29]

3.25 The introduction of end-to-end encryption on digital devices and cloud computing has also resulted in difficulties in accessing and obtaining data and digital evidence for law enforcement purposes. End-to-end encrypted instant messaging via communication apps and devices are not stored on a centralised server owned by the service provider. Instead, they can only be accessed from an end-point device such as a mobile phone, and the service provider is not able to access the content that passes through the app. Some services have a self-destruct function that will automatically delete messages from all sending and receiving devices after a certain amount of time.[30]

3.26 As encryption technology becomes cheaper and more widely available, users are increasingly able to access it to secure information and improve their own cyber security. As Mr Nathan White, Senior Legislative Manager, Access Now noted:

> …encryption is important. It provides the foundation for our digital world, and in a country like Australia, where 90 per cent of the population has access to the internet, encryption is essential for protecting not only the cybersecurity of connected critical infrastructure but also its people from criminal activity online.[31]

3.27 Dr Coyne gave the example of internet banking and the conveniences afforded by encryption:

> I had my card recently cancelled because it had been used fraudulently somewhere. I had a phone call from the ANZ. ANZ said to me, 'We can reprogram your new card within 10 minutes on your iPhone. It will take 10 days to still get your hard-copy card, but that means you can still buy things and still get money out.' Those conveniences in the 21st century come from encryption.[32]

3.28 The Law Council of Australia similarly described the important role that encryption plays in protecting the security and privacy of information shared through smartphones, personal computers and network servers. In addition:

> [e]ncryption is also a fundamental tool for providing security in the banking, financial, securities, medical, legal and e-commerce sectors as well as general messaging, communications, data protection, intellectual

[29] Dr John Coyne, *Submission 4*, p. 4.

[30] ASIC, *Submission 11*, p. 6.

[31] Mr Nathan White, Senior Legislative Manager, Access Now, *Committee Hansard*, 11 May 2018, p. 2. Access Now represents over 300 individuals, organisations and companies from more than 50 countries. It advocates the development and use of secure communications tools and technologies and rejects policies that prevent or undermine the use of strong encryption.

[32] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 5.

> property protection and the secure transfer and storage of sensitive information.[33]

3.29 Several submitters drew attention to the importance of encryption for protecting human rights such as privacy and free expression, noting that there have been calls for strong encryption to be recognised as a human right in and of itself.[34]

3.30 Scram Software noted that the use of encryption is mandated in international legislation. The European Union's General Data Protection Regulation (GDPR), for example, recommends encryption as an effective means of safeguarding private data and preventing data breach. It requires all companies that collect or process data on EU residents to comply with GDPR, regardless of where the company is domiciled.[35]

3.31 Ms Amy Stepanovich, US Policy Manager and Global Policy Council for Access Now, pointed to the beneficial impact of iPhone encryption in the US:

> …one of the benefits we've seen in the US since iPhone encryption is a lowering of crime in the United States. Street criminals are less likely to assault or commit theft against individuals who are in possession of phones that are encrypted—that had hard drive encryption—because they can't resell those phones at a profit. So, street-level crime has actually decreased here with the deployment of that type of encryption.[36]

3.32 Ms Lizzie O'Shea and Ms Elise Thomas noted that encryption is crucial for protecting communications and data sharing systems against data breaches, particularly for individuals, critical service providers such as hospitals, and private sector professionals and businesses. Small businesses are especially vulnerable, with one study finding that 59 per cent of Australian businesses recorded cyber security breaches in 2016 alone.[37]

3.33 A software vendor, Cortex IT Labs Pty Ltd, reported that encryption is a core feature of all its competitors globally, and that a key requirement for security and compliance with data sovereignty laws is that each client manages their own encryption key.[38]

3.34 However, encryption has both positive and negative impacts. According to the ACIC and Australian Institute of Criminology (AIC):

[33] Law Council of Australia, *Submission 21*, p. 7.

[34] See for example Dr Monique Mann et al, *Submission 23*, p. 13; Access Now, *Submission 14*; Law Council of Australia, *Submission 21*, p. 8.

[35] Scram Software, *Submission 5*, p. 3.

[36] Ms Amy Stepanovich, US Policy Manager and Global Policy Council, Access Now, *Committee Hansard*, 11 May 2018, p. 4.

[37] Ms Lizzie O'Shea and Ms Elise Thomas, *Submission 15*, p. 4.

[38] Cortex IT Labs Pty Ltd, *Submission 12*, p. 2.

> [e]ncryption provides government (including law enforcement and intelligence agencies), businesses and individuals with the ability to protect computer systems and data, as well as safely engage in online activities such as banking, shopping and communication. However, criminals are also employing encryption services to communicate and commit crimes outside of the visibility of law enforcement.[39]

Specialised encryption methods

3.35 Cybercriminals are increasingly employing specialised encryption methods such as The Onion Router (Tor), cryptomarkets, cryptocurrencies and botnets.

The Onion Router

3.36 The Onion Router (Tor) is free software that enables anonymous communication. It directs internet traffic through more than 7000 relays to conceal the user's identity. Such anonymity allows users to surf the internet, chat and send instant messages anonymously.[40]

3.37 Tor was originally developed as a collaborative project between the US Naval Research Laboratory and the non-profit organisation Free Haven Project to create a free, distributed, anonymous, easily deployable and encrypted network to be used by those who wished to protect their online identity.[41]

3.38 The challenge with Tor, and many other new and emerging ICTs, is that it can be used for both legitimate and illegitimate purposes. As Mr Paul Templeton explained:

> It would seem that the TOR Project, the users and volunteers are often tarnished with terms like the dark web. I would like to point out that the majority of users are everyday people who value their basic human rights.[42]

3.39 Dark web markets, such as the now defunct Silk Road and AlphaBay, use Tor to assist users to avoid detection by law enforcement and intelligence agencies, as well as social media and internet service providers.[43]

[39] ACIC and AIC, *Submission 29*, p. 6.

[40] GPEN, *Submission 19*, p. 5; CSRC, *Submission 8*, p. 6.

[41] D Moore and T Rid, 'Cryptopolitik and the Darknet', *Survival: Global Politics and Strategy*, vol. 58, no. 1, 2016, https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085 (accessed 20 December 2018).

[42] Mr Paul Templeton, *Submission 32*, p. 1. TOR or 'The Onion Routing project' refers to a type of software that allows users to use the internet anonymously. Onion routing is implemented by encryption, and is used for both legal and illegal purposes. See GPEN, *Submission 19*, p. 5.

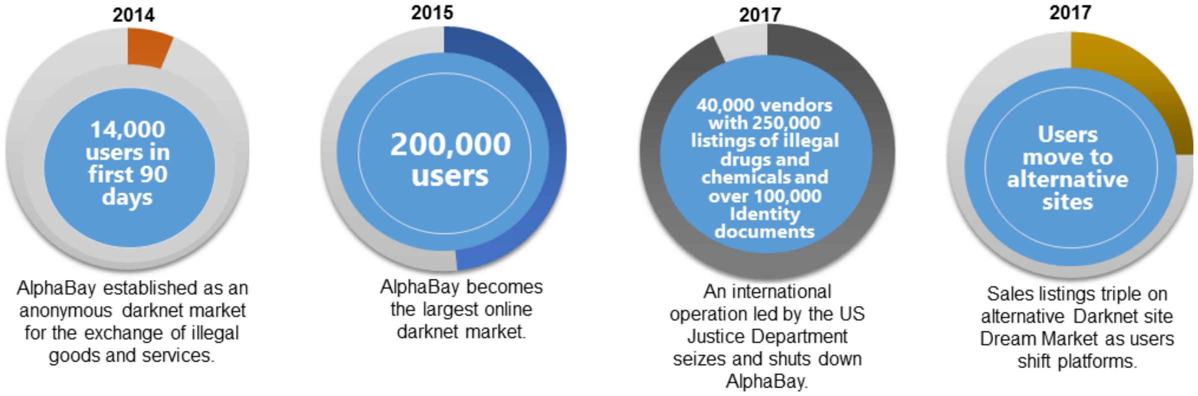
[43] CSRC, *Submission 8*, p. 6.

Cryptomarkets

3.40 Cryptomarkets, such as Silk Road and Agora, are 'e-bay style trading websites hosted on the darknet which use advanced encryption to protect the identities of users'.[44] The goods and services available via cryptomarkets include stolen information (for example credit card details, legitimate logon credentials for secure networks, and identity information), illicit goods (such as drugs and weapons), and hacking tools and botnets.[45]

3.41 The CSRC illustrated the volume of vendors and sales listings on AlphaBay, which operated on the dark web between 2014 and 2017 (see Figure 6).

Figure 6: AlphaBay dark web market: a case study[46]


2014
14,000 users in first 90 days
2015
200,000 users
2017
40,000 vendors with 250,000 listings of illegal drugs and chemicals and over 100,000 Identity documents
2017
Users move to alternative sites

AlphaBay established as an anonymous darknet market for the exchange of illegal goods and services.

AlphaBay becomes the largest online darknet market.

An international operation led by the US Justice Department seizes and shuts down AlphaBay.

Sales listings triple on alternative Darknet site Dream Market as users shift platforms.

3.42 Dr James Martin discussed the rapid increase in the popularity of cryptomarkets. He noted that these anonymous trading sites are increasingly being used by Australians to buy and sell illicit drugs, and argued that the 'unique characteristics of cryptomarket drug trading' is preferable to conventional drug dealing via closed networks or 'hotspots' such as nightclubs:

> Drug users report feeling safer and less exposed to violence when accessing drugs via a cryptomarket rather than they do when acquiring them through conventional means. One of the main reasons for this is that online dealers and users never meet in person during an exchange. Instead, drugs purchased via the darknet are delivered anonymously to users by post, thereby substituting street dealing and limiting the problems with which it is sometimes associated, such as violence, threats and robbery.[47]

[44] Dr James Martin, *Submission 9*, p. [3].

[45] CSRC, *Submission 8*, p. 6.

[46] CSRC, *Submission 8*, p. 9.

[47] Dr James Martin, *Submission 9*, [p. 3].

3.43 In 2018, US government agencies announced the results of a year-long, coordinated national operation targeting vendors of illicit goods on the darknet. It led to the arrest and potential prosecution of more than 35 darknet vendors.[48]

3.44 This followed the successful operation to shut down the Silk Road online marketplace in 2013, following an investigation that traced the administrator's digital footprint over a period of two years. Law enforcement agencies ultimately identified the administrator, Ross Ulbricht, through advertisements and coding queries that he had posted to the web in the early days of the site's development, and he was subsequently arrested and charged with narcotics trafficking, money laundering, computer-hacking and attempted murder.[49]

3.45 Similarly, AlphaBay—described by the US Department of Justice as the 'largest criminal marketplace on the Internet'—was shut down in 2017 following an international operation to seize AlphaBay's infrastructure.[50] The creator and administrator, Alexandre Cazes, was arrested by Thai authorities on behalf of US authorities and charged with a number of offences including conspiracy to commit racketeering, distribution of narcotics, identity theft, device fraud and money laundering. US law enforcement authorities worked with foreign partners to freeze and preserve millions of dollars' worth of cryptocurrencies, representing the proceeds of AlphaBay's illegal activities. The US Attorney General stated that:

> This is likely one of the most important criminal investigations of the year – taking down the largest dark net marketplace in history. Make no mistake, the forces of law and justice face a new challenge from the criminals and transnational criminal organizations who think they can commit their crimes with impunity using the dark net. The dark net is not a place to hide.[51]

Cryptocurrencies

3.46 Cryptocurrencies are a form of digital currency where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Digital currencies potentially offer a cheaper, more efficient and faster method of payment. According to AUSTRAC 'digital currency' is defined as:

[48] United States (US) Department of Justice, 'First nationwide undercover operation targeting darknet vendors results in arrests of more than 35 individuals selling illicit goods and the seizure of weapons, drugs and more than $23.6 million', *Media release*, 27 June 2018, https://www.justice.gov/usao-mdpa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35 (accessed 18 March 2019).

[49] Hal Hodson, 'Silk Road bust hints at FBI's new cybercrime powers', *New Scientist*, 4 October 2013, https://www.newscientist.com/article/dn24345-silk-road-bust-hints-at-fbis-new-cybercrime-powers/ (accessed 18 March 2019).

[50] The US Department of Justice, 'AlphaBay, the largest online 'dark market' shut down', *Media release*, 20 July 2017, https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down (accessed 18 March 2019).

[51] Jeff Sessions, cited in 'AlphaBay, the largest online 'dark market' shut down'.

> …[a] digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the digital currency.[52]

3.47 Cryptocurrencies give users a degree of anonymity and an alternative to currencies controlled by central banks and governments, making them attractive to organised criminal groups and for illicit activities such as money laundering, tax avoidance and purchasing illicit goods and services. As AUSTRAC explained, digital currencies offer:

- greater anonymity compared with traditional non-cash payment methods;
- limited transparency because transactions are made on a peer-to-peer basis, generally outside the regulated financial system; and
- different components of a digital currency system that may be located in many countries and subject to varying degrees of oversight.[53]

3.48 ASIC stated that the difficulty in gaining direct access to the dark web and the limited direct visibility of conduct perpetuated through it is compounded by the use of virtual currencies such as Bitcoin.[54]

3.49 In response to the risks posed by digital currencies, the Australian Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* in December 2017. The Act included the first phase of reforms to Australia's anti-money laundering and counter-terrorism financing regulation framework, designed to close a regulatory gap by regulating digital currency exchange providers.[55]

3.50 AUSTRAC reported that it has been working on a number of private, business and academic partnerships to address the law enforcement challenges of digital currencies, including:

- working with digital currency exchange providers to gain greater insight into the operation of the sector and to assist them in implementing the regulatory reforms;
- the Fintel Alliance, a public-private collaborative partnership through a national Centre of Excellence for financial intelligence, providing enhanced

[52] Australian Transaction Reports and Analysis Centre (AUSTRAC), *Submission 30*, p. 5. See also Chapter 1 for discussion of cryptomarkets.

[53] AUSTRAC, *Submission 30*, p. 5.

[54] ASIC, *Submission 11*, p. 5.

[55] AUSTRAC, *Submission 30*, p. 5.

information and intelligence-sharing arrangements that helps to identify and investigate serious crimes affecting Australia;

- an Operations Hub focused on the Mossack Fonseca matter (Panama Papers), identifying and profiling online money mules, and enhancing the use of the Australian Cybercrime Online Reporting Network (ACORN) data;
- an 'Alerting Initiative' enabling the discovery of financial crime risks through joining disparate and distributed data silos; and
- the Business Research and Innovation Initiative (BRII), conducted by the Department of Industry, Innovation and Science, to develop innovative solutions for government policy and service delivery challenges.[56]

Botnets

3.51 Dark web markets also sell technologies such as hacking tools and offer botnets for sale or hire. Botnets are 'zombie' computer networks comprising up to millions of compromised but legitimate devices connected to the internet. A botnet user is able to launch a 'Distributed Denial of Service' cyberattack against any organisation connected to the internet.[57] The CSRC advised that '[f]or as little as $5 it is possible to hire enough botnet capability to block a large online store site for five minutes'.[58]

Communication interception

3.52 DHA, AGD and ABF warned that encryption in devices and applications is having a serious impact on criminal and national security investigations and prosecutions, preventing law enforcement agencies from accessing communications, even where this interception has been undertaken lawfully:[59]

> Lawfully intercepted or accessed communications are difficult or impossible to be decrypted and used operationally. Over 65 per cent of data being lawfully intercepted by the AFP now uses some form of encryption. Encryption impacts at least nine out of every 10 of ASIO's priority cases. ABF activities to disrupt and deter organised criminal activities, such as the importation of drugs and pre-cursor chemicals as well as systematic revenue evasion, often encounters sophisticated methodologies using ICT. It is estimated that by 2020 all electronic communications of investigative value will be encrypted. In most instances encryption is incapable of being overcome, limiting the possible avenues for law enforcement to investigate a criminal operation.[60]

[56] AUSTRAC, *Submission 30*, pp. 8–9.

[57] CSRC, *Submission 8*, p. 7. See also GPEN, *Submission 19*, p. 5.

[58] CSRC, *Submission 8*, p. 7.

[59] DHA, AGD and ABF, *Submission 28*, p. 9.

[60] DHA, AGD and ABF, *Submission 28*, p. 16.

3.53 Mr Andrew Warnes, Assistant Secretary, Communications Security and Intelligence Branch, AGD, outlined the nature of the problem:

> Before you had a very small number of telecommunications providers through which communications transited. In actual fact, going back some way, you might have had only one you had to deal with, and they were government owned. That's obviously changed significantly now. The obligations that sit under the Telecommunications Act 1997 under section 313 for reasonable assistance to law enforcement only applies now to the subset of telecommunications providers that are on the carriers and not to the over-the-top providers, the social media platforms and things. When you now put on an intercept, that communication may be potentially encrypted and you may not get information back that is in a usable form or you may get information that takes some time for you to be able to decipher and use.[61]

3.54 DHA, AGD and ABF noted that there are cases where the problem of encryption has the potential to be addressed, particularly in devices intercepted at Australia's borders. However, 'inconsistent capabilities across different law enforcement agencies inhibit this from taking place', and they recommended that this vulnerability could be addressed if law enforcement agencies pooled their resources.[62]

3.55 The CSRC commented that '[c]riminal use of uncrackable encrypted mobile phones has become a significant obstacle to effective law enforcement investigations'[63] and echoed the issues described by the DHA, AGD and ABF about the 'national effort in fighting cybercrime' lacking coordination and cooperation. Mr David Irvine, Chair, CSRC remarked:

> At the moment, it's fractionated, fragmented, between state police forces, numerous federal government agencies and so on, each operating under their own separate legislation, often, and some with really high-density pockets of expertise in one particular area that are not necessarily replicated in the state next door or whatever.[64]

3.56 The scale of the encryption challenge was illustrated in the US where the Federal Bureau of Investigation (FBI) reported that, over an 11-month period, it was unable to access over half (about 7000) of the seized mobile devices in its possession due to encrypted content. As a result, the US Department of Justice has called for tech companies to implement 'responsible encryption', allowing law enforcement to access

[61] Mr Andrew Warnes, Assistant Secretary, Communications Security and Intelligence Branch, AGD, *Committee Hansard*, 11 May 2018, pp. 48–49.

[62] DHA, AGD and ABF, *Submission 28*, p. 16.

[63] CSRC, *Submission 8*, p. 6.

[64] Dr David Irvine, Chair, CRSC, *Committee Hansard*, 29 March 2018, p. 23.

data only with judicial authorisation, similar to existing access provisions relating to security keys, key recovery for forgotten passwords, and operating system updates.[65]

3.57 The Western Australia Police Force (WA Police) outlined the scope of the encryption challenge for state and territory law enforcement:

- Common residential grade mobile telephones and computer systems now incorporate encryption for data security and transmission which cannot be defeated by police agencies. In many instances these encryption services are turned on by default and used without the knowledge of the operator.
- Many off site data storage services are moving to a form of encryption where the encryption keys are held by the user. This means the service provider cannot access the data held in their storage facilities, a common sense approach which relieves the service provider of any responsibility for the data stored therein. Whilst this approach does alter the challenge for police, it has the advantage of removing service providers from any role in censorship or monitoring of their clients' data.
- An increasing proportion of Internet traffic now uses some form of encryption which makes midstream interception unreadable. In short, this means data and telephone interceptions captured by police are encrypted and cannot be understood.
- It appears that major telecommunications service providers are moving all communications services to Voice over Internet Protocol (VoIP). VoIP uses standard Internet protocols to transmit its information, and is frequently encrypted and cannot be decrypted by police. This technology has the potential to render telephone interception methods ineffective.[66]

3.58 With regard to interception, Dr Coyne argued:

> …philosophically, we need to stop looking backwards and look forwards and be real about what we can achieve. We may not say it out loud but the question in committees like this and in submissions has always been: how do we return intercepts back to the days of the 1970s and 1980s? How do we get back to having that level of telephone intercept capability? That may not be the real question. The real question is: how do we collect sufficient intelligence to undertake the investigations that make our community safer? The answer to that may not be in the legislation. It's going to cost more money because there'll be more surveillance, more listening devices, more tracking devices. It could be more physical surveillance in the sense of people travelling backwards and forwards across jurisdictions and working with foreign partners. Unfortunately, looking forward, what we can't do is keep on asking ourselves this backwards question…I think it's about police

[65] The US Department of Justice, 'Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy', 10 October 2017, cited in ASIC, *Submission 11*, p. 6.

[66] Western Australia Police Force (WA Police), *Submission 31*, p. 7.

> changing their techniques. I just don't think that we're going to be able to legislate our way out of this at all.[67]

3.59 Dr Coyne reflected on the cyber "arms race" between criminals and law enforcement, stating:

> What I'd like to see is the gap or the space between the time that criminals institute these new capabilities and the time we take to react to them to close. At the moment, the key message here, especially in the technology space, is that that problem, the time gap, is getting wider. We want to close that time gap. I think that needs to be the key priority.[68]

Disruption

3.60 Disruption techniques are commonly used by law enforcement agencies as a means to disrupt the supply of encrypted telecommunication devices such as phones, seeking to prevent the targeted phones from being distributed to members of the public. This is often achieved by bringing charges contrary to the proceeds of crime offence provisions. Suppliers may also be prohibited from mainstream banking, and the agents selling them subject to surveillance on the basis that they have no legitimate reason to use high-grade encryption to communicate.[69]

3.61 The International Association of Prosecutors, Global Prosecutors E-Crime Network (GPEN) noted that law enforcement agencies in the US and Europe have had some success in disrupting activity on the dark web.[70]

3.62 Dr Coyne stated that 'a very small yet incredibly successful number of enforcement officers are focussed on the disruption of threats' in Australia.[71] He noted, however, that there is a prevailing misconception that the aim of law enforcement is to arrest people, and that agencies are held accountable through key performance indicators such as arrests, seizures and successful prosecutions. Rather, he argued that the aim is to make society safer, and he cited examples where alternative approaches to law enforcement such as disruption have been effective in deterring crime:

> The chances of us prosecuting a number of cybercriminals is very, very low. The chance that we'll collect sufficient evidence to be able to prove to a foreign jurisdiction and then go through the process, which would be incredibly costly, of bringing those people to Australia, even when it is possible, and proving beyond reasonable doubt that they are guilty is very low to unlikely, I suspect. And, as a result of that, we have to look at

[67] Dr John Coyne, *Committee Hansard*, 29 March 2018, pp. 6–7.

[68] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 7.

[69] Nyman Gibson Miralis Defence Lawyers and Advisors, *Submission 27*, [p. 2].

[70] GPEN, *Submission 19*, p. 5.

[71] Dr John Coyne, *Submission 4*, p. 6.

> alternative mechanisms to disrupt them...if you keep on pushing law enforcement to increase the percentage of seizures, they'll focus only on that, not on reducing the supply, and those are two different outcomes.[72]

3.63 Mr Matthew Loeb, Chief Executive Officer, ISACA, considered that, whilst disruption can unsettle criminals, it does not necessarily eradicate the potential risk. He argued that one of the most critical challenges is containing attacks and mitigating the risk of greater harm to a larger group of people. For example:

> …if there is a situation where a cyber related incident could lead to a physical incident, there may have to be a strategy to disrupt that to prevent harm to many, recognising that there may be a risk of harm to a few. These are difficult choices. I'm not a law enforcement official, but I can imagine the stress that goes with trying to size up those situations in order to maximise public safety.[73]

Accessing cloud-stored data

3.64 Cloud computing provides for storing and potential processing of data offsite from a person's or entity's main premises. Data is often stored overseas or replicated across numerous data centres. Data stored in the cloud may also be encrypted, and some providers implement a 'zero knowledge system', meaning that all data held in the cloud is encrypted by the client before being transmitted and stored in the cloud and cannot be decrypted without obtaining the encryption key from the client.[74]

3.65 Scram Software remarked that the use of technologies such as cloud computing, biometrics, genomics, big data has led to more sensitive information being stored digitally on servers that are vulnerable to cybercrime and human error resulting in data breaches.[75]

3.66 ASIC stated that, in addition to encryption, cloud computing poses particular challenges associated with 'geographical disparity and forensic imaging', as follows:

(a) it can be difficult to identify the precise location of the data (which may be spread across multiple storage servers);

(b) if data is stored overseas, ASIC's immediate information-gathering powers no longer apply and the provider may be restricted by local laws as to the provision of any information to ASIC; and

(c) it can take a significant amount of time to capture data from a cloud storage location over the internet (depending on the server hosting the

[72] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 4.

[73] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 13.

[74] ASIC, *Submission 11*, p. 6.

[75] Scram Software, *Submission 5*, p. 3.

> data and the internet connection used to acquire it), particularly for a large dataset.[76]

3.67 The ACIC and AIC warned that the increasing reach of the global communications supply chain means that more Australians are using services provided by offshore entities, with implications for Australian law enforcement:

> The issue of accessing communications is further amplified as the amount of stored communications and telecommunications data held by traditional carriers and carriage service providers is decreasing as more individuals are using third party applications or over the top providers, which are also commonly offshore entities.[77]

3.68 The ACIC and AIC noted that, while law enforcement agencies can lawfully access stored communications and telecommunications data held by Australian carriers and providers, they are required to engage in the Mutual Legal Assistance Treaties (MLAT) process to access data held offshore, and that process can take 18 months or more.[78] The AFP and AGD similarly described MLATs as 'a very difficult process',[79] explaining that the 'sheer volume' of MLATs—which go through a central authority in New York—is a significant contributor to delays.[80] The AFP also clarified that '[t]o be clear, it's not pushback or a reluctance on behalf of the service providers; it's the bureaucratic process attached to it to get it to the service provider'.[81]

3.69 The WA Police submitted that, whilst mechanisms to facilitate inter-jurisdictional law enforcement cooperation, such as MLATs, enable police to access digital evidence in serious offences, cloud-stored data usually involves non-serious offences where data is stored offsite without the user's knowledge. In addition, the data may be stored in a different jurisdiction than the service provider's headquarters, and the service provider may not be able to access the data due to customer privacy encryption.[82]

[76] ASIC, *Submission 11*, p. 7.

[77] ACIC and AIC, *Submission 29*, p. 8.

[78] ACIC and AIC, *Submission 29*, p. 8; Mr Michael Phelan, Chief Executive Officer, ACIC, *Committee Hansard*, 11 May 2018, p. 45. See Chapter 2 for further discussion of Mutual Legal Assistance Treaties.

[79] Mr Andrew Warnes, Assistant Secretary, Communications Security and Intelligence Branch, AGD, *Committee Hansard*, 11 May 2018, p. 45.

[80] Mr Ramzi Jabbour, Deputy Commissioner, Capability, AFP, *Committee Hansard,* 11 May 2018, p. 45.

[81] Mr Ramzi Jabbour, Deputy Commissioner, AFP, *Committee Hansard*, 11 May 2018, p. 45.

[82] WA Police, *Submission 31*, p. 2.

3.70 Professor Dan Jerker B Svantesson identified 25 issues regarding privately-held cloud stored data that need to be taken into account when designing a 'functioning international system':[83]

> A key challenge in designing a functioning international system ensuring effective law enforcement access to cloud-stored data held by private parties, while maintaining appropriate safeguards, is to determine when law enforcement has jurisdiction to request data held by a foreign company, or indeed, held by a domestic company but stored on servers in another country. In this context, we need to move away from territoriality as a core principle of jurisdiction, in favour of a framework that fits better with the world we live in today.[84]

3.71 WA Police advised that police are often unable to access cloud-stored data for legal reasons, and that legislation has failed to keep pace with technological advances and its effect on society and criminal behaviour.[85] They submitted that legislative reform is required to enable police to seize offsite data that is accessed or controlled from another jurisdiction:

> These would require minor amendment to allow seizure from unique locations on the internet, as well as an accompanying power to demand access codes with associated non-compliance penalties.[86]

3.72 WA Police also noted that Commonwealth and Victorian legislation allows offsite data to be seized if police have and use the devices used to store and access the data, and argued that this approach should be extended to include access or control from within a jurisdiction:

> For example, if police can satisfy a judicial authority that data has been accessed or controlled from a jurisdiction, then that data is deemed to be in that jurisdiction and can be seized from that jurisdiction using the relevant search and seizure laws. These would require minor amendment to allow seizure from unique locations on the internet, as well as an accompanying power to demand access codes with associated non-compliance penalties.[87]

3.73 AGD discussed the recently enacted *Clarifying Lawful Overseas Use of Data Act 2018* (US) (CLOUD Act) which has established a regime permitting countries to negotiate 'bilateral agreements with particular safeguards in those agreements with the United States':

> Congress has an opportunity to endorse or reject those agreements and that will provide the ability to serve warrants of a domestic country on a US provider directly, so circumventing the mutual assistance process. I think,

[83] Professor Dan Jerker B Svantesson, *Submission 3*, p. 8.

[84] Professor Dan Jerker B Svantesson, *Submission 3*, p. 2.

[85] WA Police, *Submission 31*, p. 2.

[86] WA Police, *Submission 31*, p. 3.

[87] WA Police, *Submission 31*, p. 3.

> chair, maybe some of your questions today are going to what can be done. I think the answer might be that these are the types of arrangements that may need to be set-up.
>
> We know that the UK is in the process of negotiating what would be the first agreement with the US around this. The Minister for Law Enforcement, Minister Taylor, has already publicly said he is very keen for Australia to be next and to negotiate an agreement, so that's what we'll be looking to do, because we can certainly see the value of trying to fix that problem we have with mutual assistance around the time it takes to get that information from those communications providers based in the US.[88]

Using traditional and cyber-enabled investigation techniques

3.74 The CSRC argued that criminal activity committed via cyberspace requires both traditional law enforcement investigation techniques and cyber exploitation and investigation techniques:

> Law enforcement agencies have long used elements of Cyberspace, including the information stored within it, to assist in criminal investigations. The use of telecommunications metadata and CCTV systems are well-understood examples. A key challenge in the fight against criminal activity using the vector of Cyberspace is the ability of agencies to keep up with the rapidity and constancy of changes in cybercrime technology and the modus operandi of criminal activity. For example, the use of Ransomware as an extortion tool is estimated by one source to have increased 2000% in the last two years as the new generation of cyber criminals increasingly resemble traditional organised crime syndicates.[89]

3.75 As previously noted (see paragraph 3.58), Dr Coyne suggested that, given the increasing use of encryption for criminal purposes, the solution for law enforcement may lie in adopting alternative—and potentially more costly—investigative techniques to telephone interception.[90]

3.76 Given the nature of its work, the Australian Commission for Law Enforcement Integrity (ACLEI) often investigates people who have intimate knowledge of the cyber capabilities and weaknesses of law enforcement agencies. ACLEI stated that much of the information it gathers is done so covertly, 'including through lawful access to digital records, and by using electronic surveillance capabilities'.[91]

[88] Mr Andrew Warnes, Assistant Secretary, Communications Security and Intelligence Branch,AGD, *Committee Hansard*, 11 May 2018, p. 45.

[89] CSRC, *Submission 8*, p. 9.

[90] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 6. See also Chapter 6 for further discussion of the challenges for law enforcement in securing electronic evidence.

[91] ACLEI, *Submission 1*, p. 1.

3.77 ACLEI remarked:

> Ensuring access to retained data has been an important measure in the fight against organised crime and corruption. Even so, encryption and other counter-JCT surveillance methods being used by criminal groups continue to impact law enforcement reach and efficiency.[92]

3.78 As a result, ACLEI has begun adapting its operational strategies using the statutory framework available to it, including through the use of:

- physical surveillance;
- human source intelligence;
- agreements with private and public entities to access collected data for a law enforcement purpose;
- better data management and connectivity of internal data sets;
- dissemination of information and intelligence to (and from) other entities;
- computer forensics;
- forensic accounting; and
- coercive hearings, held under Part 9 of the *Law Enforcement Integrity Commissioner Act 2006* (LEIC Act).[93]

3.79 ACLEI noted, however, that these strategies tend to be 'more labour intensive and costly alternatives' compared to "traditional" telephone interception and related tactics, and that they also have the potential to increase the risk that a person of interest will be alerted to ACLEI's investigation earlier than is presently the case which may compromise or limit the investigation.[94]

3.80 Several submitters identified mechanisms that may help to address this problem. ACLEI recommended that consideration be given to a statutory framework for Delayed Notification Search Warrants (DNSW) for serious crime and corruption offences, as used by the New South Wales Police and the Australian Federal Police (AFP). Such a strategy would assist ACLEI to obtain information covertly, particularly as ICT surveillance methods become increasingly limited:[95]

> Since corruption thrives on secrecy-and law enforcement corruption thrives on insider knowledge to hide tracks and avoid detection-a DNSW regime would be a particularly valuable means of ACLEI obtaining information

[92] ACLEI, *Submission 1*, p. 2.

[93] ACLEI, *Submission 1*, p. 2.

[94] ACLEI, *Submission 1*, p. 2.

[95] ACLEI, *Submission 1*, p. 2.

> covertly, especially when the effectiveness of ICT surveillance methods may become more limited in future.[96]

3.81 Dr Coyne suggested that the ACIC establish an 'Indicators and Warning (I&W) solution' to address the problem of illicit marketing of drugs or weapons via the dark web, in order to identify disruptive changes in the global supply illicit chains that impact on Australia's market.[97]

3.82 Dr Coyne also recommended that an independent entity, like the Australian Strategic Policy Institute (ASPI), be engaged to review current models used by agencies within the Home Affairs portfolio for categorising and prioritising cases, and that Home Affairs should consider how existing network-focussed strategies, such as the one used to close Silk Road, can be further enhanced.[98]

3.83 WA Police stated that the scope of criminal activity conducted within the dark web is not well understood, and recommended that a national working party be established to develop, in consultation with law enforcement professionals, a 'cohesive national strategy for understanding or addressing the challenge' of the dark web.[99] WA Police suggested that the working party could begin by examining data collected by the ACIC's Encrypted Communications Working Party in 2014−15.[100]

Committee view

3.84 The challenges to law enforcement posed by criminal activity 'going dark' are significant and ongoing. As the implementation and uptake of encryption increases, including through the use of entirely legal infrastructure such as 5G networks, the impact on law enforcement's capacity to detect and disrupt cyber and cyber-enabled crime will only be exacerbated.

3.85 The committee is cognisant of avoiding duplication of effort and resources in addressing many of the cyber challenges facing law enforcement, which are largely consistent between federal and state and territory agencies (and indeed globally). The committee therefore considers that the National Cybercrime Working Group, which is currently overseeing the development of a new National Plan to Combat Cybercrime, is best placed to review the results of the Encrypted Communications Working Party

[96] ACLEI, *Submission 1*, p. 2.

[97] Dr John Coyne, *Submission 4*, p. 8.

[98] Dr John Coyne, *Submission 4*, p. 8. 'Silk Road' was an online marketplace operating in the dark web where buyers could browse the market anonymously using cryptocurrency. It was successfully shut down by US government agencies in 2013. More recently, the US Justice Department shut down AlphaBay, a dark website ten times the size of Silk Road. See ASIC, *Submission 11*, p. 4.

[99] WA Police, *Submission 31*, p. 6.

[100] WA Police, *Submission 31*, p. 7.

undertaken for the ACIC in 2014−15, and to consider the merits of initiatives proposed during this inquiry, including:

- a national statutory framework for Delayed Notification Search Warrants for serious crime and corruption offences, such as that currently used by the New South Wales Police and the AFP;
- a framework for an Indicators and Warning system, to sit within the ACIC, aimed at identifying disruptive changes in the global supply illicit chains that impact on Australia's market;
- an independent entity to review current case categorisation and prioritisation models used by agencies within the Home Affairs Portfolio; and
- a review of how existing law enforcement strategies to tackle activities facilitated by the dark web, such as that used to close Silk Road, can be enhanced for wider application.

Recommendation 1

3.86 The committee recommends that the National Cybercrime Working Group examines and reports on the merits of the following initiatives as part of its work developing a new National Plan to Combat Cybercrime:

- **a national statutory framework for Delayed Notification Search Warrants for serious crime and corruption offences;**
- **a framework for an Indicators and Warning system, to sit within the ACIC, aimed at identifying disruptive changes in the global illicit supply chains that impact on Australia's market;**
- **an independent entity to review current case categorisation and prioritisation models used by agencies within the Home Affairs Portfolio; and**
- **a review of how existing law enforcement strategies to tackle activities facilitated by the dark web, such as that used to close Silk Road, can be enhanced for wider application.**

Chapter 4

Responding to the encryption challenge

4.1 As discussed in Chapter 1, the increasing prevalence of encrypted data and communications represents a significant challenge to current investigative and interception capabilities in law enforcement. As the Australian Securities and Investments Commission (ASIC) stated:

> While encryption has clear benefits in safeguarding the privacy and security of sensitive data, it poses challenges for law enforcement agencies in obtaining access, in appropriate cases, to the encrypted content and devices.[1]

4.2 The Australian Criminal Intelligence Commission (ACIC) and Australian Institute of Criminology (AIC) emphasised the increasing role of encrypted communication devices and applications in criminal activities:

> Increasingly, criminal activities are committed with the assistance of technology either via the online environment or through advances in technological capabilities, such as secure communications which include but are not limited to communication devices with military grade encryption, remote wipe capabilities, duress passwords and secure cloud-based services…The online environment enables crime to be committed with relative anonymity, a characteristic that is attractive to serious and organised crime groups and other motivated individuals, making the identification and prosecution of offenders more difficult.[2]

4.3 Similarly, ISACA noted that nations across the world have been grappling with the encryption challenge for several years, and submitted that the most effective way to address this challenge is to focus law-enforcement efforts on research and development.[3]

4.4 Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia and Future Wise noted that governments continue to argue for greater powers to address the encryption challenge:

> The rationale behind this argument is that encrypted messaging apps are having detrimental impacts on their ability to prevent, detect and investigate serious crimes such as terrorism and the distribution of child exploitation

[1] Australian Securities and Investments Commission (ASIC), *Submission 11*, p. 6.

[2] Australian Criminal Intelligence Commission (ACIC) and Australian Institute of Criminology (AIC), *Submission 29*, p. 4.

[3] ISACA, *Submission 13*, [p. 7].

material. Accordingly, these agencies insist that further powers are needed to enable access to encrypted communications.[4]

4.5 Dr Mann et al rejected this claim, instead arguing that:

> In spite of any claims that end-to-end encryption tools introduce insurmountable obstacles for intelligence gathering and criminal investigation, we insist that our present digital age offers an unparalleled opportunity for intelligence gathering and criminal investigation compared with any previous point in history. Australian authorities already have extensive technical and legal capabilities at their disposal to gather, store, and analyse social and geolocational data to facilitate operations.[5]

Five Eyes Alliance Statement of Principles

4.6 As outlined in Chapter 2, the Five Eyes Alliance is an intelligence alliance formed in 1946 and now comprising the United Kingdom (UK), United States (US), Canada, Australia and New Zealand (NZ).

4.7 On 26 June 2017, the Five Country Ministerial Meeting of the Five Eyes Alliance partners discussed the shared challenge of encryption, noting that it can severely undermine public safety efforts by 'impeding lawful access to the content of communications during investigations into serious crimes'. In response, the partners committed to engaging with communications and technology companies to explore shared solutions which 'proportionately balance the cybersecurity and the rights and freedoms of individuals'.[6]

4.8 On 29 August 2018, a joint meeting was held between the Attorneys-General and Interior Ministers from the Five Eyes nations to further discuss encryption and the problem of 'going dark'. This meeting resulted in the development of a framework for discussion with industry to resolve the challenge of encryption 'while respecting human rights and fundamental freedoms'.[7]

4.9 The agreement was set out in the Five Eyes Alliance *Statement of Principles on Access to Evidence and Encryption* (Statement of Principles), affirming:

(i) a mutual public safety responsibility between governments and technology providers that obliges assistance, while recognising the need to 'ensure the ability of citizens to protect their sensitive data';

[4] Dr Monique Mann, Dr Adam Molnar, Dr Ian Warren and Dr Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia and Future Wise, *Submission 23*, p. 11.

[5] Dr Monique Mann et al, *Submission 23*, p. 12.

[6] Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF), *Submission 28*, p. 17.

[7] DHA, 'Five Country Ministerial 2018: official communiqué', *Media release*, 30 August 2018, p. 3.

(ii) the primacy of the rule of law and due process protections to ensure that 'lawful access should always be subject to oversight by independent authorities and/or subject to judicial review'; and

(iii) '[f]reedom of choice for lawful access solutions' so that technology providers can 'voluntarily establish…customised solutions, tailored to their individual system architectures that are capable of meeting lawful access requirements'.[8]

4.10 The Statement of Principles explain that 'appropriate government authorities should be able to seek access to otherwise private information when a court or independent authority has authorised such access based on established legal standards', similar to the principle that allows government authorities to search homes, vehicles, and personal effects with valid legal authority.[9]

4.11 The Statement of Principles notes the 'increasing gap between the ability of law enforcement to lawfully access data and their ability to acquire and use the content of that data'. It indicates that each of the Five Eyes jurisdictions will consider how best to implement the principles, including with the voluntary cooperation of industry partners.[10]

Five Eyes encryption laws

4.12 Of the Five Eyes partners, the UK and New Zealand have existing laws obliging industry to assist with access to encrypted communications, whereas the US and Canada have not as yet amended existing provisions to impose comparable requirements on technology providers.[11]

4.13 The *Investigatory Powers Act 2016* (UK) extends the Secretary of State's power to issue 'technical capability notices to require telecommunications operators to

[8] Five Country Ministerial/Quintet Meeting of Attorneys-General Australia 2018, 'Statement of principles on access to evidence and encryption', DHA, 30 August 2018, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F6345572%22 (accessed 21 January 2019).

[9] DHA, 'Statement of Principles on Access to Evidence and Encryption', https://web.archive.org/web/20180925154820/https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption (accessed 22 January 2019).

[10] DHA, 'Statement of Principles'.

[11] *Investigatory Powers Act 2016* (UK), http://www.legislation.gov.uk/ukpga/2016/25/contents; and *Telecommunications (Interception Capability and Security) Act 2013* (NZ), http://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177923.html (all accessed 21 January 2019).

maintain the capability to provide data in an intelligible format where it is proportionate, technically feasible and reasonably practicable to do so'.[12]

4.14 New Zealand's powers are broadly analogous to technical capability notices under the UK's legislation, whereby the New Zealand government can 'compel assistance from service providers to decrypt information in response to a warning provided by a "surveillance agency"'.[13]

Australia's new encryption laws

4.15 Australia was the first of the Five Eyes Alliance to introduce encryption legislation since the release of the Statement of Principles.

4.16 The Minister for Home Affairs, the Hon Peter Dutton MP, introduced the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 on 20 September 2018. The Explanatory Memorandum outlined the purpose of the legislation as follows:

> National security and law enforcement agencies already work cooperatively with industry and other partners in relation to a range of telecommunications interception matters. The Bill will enhance cooperation by introducing a new framework for industry assistance, including new powers to secure assistance from key companies in the communications supply chain both within and outside Australia (Schedule 1). It will also strengthen agencies' ability to adapt to a digital environment characterised by encryption by enhancing agencies' collection capabilities such as computer access (Schedules 2, 3, 4 and 5).
>
> The computer access powers in Schedules 2 to 5 will enable domestic law enforcement agencies to better assist international law enforcement partners by undertaking these powers on behalf of those partners where approved through Australia's mutual assistance framework. These powers recognise the fact that computers, communications and encryption are now global and perpetrators of crimes and terrorist acts have a global reach through these mediums. This will be based on the principle of reciprocity—that Australia will work with those who work with Australia—and any other conditions the Attorney-General deems appropriate.[14]

4.17 The Attorney-General, the Hon Christian Porter MP, referred the Bill to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for consideration.

[12] DHA, AGD and ABF, *Submission 28*, p. 17; see also Ms Esther George, Lead Cybercrime Consultant, International Association of Prosecutors, *Committee Hansard*, 29 March 2018, p. 46.

[13] DHA, AGD and ABF, *Submission 28*, p. 17.

[14] House of Representatives, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, *Explanatory Memorandum*, pp. 2–3, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195 (accessed 12 December 2018).

4.18 Following a government request to expedite the inquiry, the Chair and Deputy Chair of the PJCIS issued a statement pointing to the committee's reviews of previous national security laws, stating that its reports had 'been carefully developed to ensure that new powers are proportionate and appropriately balanced with human rights and privacy, and that commensurate oversight and accountability is provided'.[15]

4.19 On 22 November 2018, the committee received advice from the Minister for Home Affairs that 'there was an immediate need to provide agencies with additional powers and to pass the Bill in the last sitting week of 2018'.[16]

4.20 The Minister explained that the request for acceleration of the committee's consideration of the Bill was made 'in light of the recent fatal terrorist attack in Melbourne and the subsequent disruption of alleged planning for a mass casualty attack by three individuals', and concern that Australia's agencies could not rule out the possibility that others may have been inspired to plan and execute terrorist attacks in the forthcoming Christmas-New Year period.[17] The committee stated in its Advisory Report that it accepted:

> …that there is a genuine and immediate need for agencies to have tools to respond to the challenges of encrypted communications. The absence of these tools results in an escalation of risk and has been hampering agency investigations over several years. As the uptake of encrypted messaging applications increases, it is increasingly putting the community at risk from perpetrators of serious crimes who are able to evade detection.[18]

4.21 The committee recommended that the Parliament immediately pass the Bill, following inclusion of amendments recommended by the committee in its Advisory Report. The committee also recommended that, once the Bill (as amended) was passed by the Parliament, the committee undertakes a review of the new legislation to be completed by 3 April 2019.[19] The Bill, with amendments, passed both Houses on 6 December 2018.

[15] Parliamentary Joint Committee on Intelligence and Security (PJCIS), Joint statement by Chair and Deputy Chair, *Media release*, 22 November 2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Media_Releases (accessed 21 January 2019).

[16] PJCIS, *Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, December 2018, pp. 1−2, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1 (accessed 13 December 2018).

[17] PJCIS, *Advisory Report*, p. 2.

[18] PJCIS, *Advisory Report*, p. 2.

[19] PJCIS, *Advisory Report*, Recommendation 1, p. 3 and Recommendation 16, p. 8. The Independent National Security Legislation Monitor is required to review its operation, effectiveness and implications after 18 months.

4.22 On 6 December 2018, the Senate referred the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) to the PJCIS for review and report by 3 April 2019.[20]

Balancing privacy and risk

4.23 The provisions of the new legislation attracted debate in Australia and overseas. Some technology experts warned, for example, that despite the last-minute amendments, the legislation has the potential to damage the credibility of the ICT industry as a result of its provision for voluntary and mandatory industry assistance to help government access the content of encrypted communications.[21]

4.24 The credit ratings group Fitch observed that the new encryption laws would weaken the security of messages, and could harm Australia's flourishing tech sector as well as global operations of tech giants such as Google, Facebook and Apple.[22]

4.25 The Inspector-General of Intelligence and Security (IGIS) submitted to the PJCIS review of the TOLA Act that she had a number of outstanding concerns relating to the scope of IGIS oversight of the new and expanded powers contained in Schedules 2 and 5 to the Act.[23]

4.26 However, Mr Mike Burgess, Director-General of the Australian Signals Directorate (ASD), argued that the new legislation provided 'significant checks and balances' on law enforcement agencies, and was designed to target terrorists, paedophiles and criminals, not law-abiding Australians.[24]

[20] See Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct (accessed 11 February 2019).

[21] See, for example, P Smith, Y Redrup and A Tillett, '"As bad as Huawei": Australian encryption bill slammed after passing House of Reps', *Financial Review*, 6 December 2018, https://www.afr.com/technology/web/security/as-bad-as-huawei-australian-encryption-bill-slammed-after-passing-parliament-20181206-h18tk3; A Bogle, '"Outlandish" encryption laws leave Australian tech industry angry and confused', *ABC News*, 7 December 2018, https://www.abc.net.au/news/science/2018-12-07/encryption-bill-australian-technology-industry-fuming-mad/10589962 (all accessed 11 February 2019).

[22] C Kruger, '"Negative for tech": Fitch slams encryption laws, *Sydney Morning Herald*, 13 December 2018, https://www.smh.com.au/technology/negative-for-tech-sector-fitch-slams-australia-s-new-encryption-laws-20181213-p50m55.html (accessed 20 December 2018).

[23] Inspector-General of Intelligence and Security (IGIS), *Submission 1.1*, PJCIS, Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, pp. 6–8. The overarching purpose of the IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.

[24] Mr Mike Burgess cited in A Probyn, 'Spy chief argues encryption laws target terrorists, not everyday Australians, in "myth-busting" missive', *ABC News*, 12 December 2018, https://www.abc.net.au/news/2018-12-12/encryption-laws-mike-burgess-australian-signals-directorate/10612570 (accessed 20 December 2018).

4.27 The Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF) also pointed out—in their submission to this inquiry—that domestic carriers are already required under the *Telecommunications Act 1997* to provide 'reasonable assistance' to agencies seeking to implement warrants and enforce the law, and noted that the Australian government has stated that companies would not be required to build so-called 'backdoors'. In other words, encryption would continue to secure the private and sensitive information of businesses, governments and individuals.[25]

4.28 Several submitters and witnesses outlined what they saw as potential implications of the new encryption laws. Some raised broader concerns about 'bans', 'backdoors' or other 'weakening' of encryption technologies, and whether it was feasible to facilitate decryption by law enforcement agencies without also making it easier for criminals and foreign spy agencies to access the data.[26]

4.29 Others argued that weakening encryption tools will weaken security of digital communications generally, 'criminalising activities that are important for maintaining public safety, cyber security and digital innovation', as well as having a negative impact on individual privacy and freedom of expression.[27]

4.30 Drs Mann, Molnar, Warren and Daly stated that:

> While it might be the case that such proposals may facilitate law enforcement access to communications at a network-level scale, they will similarly do so for criminal hackers, organised criminals, or foreign state actors who acquire access. Computer scientists have noted that any introduction of a 'backdoor' vulnerability for law enforcement and security intelligence will similarly do so for malicious actors.[28]

4.31 They noted that Australian officials already have a range of selective and targeted technical and legal powers to address the issue of 'going dark'. These include existing powers, via amendments to the *Cybercrime Act 2001* (Cth) that introduced a new section 3LA under the *Crimes Act 1914* (Cth) to provide for lawful authorities to compel passwords, as well as existing powers to facilitate targeting hacking of end-point devices.[29]

[25] DHA, AGD, and ABF, *Submission 28*, p. 16.

[26] See for example, Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, *Submission 2*, [p. 3]; Dr John Coyne, *Submission 4*, p. 5; Pirate Party Australia, *Submission 16*, [pp. 6–7]; Dr Monique Mann, Co-Chair, Surveillance Committee, Board of Directors, Australian Privacy Foundation and Dr Adam Molnar, Vice-Chair, Australian Privacy Foundation, *Committee Hansard*, 29 March 2018, p. 16.

[27] Dr Monique Mann et al, *Submission 23*, p. 12.

[28] Dr Monique Mann et al, *Submission 23*, p. 13.

[29] Dr Monique Mann et al, *Submission 23*, p. 14.

4.32 Mr Nathan White, Senior Legislative Manager, Access Now warned that enabling law enforcement agencies to bypass encryption poses security threats and is unlikely to solve law enforcement's problems, and advocated other means to assist law enforcement in dealing with cybercrime:[30]

> …undermining encryption hurts security. Every proposal for a mechanism to allow law enforcement to bypass encryption has been found to have security flaws that could, if deployed, cause great damage to people, governments and infrastructure. It could also have knock-on effects that we cannot anticipate today…undermining encryption will not solve law enforcement's problems. Principles of sovereignty and criminal incentives will likely drive law enforcement targets toward tools and technologies that are beyond the reach of any mandated access mechanism, leaving those who are less technically sophisticated or financially privileged to bear the brunt of any insecurity caused by the mandate.[31]

4.33 Dr John Coyne similarly argued that:

> …the idea that you can legislate your way out of the encryption challenge is deeply flawed….The bigger debate on this—and the public needs to know this—is that by wiring in back doors and by doing those sorts of approaches, we weaken and undermine all the benefits that come from encryption. It's part of our everyday life. It's what facilitates ease.[32]

4.34 The Law Council of Australia expressed concern that proposed powers contained in the Australian government's new encryption laws could have unintended consequences for the 'privacy and cybersecurity of individuals and regulation of the telecommunications sector'.[33] The Law Council considered that:

> …any restrictions on encryption and online anonymity must be provided for by law and are precise, public and transparent, must only be imposed for legitimate grounds under Article 19(3) of the ICCPR, and must conform to the strict tests of necessity and proportionality. This includes consideration of the possibility that encroachments on encryption and anonymity may be exploited by the same criminal and terrorist networks that the limitations deter.[34]

4.35 Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, stated that compliance to the new laws will only apply to encryption implemented by the company that owns the system, and that it is possible for a user to

[30] Mr Nathan White, Senior Legislative Manager, Access Now, *Committee Hansard*, 11 May 2018, p. 2.

[31] Mr Nathan White, Senior Legislative Manager Access Now, *Committee Hansard*, 11 May 2018, p. 2.

[32] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 5.

[33] Law Council of Australia, *Submission 21*, p. 11.

[34] Law Council of Australia, *Submission 21*, p. 8.

install some encryption software from elsewhere and use it to encrypt files on that company's system.[35]

4.36 In response to the question as to whether it is possible to 'facilitate decryption by legitimate law enforcement, without also making it easier for bad actors such as criminals and foreign spy agencies to access the data too', Dr Teague responded 'No':

> The reason is simply that the legitimate law enforcement operatives are doing (for good reasons) exactly what criminals and other bad actors do: exposing someone else's data without their consent. Any change that makes this easier is likely, unfortunately, to make malicious hacking easier too. There are numerous examples of tools or weaknesses that were employed first for legitimate law enforcement and intelligence purposes, but were later shown to be exploitable by everyone (FREAK/Logjam, Dual-EC-DRBG, Wannacry).[36]

4.37 Ms Lizzie O'Shea and Ms Elise Thomas noted that overseas governments have had little success in regulating encryption, most recently in the UK where the *Investigatory Powers Act 2016* (UK) required technology companies to assist the government to decrypt messages where 'technically feasible':

> Approaches proposed or used in other countries include outright prohibitions on encryption, escrow of encryption keys, or limitations on the strength of encryption. Each of these has been demonstrated to have serious risks…Built-in weaknesses in encryption systems are not features that can be exploited only by the government; they can also be used by criminals and foreign enemies. Information about any backdoor will be highly valuable, and a honeypot for hackers, making it hard to keep safe.[37]

4.38 The Digital Industry Group Incorporated (DIGI) argued that great care must be taken in developing government policy around investigatory powers to ensure that the effectiveness of encryption technology is not comprised, stating that other countries have chosen alternative approaches to legislated intervention:

> A number of governments around the world have rejected such legal and market interventions in favour of a broader policy response which embraces international engagement, technical training for agencies, investment in new investigatory techniques and enhanced company engagement.[38]

4.39 The Law Council also noted that regulation of encryption by other nations has not been shown to be necessary when considering 'the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that

[35] Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, *Submission 2*, [p. 2].

[36] Dr Vanessa Teague, Melbourne School of Engineering, The University of Melbourne, *Submission 2*, [p. 3].

[37] Ms Lizzie O’Shea and Ms Elise Thomas, *Submission 15*, pp. 1−2.

[38] Digital Industry Group Incorporated (DIGI), *Submission 20*, p. 6.

may already provide substantial information for specific law enforcement or other legitimate purposes'.[39]

4.40 DHA, AGD and ABF stated that legal frameworks need to be monitored regularly in order to keep pace with community expectations in this rapidly changing environment. Legal frameworks must 'balance the legitimate needs of law enforcement with the privacy, rights and freedoms of individuals'.[40]

4.41 DHA, AGD and ABF also noted that the legislative response will only ever address some of the law enforcement issues posed by encryption, and predicted that the continuing challenges posed by end-to-end encrypted communications mean that agency powers will need to be continually reviewed:[41]

> In this environment, it will be increasingly important for law enforcement agencies to utilise alternative methods to investigate serious crimes and combat threats to public safety and national security. For this purpose, the range of powers available to agencies must continually be examined.[42]

Committee view

4.42 Over recent years, the Australian government has introduced a series of legislative reforms with the aim of supporting law enforcement in their ability to respond to the threats posed by new and emerging ICTs.

4.43 The government's response to the challenges arising from new and emerging ICTs must balance the needs of law enforcement with the civil rights and liberties of Australians. The committee acknowledges there is an inherent tension between these and those engaged in this debate have, at times, strongly held and opposing views. It is for this reason that where the appropriate balance lies between law enforcement needs and civil rights and liberties must be resolved by the Australian government together with the Australian public, and not just by one or the other.

4.44 The committee accepts that there are cogent arguments put by government and law enforcement agencies for legislative reform to occur expeditiously. However, that need for swift enactment of law enforcement powers should not come at the expense of public engagement and debate on these issues.

4.45 The committee is aware that the UK government ran a seven week formal consultation process on its proposed amendments to the Investigatory Powers Act and the associated draft communications data code of practice, which provided 'more detail on how the new regime will work in practice'. The UK government stated that it 'does not normally consult on such regulations' but 'given the ongoing public interest

[39] Law Council of Australia, *Submission 21*, p. 7.

[40] DHA, AGD and ABF, *Submission 28*, p. 9.

[41] DHA, AGD and ABF, *Submission 28*, p. 16.

[42] DHA, AGD and ABF, *Submission 28*, p. 16.

in investigatory powers we consider it important to consult on potential changes to the legislative regime in order to inform the legislative response and subsequent Parliamentary debate'.[43]

4.46 The UK process was not without criticism, but the committee acknowledges the UK government's efforts to engage the public in the debate about the extent and appropriateness of certain investigatory powers for law enforcement in the cyber environment. The committee urges the Australian government to ensure that public consultation is undertaken when investigatory powers to tackle cybercrime are similarly amended or introduced in this country.

4.47 The committee acknowledges the public debate that has occurred in relation to the TOLA Act, and the range of different views amongst policymakers, law enforcement agencies, legal and technology experts, and users of ICTs, as to the most appropriate balance between law enforcement powers and human rights. The committee expects that the Australian government will carefully consider the views put and these will be appropriately reflected in the legislation.

4.48 The committee recognises that Australia's new encryption laws represent the first legislation to be introduced by a Five Eyes Alliance member since the release of the Alliance's Statement of Principles, and that the new legislation is entering new territory in extending law enforcement powers to access otherwise private information. The committee reiterates the view expressed by the DHA, AGD and ABF that the relevant legislative and regulatory regimes need to be continuously monitored and reviewed in order to identify, in a timely manner, gaps and constraints that may be limiting the ability of Australian law enforcement agencies to respond to the challenges of new and emerging ICTs.

4.49 The committee also considers that the powers given to law enforcement agencies must be subject to regular monitoring to ensure that the legislative and regulatory framework is keeping pace with new and emerging ICTs while respecting the human rights and fundamental freedoms of Australians.

4.50 To this end, the committee suggests that a task force would be an effective and flexible mechanism for monitoring the development of new and emerging ICTs and identifying gaps and vulnerabilities in Australia's law enforcement legislative and regulatory framework, as well as consulting and advising on the balance between investigatory powers and civil rights and liberties.

4.51 The committee envisages that such a task force would comprise ICT, legal, law enforcement and security experts (including academia), and be responsible for reporting to the Australian government at regular intervals on aspects of the legislative

[43] Gov.UK, *Consultation outcome: Investigatory Powers Act 2016*, available: https://www.gov.uk/government/consultations/investigatory-powers-act-2016 (accessed 19 March 2019).

and regulatory framework that may require amendment in order for law enforcement to keep pace with this rapidly changing environment.

Recommendation 2

4.52 The committee recommends that the Australian government considers establishing a task force comprising information and communications technology (ICT), legal, law enforcement and security experts, including from academia, to:

- **monitor the development, and examine and advise on the impact of new and emerging ICTs on Australian law enforcement;**
- **identify specific gaps and vulnerabilities in the current legislative and regulatory frameworks that may be limiting the ability of Australian law enforcement agencies to investigate, disrupt or otherwise deal with cybercrime, including encryption services and encrypted devices;**
- **consult and advise on the balance between investigatory powers to tackle cybercrime and their impact on civil rights and liberties;**
- **report to the Australian government at regular intervals on the appropriateness of current legislative and regulatory frameworks; and**
- **recommend any changes that may be necessary to ensure that law enforcement agencies are keeping pace with and capable of tackling new cyber challenges as they arise.**

Chapter 5

Operational challenges and vulnerabilities

5.1 Law enforcement agencies across Australian and international jurisdictions are confronting a range of similar operational challenges that derive, in part, from the global reach of cybercrime and associated technology.[1]

5.2 The Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF) summarised the challenges and opportunities of new and emerging ICTs for Australian law enforcement.

> The evolving digital environment provides criminals with new avenues to commit a range of serious and complex crimes, including terrorism, firearms and drug trafficking, human trafficking and child sexual abuse. Extremist individuals and terrorist organisations are increasingly using social media and other online tools to facilitate and promote their activities. Similarly, online platforms provide unprecedented connection and storage for the easy sharing, promotion and discussion of child sexual abuse material. New technologies are also making these crimes more complex for law enforcement agencies to investigate. The use of cyber elements for criminal purpose is growing, creating unprecedented risks for both individuals and businesses…New technologies also provide the potential for improved investigative and operational outcomes. The goal is to ensure law enforcement agencies are well-positioned to harness these opportunities, by being nimble and 'ahead of the curve', as well as being capable of tackling new challenges as they arise.[2]

5.3 Dr John Coyne similarly discussed the challenge for Australian law enforcement agencies:

> Divining future developments in technology—and their law enforcement implications—is no easy task: the art of the possible is changing almost daily. The last 15 years of technological advancement is a mere sample of the potentially staggering change that will confront policy makers as we approach 2030. How well governments respond to this change will be dependent on agility in policy development, technology adoption and programme implementation. The big challenge for Australian law enforcement agencies relates to how they create the culture and capability

[1] International Association of Prosecutors—Global Prosecutors E-Crime Network (GPEN), *Submission 19*, p. 5. See Chapter 1 for further discussion of new and emerging ICTs and the implications for law enforcement.

[2] Department of Home Affairs (DHA), Attorney-General's Department (AGD) and Australian Border Force (ABF), *Submission 28*, p. 9.

> development structures to support rapid innovation to protect citizens in a constantly changing landscape.[3]

5.4 The Cyber Security Research Centre (CSRC) observed that, whilst Australia's intelligence and law enforcement agencies are carrying out outstanding work:

> …Australia's emerging national capacity to cope with the pace of change and to counter threats and criminal activity conducted in Cyberspace remains under-developed, uncoordinated and dispersed. There is a pressing need to maximise and build on current expertise dispersed around the country so that Australia is better prepared to face the challenge of countering the malicious misuse of cyber technology.[4]

5.5 This chapter will consider these operational challenges in the context of:

- geographical and jurisdictional constraints;
- workforce skills and capabilities;
- ICT capabilities; and
- data management.

Geographical and jurisdictional constraints

5.6 A key challenge is that, while cybercrime is conducted on a global scale, Australian law enforcement is constrained by geography and jurisdictional reach. This is exacerbated by the fact that commercial entities and criminal offenders operate 'in the digital landscape rather than the geographic or jurisdictional landscapes'.[5]

5.7 In other words, unlike other forms of crime, cybercrime has 'no local flavour'. Data collected by the Western Australia Police Force (WA Police), for example, shows that 30−40 per cent of cybercrime offences are committed by international offenders, and that victims and offenders reside in the same jurisdiction in only seven per cent of cases.[6]

5.8 This has significant implications for law enforcement, as DHA, AGD and ABF explained:

> Crimes can be committed across state and national borders, with the perpetrator located in one jurisdiction and the victim in another. This makes investigations more protracted, expensive and reliant on cooperation between multiple jurisdictions. Investigations into less serious cross-border crimes, where the impact on the victim may be relatively small, become less viable. Regardless of the jurisdiction in which a crime is committed,

[3] Dr John Coyne, *Submission 4*, p. 3.

[4] Cyber Security Research Centre (CSRC), *Submission 8*, p. 10.

[5] Western Australia Police Force (WA Police), *Submission 31*, p. 1.

[6] WA Police, *Submission 31*, p. 1.

> evidence is frequently located offshore due to the range of international companies now supplying communications services to Australians—for example, over the top voice and messaging applications, email and cloud storage.[7]

5.9 Similarly, the Australian Criminal Intelligence Commission (ACIC) and Australian Institute of Criminology (AIC) noted that technology has 'dissolved borders that previously protected victims from offshore offenders'.[8] The availability of technology to reduce law enforcement visibility of serious and organised crime groups' activities has impacted on how law enforcement agencies undertake their work.[9]

5.10 Detective Inspector Tim Thomas, Assistant Divisional Officer for Technology Crime Services, WA Police, explained the approach when the victim of a cybercrime resides in a different jurisdiction to the perpetrator:

> The simple reality for us is very straightforward. We've already given you the statistic that seven per cent of offences have the offender and the victim in the same jurisdiction. The question is: what do we do when they're not in the same jurisdiction?...when we're faced with a very common scenario—say we have a victim in Western Australia who has lost $2,000 in some kind of online fraud, which is very common, and the offender is in another country—we've got two choices: to focus on the offender and try and achieve something or to basically do nothing. So we choose to focus on the offender.[10]

5.11 Detective Inspector Thomas noted that Australian law enforcement uses a national cybercrime management protocol model, although the model is not necessarily well understood or supported across the jurisdictions:

> We have been using this model in Western Australia for three years and we give direct communications to our victims. We tell them exactly what the situation is and what the policing objective is, and we've found that the public are very receptive to this. They understand that the online environment is different to the traditional environment and they understand that the objective of preventing the offender from continuing to offend is, in some cases, the only valid approach that can be taken.[11]

[7] DHA, AGD and ABF, *Submission 28*, p. 9.

[8] Australian Criminal Intelligence Commission (ACIC) and Australian Institute of Criminology (AIC), *Submission 29*, p. 4.

[9] ACIC and AIC, *Submission 29*, p. 4.

[10] Detective Inspector Tim Thomas, Assistant Divisional Officer for Technology Crime Services, WA Police, *Committee Hansard*, 29 March 2018, p. 30.

[11] Detective Inspector Tim Thomas, Assistant Divisional Officer for Technology Crime Services, WA Police, *Committee Hansard*, 29 March 2018, p. 30.

5.12 Mr Matthew Loeb, Chief Executive Officer, ISACA, pointed out that law enforcement agencies are hampered by the lack of international agreements that enable cybercrime to be investigated across multiple jurisdictions:

> I believe the No. 1 biggest challenge here is that even if we can track perpetrators in other places there it is a limitation to enforcement of the criminals because of lack of treaties and legal understandings between nations. Believe it or not, that is also true inside the US—the laws of one state differ from the laws of the other and the interpretations can vary.[12]

5.13 Detective Inspector Thomas John Shillito (John) Manley, Officer in Charge of the Victorian Joint Anti-Child Exploitation team, Victoria Police, stated that the challenge for the Five Eyes Alliance is in finding a more efficient way of coordinating cybercrime-related law enforcement activities across the member countries. He noted that the mutual assistance legislation is cumbersome, having been developed to deal with the world before computers, and law enforcement agencies may pursue alternative paths to facilitate an investigation:[13]

> From my perspective, when it comes to mutual assistance, if we could somehow work out a better way of doing things within the Five Eyes group, that would be hugely helpful—some arrangement where perhaps we had a national Australian warrant, or warrants, depending on what was required, that each law enforcement agency would submit so the international jurisdiction wouldn't have to deal with a whole range of warrants from different states; some national warrant for us to get what we want. The production of that warrant would then cause the internet service provider or whoever in that Five Eyes country to automatically provide the data. That would be really useful. There has got to be some simpler way of doing business.[14]

5.14 Digital Industry Group Incorporated (DIGI) stated that existing international standards for requesting data from jurisdictions other than the United States are outdated and in need of modernisation:

> Efforts are underway to develop new international agreements between like-minded governments which both respect the rights of the individual and provide for the legitimate interests of public safety agencies.[15]

5.15 Dr Adam Molnar, Vice Chair, Surveillance Committee, Australian Privacy Foundation, argued that Mutual Legal Assistance Treaties (MLATs) should be

[12] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 12.

[13] Detective Inspector Thomas John Shillito (John) Manley, Officer in Charge of the Victorian Joint Anti-Child Exploitation team, Victoria Police, *Committee Hansard*, 11 May 2018, p. 33.

[14] Detective Inspector Thomas John Shillito (John) Manley, Officer in Charge of the Victorian Joint Anti-Child Exploitation team, Victoria Police, *Committee Hansard*, 11 May 2018, p. 34.

[15] Digital Industry Group Incorporated (DIGI), *Submission 20*, p. 4.

preserved but 'reconfigured [so that they] actually address the new reality of not just cross-border lawful access requests but also the idea of computer network operations':

> I think some of our colleagues have taken a more narrow view of the role of MLATs in relation to cross-border data access requests to private companies in overseas jurisdictions and some of the rules around disclosing that information, but that's only a more narrow vision of how law enforcement is currently operating across international jurisdiction.[16]

Workforce skills and capabilities

5.16 The issue of law enforcement agencies attracting and retaining suitably skilled staff was an issue that arose throughout the course of the inquiry.

5.17 Mr Loeb stated that, whilst law enforcement agencies may realise the positive benefits of ICTs in their work, their workforces need to be 'grounded in technology and possess a level of expertise that enables them to leverage these technologies to spot criminal activities'.[17]

5.18 Mr Alexandru Caciuloiu, Cybercrime Project Coordinator, Southeast Asia and the Pacific, United Nations Office on Drugs and Crime (UNODC) Regional Office for Southeast Asia and the Pacific, made a similar point:

> As crime gets more specialised and more technological, law enforcement needs to become tech savvy. Law enforcement needs to understand the internet, how technologies work and how to leverage these technologies for the criminal justice process. That involves a lot of knowledge, staff that have very good understanding and training in this area, and also a lot of specialist tools that are very expensive.[18]

Specialist staff

5.19 Several submitters highlighted the challenges associated with recruiting suitable staff and maintaining ICT skills and capabilities in Australian law enforcement agencies, within a rapidly changing ICT environment, although the DHA, AGD and ABF noted that '[t]his is not a challenge faced by law enforcement in isolation'.[19]

[16] Dr Adam Molnar, Vice Chair, Surveillance Committee, Australian Privacy Foundation, *Committee Hansard*, 29 March 2018, p. 19.

[17] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 10.

[18] Mr Alexandru Caciuloiu, Cybercrime Project Coordinator, Southeast Asia and the Pacific, United Nations Office on Drugs and Crime Regional Office for Southeast Asia and the Pacific, *Committee Hansard*, 11 May 2018, p. 39.

[19] DHA, AGD and ABF, *Submission 28*, p. 6. Also see CSRC, *Submission 8*, p. 12.

5.20 When asked about recruitment by the AFP and ACIC, and their ability to attract technology experts, Dr Coyne remarked:

> The short answer to that is in some cases we are, but overall the system doesn't encourage that. Also, the very nature of employment and law enforcement has changed. If you look towards the latest future strategy for the Australian Federal Police, they highlight this. Operationalising that strategy is incredibly difficult. For instance, take the case of obtaining a data scientist. If the AFP wanted to obtain a data scientist and wanted them to be a sworn police officer, they would have to put that person through 12 months at the academy, bring them out of the police academy, give them two years of investigative experience and then return them to being a sworn data scientist. That's clearly not workable. The models that we have for bringing people into the Public Service are flawed in the same way. It's incredibly difficult, at a time when data scientists or forensic accountants are in great demand, to get them to move from our major cities, like Sydney or Melbourne, and take up a job for less money in the Australian Public Service. That is incredibly difficult. This is where we have to revisit these models and look at alternative approaches.[20]

5.21 The CSRC pointed out that, whilst there are currently concentrations of cyber-related expertise within both government and non-government agencies across Australian jurisdictions, law enforcement responses are dispersed and this fragmentation is undermining the ability of agencies to cope with the pace of technological developments. It argued that there should be a better way of coordinating across national, state and territory government agencies, police forces and areas of cyber expertise:

> The national picture…remains one of fragmentation and disaggregation. Resources are scarce—in terms of funding and skilled personnel. There is a severe shortage of cyber experts and cyber-trained investigators within both government and industry. This situation is exacerbated by the relentlessness speed with which the cyber environment evolves; cyber criminals have generally been able to adapt to this evolution and change tactics more quickly than investigative agencies. If not effectively countered, cybercrime will continue to become even more pervasive and public confidence in the efficacy of Australian law enforcement investigations and regulatory compliance measures will diminish. Failure to address cybercrime effectively will also lead to a loss of confidence for businesses operating online in Cyberspace.[21]

5.22 The CSRC also highlighted the importance of concentrating expertise, noting that there are a number of potential non-government partners with cyber security capabilities, including academic centres of excellence and research centres specialising in cyber security and cybercrime studies, as well as specialist advice

[20] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 2.

[21] CSRC, *Submission 8*, pp. 11−12.

available from the private sector producers of technologies exploited by cybercriminals:[22]

> One of the principal benefits is, if you concentrate your expertise, you have a much, much better chance of keeping up with the pace of technological change which is occurring in this sector. If we owe it to our law enforcement to have the best tools available, then this is one potential way of getting there—that is, approaching it on a national basis.[23]

5.23 The CSRC recommended the establishment of a single Commonwealth-led cooperative entity, providing expert cybercrime investigative support services to government, national security and law enforcement agencies. The CSRC argued that such '[n]ational cooperative arrangements would constitute a critical mass of expertise able to operate on a scale that is too difficult and too expensive to achieve in a myriad of small under-resourced cybercrime capabilities spread around the country.'[24]

5.24 The CSRC explained that the proposed entity would not duplicate the roles of existing agencies, but rather that participating agencies would second expert cyber-investigative staff to contribute to investigations conducted by their parent agencies, leveraging common technical skillsets, methods and technologies concentrated in the new entity.[25] Such an entity should also be able to draw on the expertise of the Australian Signals Directorate which, under the *Intelligence Services Act 2001*, is currently limited in its capacity to contribute to Australian law enforcement investigations.[26]

5.25 WA Police noted that specialist ICT-related services such as decryption, chip-off forensics, and some covert services 'will always exceed the resources of a single jurisdiction' and, like the CSRC, recommended the creation of 'centres of capability which are resourced and structured to supply some level of national service'.[27]

5.26 DIGI outlined the 'single point of contact' (SPOC) model, adopted in the United Kingdom (UK), intended to ensure that all law enforcement officers are equipped with the necessary tools and information for tackling crimes involving an online element:

> These designated SPOCs sit within each constabulary and are trained experts in how to obtain, interrogate and analyse digital information which can be instrumental in modern day investigations. The digital industry can focus their training efforts in a much more effective and targeted fashion, and officers within each constabulary have internal experts to draw on to

[22] CSRC, *Submission 8*, pp. 11−12.

[23] Mr David Irvine, Chair, CSRC, *Committee Hansard*, 29 March 2018, p. 23.

[24] CSRC, *Submission 8*, p. 2.

[25] CSRC, *Submission 8*, pp. 13−14.

[26] Mr David Irvine, Chair, CSRC, *Committee Hansard*, 29 March 2018, p. 23.

[27] WA Police, *Submission 31*, pp. 1, 4.

> ask questions, sanity check investigatory options and channel data access requests through. This model came about through a recognition that it could be challenging to ensure that all law enforcement officers are equipped with the necessary knowledge and experience in requesting, interpreting and applying electronic data to an investigation. Recent advances in technologies such as encryption, cloud computing, connected devices, Big Data analytics, artificial intelligence, and virtual reality have presented law enforcement agencies with new methods and tactics for tackling crimes that involve an online element. Given the speed with which emerging technologies and platforms evolve, the SPOC model also makes it easier to keep officers up to date with the latest investigative tools and information.[28]

5.27 The UK National Crime Agency (NCA) has also sought to enhance its workforce through the use of 'volunteer crime-fighters' called 'NCA Specials'. NCA Specials are recruited 'because of their specialist, niche expertise and skills that are rarely available within law enforcement, but that are of huge value in the fight against serious and organised crime'.[29] Cyber security is an area of expertise sought by the NCA in prospective NCA Specials.

5.28 NCA Specials:

> are part time, unpaid NCA officers and are Crown servants by virtue of being employed by the NCA to exercise the functions of a Crown body; they are not civil servants. They are unpaid employees, working under a contract of employment, and under the direction and control of the NCA Director General, exercising authorised NCA functions personally.[30]

5.29 NCA Specials are appointed by a panel comprising business representatives and the NCA Specials and Volunteers Manager, which assesses applications 'against any skills gaps identified where a niche specialism (which is impracticable to fill through conventional employment) can enhance the agency's capability'.[31] NCA Specials are security vetted and subject to the same conduct and confidentiality regime as NCA officers.[32]

5.30 ISACA discussed leveraging existing talent and incentivising people with technological aptitude to become involved in law enforcement work. Mr Loeb stated:

> …we have to be realistic about the investments we make. When I say 'investments' this time, it's not just financial investments; it's thinking about

[28] DIGI, *Submission 20*, p. 3.

[29] National Crime Agency (NCA), *NCA Specials*, available: http://www.nationalcrimeagency.gov.uk/careers/specials (accessed 21 March 2019).

[30] NCA, *NCA Specials: Frequently Asked Questions*, 20 July 2017, available: http://www.nationalcrimeagency.gov.uk/publications/559-nca-specials-faq/file (accessed 21 March 2019).

[31] NCA, *NCA Specials: Frequently Asked Questions*, 20 July 2017.

[32] NCA, *NCA Specials: Frequently Asked Questions*, 20 July 2017.

> how we leverage the knowledge and resources of people who are either directly or indirectly engaged in cyber related activities, particularly in the prevention side. By that I mean when we look at the talent, it will help us in the long term that we're moving into an era where we have digital natives coming into the workforce who demonstrate greater technological aptitude than older geezers like me. They'll come with an aptitude to learn faster and be more adept at embracing these things, but how do we leverage the talent we have in the interim?
>
> Part of this relates to law enforcement and security personnel in general. We need to find ways of incentivising people with the proper technological aptitude to get involved. We're seeing that if you demonstrate technological aptitude, you can do some of this security work simply by being trained.[33]

5.31 Mr Loeb also gave the example from 2017, where ISACA firms:

> took 55 people of non-traditional, non-technological backgrounds and put them through security training. At the end of 10 weeks of this security training, people whose professions included beauticians, bartenders, morticians and psychiatrists quickly became employed in cyber related positions. The lesson from that is not, 'Let's put all the beauticians through security training,' but that we need to be open to leveraging the capabilities of people who are already good at this to train people who have an aptitude for it. You can parallel those working on the technological side with those working on the law enforcement side. We have to be open to that.[34]

5.32 Following recommendations contained in *Australia's Cyber Security Strategy*, the Australian government allocated an additional $20.4 million to the Australian Federal Police (AFP) for the period 2016−20 to place liaison officers overseas and to recruit personnel with the technical skills required for cybercrime investigations.[35]

5.33 Mr Neil Gaughan, Deputy Commissioner, Operations, AFP, noted that investigators have been embedded, not only with the Australian Cyber Security Centre, but also with Australia's cyber security counterparts in other countries, contributing to the development of relevant skills:

> That has been invaluable. Not only do we get notification of real-time threats and intelligence exchange in a real-time process but, more importantly from my perspective, it's upskilling our people. The people we currently have in those two locations are world's best in relation to

[33] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 14.

[34] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 14.

[35] Mr Andrew Colvin, Commissioner, Australian Federal Police (AFP), Parliamentary Joint Committee on Law Enforcement (PJCLE), Australian Federal Police annual report, *Committee Hansard*, 22 February 2019, p. 5.

> investigations of cybercrime, and they'll come back when their term is up and be able to pass those skills on to our people here.[36]

5.34 He noted, however, that the AFP faces challenges in retaining skilled personnel because of competition for those specialised skills from other Commonwealth agencies as well as from private industry.[37]

Specialist training

5.35 Some tertiary institutions offer advanced training courses or accredited high level degrees, but there are difficulties in matching these specialist training options with the precise training and education needs of government agencies. The CSRC recommended that a national approach to cyber training is needed, including collaboration with academic centres of excellence and private sector producers of technologies that are being used by cybercriminals.[38]

5.36 The ACIC and AIC acknowledged the Australian government's recent announcement to establish two new tertiary qualifications aimed at building a national industry of cyber security professionals, and to help protect business from cybercrime. However, they argued that there is a need to also recruit and retain personnel trained in cyber-forensics as well as cyber criminologists with expertise in the 'threat environment' and knowledge of the latest international approaches to prevention and control of cybercrime.[39]

5.37 DHA, AGD and ABF stated that:

> There is also evidence that Year 11 and 12 students in Australia show a lack of interest in STEM (Science, Technology, Engineering and Mathematics) careers and ICT. This may lead to a smaller pool of graduates when recruiting for technologically capable professionals in the medium to long term.[40]

5.38 WA Police advised the committee that 'law enforcement agencies of Australia defined their common, technology crime skill requirements in a set of documents which have been endorsed by the nation's Commissioners of Police'.[41] Those documents:

[36] Mr Neil Gaughan, Deputy Commissioner, Operations, AFP, PJCLE, *Committee Hansard*, 22 February 2019, p. 6.

[37] Mr Neil Gaughan, Deputy Commissioner, Operations, AFP, PJCLE, *Committee Hansard*, 22 February 2019, p. 6.

[38] CSRC, *Submission 8*, p. 12.

[39] ACIC and AIC, *Submission 29*, p. 9.

[40] DHA, AGD and ABF, *Submission 28*, p. 12.

[41] WA Police, *Submission 31*, p. 4.

> address future need by describing the technology crime skills required from constable level to specialist level, thereby enabling police agencies to develop an interoperable technology crime capability which scales to technology use in the community in a practical and cost effective manner.
>
> The documents were created to address the absence of relevant training in the marketplace, by providing academia and training vendors with a blueprint of need.
>
> Experience has demonstrated that a cohesive national approach is required to gain and retain the attention of the marketplace.[42]

5.39 Dr Coyne stated that new models are required for recruiting technology specialists into law enforcement agencies. He discussed the Australian Taxation Office's strategy over approximately 20 years of:

> bringing in cadets in the ICT industry. They're roughly in their last year of university, they work part-time within the organisation, they have a return-of-service obligation—for want of a better term—and they deliver cutting-edge young people in the workforce. That's one example of an approach. But the bottom line…is that what we really need is to take a much more flexible and imaginative approach to staffing issues. That comes from a loosening of arrangements around the Public Service and the employment arrangements for organisations like the AFP and the ICAC. Without that, we simply will not train those people.[43]

ICT capabilities

Rapidly changing technologies

5.40 A key challenge for law enforcement is the ability of agencies to keep up with the rapidity and constancy of changes in cybercrime technology and methods of criminal activity. As the rate of technology development accelerates, policing and other law enforcement agencies must engage with it effectively before its use becomes widespread amongst criminal entities.[44]

5.41 The CSRC noted, for example, that:

> …the use of Ransomware as an extortion tool is estimated by one source to have increased 2000% in the last two years as the new generation of cyber criminals increasingly resemble traditional organised crime syndicates.[45]

[42] WA Police, *Submission 31*, p. 4.

[43] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 2.

[44] Dr Monique Mann, Dr Adam Molnar, Dr Ian Warren and Dr Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia and Future Wise, *Submission 23*, p. 2.

[45] CSRC, *Submission 8*, p. 9.

5.42 Mr Nathan White, Senior Legislative Manager, Access Now stressed that the inevitable speed of technological change puts the emphasis on improving law enforcement's ICT capabilities:

> …with quantum computing and artificial intelligence, we can't stop technology, we can't stop research and we can't stop human development. We can pass laws that might slow it down or make it harder for people to use—we can do that, sure. But eventually these technologies are going to be out there. People who want them are going to be able to get them. What I would rather do is spend my time not slowing down technology but speeding up law enforcement.[46]

5.43 DIGI noted that law enforcement agencies are increasingly adopting new and emerging ICTs during investigations, citing examples such as the operational use of 3D technology to create a virtual model of a crime scene that can be used for later examination and analysis.[47]

5.44 Mr Guy Carlisle, Chief Information Officer, Northern Territory Police, Fire and Emergency Services, pointed out that new and emerging ICTs should be viewed as an opportunity to improve policing capabilities:

> I think ICT across government needs to be seen more as an enabler or a multiplier and not just treated as a cost centre, where projects and things are about 'How do we save money?' or 'How do we reduce police?' as opposed to 'How do we enable police enforcement or provide more capability to police?' I think we also need to take more of a risk based approach to technology. For example, triple 0 and dispatch services need to be rock solid and should never use bleeding-edge or leading-edge technology, whereas other operations such as intelligence services or disruptive operations can adopt leading-edge technology.[48]

5.45 WA Police pointed out, however, that current legislation limits law enforcement from using some technology despite these technologies being available to safely disable the threat. They noted that the Customs (Prohibited Imports) Regulations 1956, for example, prohibits the importation of signal jammers and drone jammers into Australia unless exempt, and the *Radio Communications (Prohibited Device) (RNSS Jamming Devices) Declaration 2014* may prohibit drone jammers in Australia because of their capacity to jam GPS signals. WA Police argued that legislative reform may be required to enable law enforcement to use such technologies for law enforcement purposes.[49]

[46] Mr Nathan White, Senior Legislative Manager, Access Now, *Committee Hansard*, 11 May 2018, p. 6.

[47] DIGI, *Submission 20*, p. 4.

[48] Mr Guy Carlisle, Chief Information Officer, Northern Territory Police, Fire and Emergency Services, *Committee Hansard*, 29 March 2018, p. 28.

[49] WA Police, *Submission 31*, p. 3.

Financial constraints

5.46 The rapid pace of change in cybercrime technology means that the life cycle of ICT systems for law enforcement purposes is 'drastically reduced'. Dr Coyne argued that there is an urgent need for increased investment in ICT capabilities:

> Current acquisition requirements, as outlined within relevant Department of Finance guidelines, no longer meet law enforcement needs. And under certain circumstances may impede law enforcement agencies from acquiring much needed capability. Traditionally law enforcement has employed a 'grow your own' approach to subject matter expertise and capability development. In the current operating context law enforcement will need to engage more frequently with the idea of acquiring capabilities and subject matter expertise on an ad hoc contracted basis. The research and development budgets for law enforcement, especially with respect the development of ICT capabilities needs to drastically increase. While government is unlikely to regain its 'technological edge' it can work with partners and develop niche capability.[50]

5.47 Mr Loeb similarly discussed the importance of governments investing in new and emerging ICTs for law enforcement:

> The primary objective of law enforcement requires staying one step ahead of the criminal. To ensure a safe, prosperous and forward focused Australia it remains imperative that the country continues to invest in ensuring the law enforcement community has the very best ICT technologies.[51]

5.48 Ms Amie Stepanovich, United States Policy Manager and Global Policy Counsel, Access Now pointed to the importance of investing in research and education about the tools and technologies available to law enforcement:

> There are many tools and technologies available to law enforcement…investing in research of those tools and education of law enforcement, and making sure that there are proper frameworks in place is a significant, important step that we should be talking about and moving forward on.[52]

5.49 Dr Coyne warned that the longer-term impact of efficiency dividends on national security agencies has led to a 'delicate equilibrium of cuts and "just in time" policy initiatives'.[53] For law enforcement agencies such as the AFP, budget policies have required them to offset new policy proposals from within existing budgets, resulting in a 'continuous erosion of funding' for existing programs. He argued that the

[50] Dr John Coyne, *Submission 4*, p. 7.

[51] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 9.

[52] Ms Amie Stepanovich, United States Policy Manager and Global Policy Counsel, Access Now, *Committee Hansard*, 11 May 2018, p. 5.

[53] Dr John Coyne, *Submission 4*, p. 7.

wider impact of such policies has been to reduce the capacity of Australian law enforcement agencies to engage in international engagement and cooperation.[54]

Ageing and inconsistent systems

5.50 The ACIC, which is responsible for maintaining a national database of criminal information and intelligence, relies on the ageing Australian Criminal Intelligence Database (ACID) and Australian Law Enforcement Intelligence Network (ALEIN).

5.51 The ACIC and AIC argued that these are 'bespoke systems' that are no longer fit for purpose, and do not meet the modern business needs of law enforcement and intelligence agencies:

> Maintenance and implementation of new ICT and capabilities is expensive and difficult in an environment of declining budget allocations. New ICT builds can often cost in excess of double the amount of agency annual appropriations. This highlights the need for dedicated funding in order for law enforcement agencies to remain effective against the emerging technologies being utilised by serious and organised crime groups, who often have access to large sums of money which allows them to take on new technologies as they appear…Funding cycles and governance frameworks are essential to maintain accountability but could be structured to be more flexible and agile to allow agencies to be in the best position to respond to changes.[55]

5.52 The ACIC and AIC pointed to the 'interoperability issues' between Australian law enforcement ICT systems, noting that further investment in ICT architecture will enable agencies to implement connectivity solutions so that they can share data with Australia's jurisdictional partners.[56] The ACIC and AIC also noted these 'interoperability issues' exists with systems and services developed by the Commonwealth for use by state and territories or the private sector in response to a particular event or incident:

> Cultural shifts are necessary to ensure support from all parties when attempting to deliver national ICT systems and services. Systems and services need to be built on a national level to maintain pace with emerging technologies and to fully utilise the technologies readily available across all levels of government and also the private sector.[57]

5.53 In this context, the ACIC outlined its plans for a National Criminal Intelligence System (NCIS) that will address some of these challenges, giving

[54] Dr John Coyne, *Submission 4*, p. 7.

[55] ACIC and AIC, *Submission 29*, p. 11.

[56] ACIC and AIC, *Submission 29*, p. 10.

[57] ACIC and AIC, *Submission 29*, p. 10.

Australia's law enforcement and intelligence agencies the 'first truly national and unified picture of criminal activity'.[58]

Securing electronic evidence

5.54 Digital evidence is like any other evidence in that it must be 'admissible, authentic and accurate'.[59] According to the International Association of Prosecutors—Global Prosecutors E-Crime Network (GPEN), the biggest challenge of cybercrime for law enforcement is to understand the criminal activity and then to prove it:

> The anonymity of the technology involved makes it harder to trace people. The borderless nature of the internet makes it harder to track the defendant or obtain evidence quickly from other jurisdictions. The complexity of ICT crimes such as hacking, malware, ransomware, phishing, viruses, worms, Trojans, spyware, identity theft, distributed denial of service attacks (DDoS), social engineering, online stalking, harassment and child abuse images amongst others. Add to this the veracity of evidence and how it is obtained, and you can see how it can lead to lengthy arguments at court between expert witnesses. The volume of the evidence collected, and stored further creates implications for search and seizure procedures and the consequent duties of disclosure. In addition to this the legislation used to prosecute such offences often lags behind the technological developments.[60]

5.55 GPEN noted that electronic evidence may be the only way that a law enforcement agency can link a criminal act to a 'real person', but gathering this evidence poses particular difficulties for law enforcement:

> …particular forms of electronic evidence might no longer be found in possession of the ICT criminals themselves. Rather, that evidence can be found with the Internet Service Providers (ISPs), electronic communication providers and Cloud storage providers. These companies may not be incorporated or represented in the country where the crime is being investigated. And if they are, they may have stored the relevant data abroad or even distributed over multiple data storage facilities in a number of countries.[61]

5.56 DHA, AGD and ABF outlined the challenges for Australian law enforcement agencies in securing electronic or digital evidence:

> While electronic evidence is often vital to the successful investigation and prosecution of a range of offences, the process of accessing this evidence can be complex and protracted. Difficulties include identifying where the

[58] ACIC and AIC, *Submission 29*, p. 13. Also see Chapter 6 for further discussion of the National Criminal Investigation System.

[59] GPEN, *Submission 19*, p. 3.

[60] GPEN, *Submission 19*, p. 2.

[61] GPEN, *Submission 19*, p. 3.

> records are held and taking appropriate steps to have them preserved. Obtaining records from overseas-based ISPs can also cause delay and be affected by jurisdictional challenges.[62]

5.57 Dr Coyne similarly highlighted the challenges facing law enforcement agencies in collecting and analysing evidence as a result of the increasingly complex nature of cybercrime:

> Law enforcement investigations will become increasingly complex and lengthy due to the increased sophistication and technological capabilities of criminal conspiracies. Global supply chains and complex business structures are making evidence collection equally more difficult. While data analytic capabilities are increasing, law enforcement is faced with growing information flows which are difficult to store and analyse.[63]

5.58 Dr Coyne called for a greater emphasis on developing the capacity of intelligence professionals to collecting intelligence and on investing in alternative 'collection disciplines' in 'our future [telecommunications interceptions]-dark world':[64]

> For 30 years, law enforcement agencies have truncated the management of their intelligence and evidentiary collection through a default preference to TI. With the degradation of this capability, those responsible for tasking the collection of criminal intelligence and evidence must now consider alternative collection capabilities. They must also seek to employ traditional intelligence capabilities in increasingly innovative and imaginative ways. Government needs to encourage its various law enforcement agencies to place greater emphasis on alternative evidence collection methods and collection planning.[65]

Data management

5.59 The collection and management of data relating to cybercrime is often overlooked, yet it remains central to successful law enforcement and provides a 'roadmap' for future strategies.[66] The committee received a range of evidence relating to data, including:

- the increasing volume and complexity of data;
- accountability and privacy concerns;
- biometric data;
- accessing data; and

[62] DHA, AGD and ABF, *Submission 28*, p. 14.

[63] Dr John Coyne, *Submission 4*, p. 6.

[64] Dr John Coyne, *Submission 4*, pp. 8–9.

[65] Dr John Coyne, *Submission 4*, p. 5. See also Chapter 3 for discussion of the new operational reality for law enforcement.

[66] Dr John Coyne, *Submission 4*, p. 8.

- the implications for personal safety in an increasingly connected world.

Increasing volume and complexity of data

5.60 The rapidly increasing volume and complexity of digital data presents significant data collection and management challenges for law enforcement. According to one analysis, the digital universe is doubling in size every two years and the amount of digital data created and copied will reach 44 trillion gigabytes by 2020.[67]

5.61 Indeed, in 2007, the Information Commissioner's Officer in the UK described the challenge of increasing data volumes facing it as akin to looking for a need in a haystack while the haystack is being made larger and larger, stating '[t]he simple acquisition of more and more information does not actually mean that people make better judgements'.[68]

5.62 The Data to Decisions Cooperative Research Centre (D2D CRC), established in 2014 to address the 'Big Data challenges' facing Australia's national security agencies, pointed to the impact on legislative and regulatory frameworks of this increasing volume and complexity:

> …our research has found that changing technology has rendered some of the existing law and policy regarding use of such technology law enforcement agencies outdated or confusing, creating challenges for information sharing and use of open source data by law enforcement agencies. The complexities of enhanced data analytics similarly create governance challenges, requiring appropriate attention to governance capacity and capabilities.[69]

5.63 Ms Tania Churchill, Director, Enterprise Analytics, Australian Transaction Reports and Analysis Centre (AUSTRAC) pointed to the importance of matching data that may be held by different agencies:

> We recently did a big data-matching project with the Department of Human Services that showed the effectiveness of using specialist expertise from both agencies and the power of matching in this instance our financial data with welfare data and using that to find welfare fraud. That was a hugely effective exercise. At the moment we're looking at expanding the matching algorithm that we developed so that we can start to match data with other

[67] 'The digital universe of opportunities: rich data and the increasing value of the Internet of Things', *IDC*, April 2014, https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm (accessed 18 February 2019).

[68] Mr Jonathon Bamford, Assistant Commissioner, Information Commissioner's Office, *Uncorrected transcript of oral evidence given before the House of Commons Home Affairs Committee*, 1 May 2007, available: https://publications.parliament.uk/pa/cm200607/cmselect/cmhaff/uc508-i/uc50802.htm (accessed 21 March 2019).

[69] Data to Decisions Cooperative Research Centre (D2D CRC), *Submission 7*, p. 2.

> agencies—for instance, Home Affairs. We've also talked to AFP—those kinds of areas—because, while each of the agencies here have highly specialised datasets that are very valuable in their own right, it's when you start to bring them together that you see a perspective of criminal behaviour that you generally can't see when you're looking at one slice of data by itself.[70]

5.64 The CSRC drew attention to the increased use of cyber transactions between government and citizens, making most government departments and agencies potential targets of cybercrime. The CSRC argued that agencies responsible for cybercrime investigation will increasingly be required to assist other government agencies to protect their data and clients.[71]

5.65 The D2D CRC recommended a series of legislative measures that may address the big data issues facing law enforcement agencies, including:

- simplifying the legal framework for information sharing by bringing disparate laws together rather than having to update different pieces of legislation;
- developing consistent and comprehensive definitions to clarify core information concepts in the digital age, beginning with standardising and updating legislative terminology relating to access, use and disclosure of data across jurisdictions;
- updating and simplifying terminology and concepts relating to the concept of data ownership and restrictions on disclosure;
- a consistent principles-based and risk-based approach to information sharing between law enforcement agencies;
- assessing data governance capabilities of and providing appropriate support to senior management of national security and law enforcement agencies;
- addressing the inadequacy of MLAT processes for Australian law enforcement; and
- examining mechanisms for increasing language abilities in law enforcement agencies for access to non-English language social media.[72]

5.66 Alternative measures to assist law enforcement agencies to manage the increasing volume of data put to the committee included:

- a Hybrid Cloud Strategy using a mixture of public and private cloud storage services that allows sharing of data and applications;

[70] Ms Tania Churchill, Director, Enterprise Analytics, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 11 May 2018, p. 54.

[71] CSRC, *Submission 8*, p. 10.

[72] D2D CRC, *Submission 7*, pp. 4−8.

- machine learning to sort and filter significant volumes of data for human analysis; and
- artificial intelligence and other advanced analytics techniques.[73]

Accountability and privacy issues

5.67 Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia, and Future Wise expressed concern that the expansion of data collection and information sharing by law enforcement and security agencies has not been matched with an expansion in independent oversight of policing activity.[74]

5.68 They argued that the new data-driven approaches to policing, involving the widespread collection of information, implementation of data-led decision making, and the use of algorithmic profiling, have had unintended consequences for human and due process rights. They contended that, in policing contexts, law enforcement agencies require greater accountability and regulation involving digital data collection and information sharing, such as has occurred in the European Union through the new General Data Protection Regulation:

> These processes are not neutral, and there is the potential for bias and discrimination to become inscrutable and incontestable with increased barriers to transparency via a potentially false veil of objectivity provided by computerisation…In striving for increased efficiency through automation, procedural and due process safeguards may be undercut. New forms of 'automatic justice' are challenging the traditional model of criminal justice where divisions between surveillance, adjudication and punishment are eroding with new forms of surveillance and automated decision-making that remove humans entirely. Here, 'black-box' decision-making creates a lack of transparency in how policing decisions are being made by machines.[75]

5.69 Dr Molnar stated that the obligation to store metadata that may indicate sensitive personal information should be subject to the same judicial authorisation requirements as content.[76] Dr Mann added that the European Union had ceased data retention schemes because they were found to present 'a disproportionate interference with individual human rights'.[77]

[73] Confidential, *Submission 33*, p. 7–8.

[74] Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia, and Future Wise, *Submission 23*, p. 18.

[75] Dr Monique Mann et al, *Submission 23*, pp. 15−16.

[76] Dr Adam Molnar, Vice-Chair, Australian Privacy Foundation, *Committee Hansard*, 29 March 2018, p. 17.

[77] Dr Monique Mann, Co-Chair, Surveillance Committee, Board of Directors, Australian Privacy Foundation, *Committee Hansard*, 29 March 2018, p. 17.

5.70 Drs Mann, Molnar, Warren and Daly recommended that new rules should be developed for digital evidence collection and exchange to assist prosecutions whilst preserving due process and human rights. For example, a judicial warrant should be required to enable law enforcement to access telecommunications information, on the basis that the current data retention scheme is 'at odds with international precedent'.[78]

5.71 In this context, Ms Churchill noted the challenge of combining data lawfully:

> …if you're going to use a specific piece of data in an administrative decision, an investigation or a prosecution, you've got to have complete visibility of the provenance of the data—in a legal sense—how was the data collected? And was there a lawful reason to use the data?...[T]hat's a real challenge for our legislative frameworks.[79]

5.72 Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, D2D CRC, highlighted the importance of having a common data governance framework across jurisdictions, and the need for greater public awareness of how data is collected and used by law enforcement:

> …the difficulty with the current legislative regime is that it's too complex for the public to understand. Even if you told the public everything about how the current law operates, I think you'd just confuse them. It's important…that the public understand. Because the legislation is complex and hard, it is not easy for the public to understand what's going on. In an earlier project…we spoke to agencies and asked them to identify the laws that were relevant to the use of big data for national security and law enforcement and we also asked civil society organisations and others the same question. What was really interesting was that they didn't give the same answers. These were often people who were in the area, but they still had a very different sense of what the laws were.[80]

5.73 Dr Bennett Moses pointed to the process in the UK in developing the *Investigatory Powers Act 2016* (UK) which involved 'extensive public engagement around what agencies should and shouldn't be allowed to do' (see Chapter 4 for discussion about the UK consultation process). She suggested that Australia needed to undertake a similar public engagement process.[81]

[78] Dr Monique Mann et al, *Submission 23*, pp. 9, 11.

[79] Ms Tania Churchill, Director, Enterprise Analytics, AUSTRAC, *Committee Hansard*, 11 May 2018, p. 55.

[80] Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, D2D CRC, *Committee Hansard*, 11 May 2018, p. 13.

[81] Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, D2D CRC, *Committee Hansard*, 11 May 2018, p. 13.

Biometric data and facial recognition systems

5.74 In late 2015, the Council of Australian Governments announced that members had agreed to establish a National Facial Biometric Matching Capability as part of a package of legislative and practical measures to further strengthen Australia's nationally-consistent approach to 'countering the evolving terrorist threat and help make Australians safer'.[82]

5.75 Drs Mann, Molnar, Warren and Daly argued that this system represented an example of 'function creep', where information collected for one purpose (such as licences and passports) may be used for secondary purposes beyond the scope or conditions of its original collection, without individuals being aware of or consenting to these secondary uses.[83]

5.76 They noted that a study of this new approach to policing in the Los Angeles Police Department had indicated that widening the 'criminal justice dragnet' reinforced discrimination and disadvantage by targeting 'risky' individuals or groups already marginalised, and had resulted in individuals seeking to avoid surveillance by avoiding all contact with institutions, such as social services, that use such methods.[84]

5.77 In November 2018 Mr Michael Phelan, Chief Executive Officer, ACIC, advised the committee that the contract to develop the Biometric Identification Services (BIS) had been terminated in June 2018 based on a cost-benefit analysis of the project. Mr Phelan stated that:

> …for identification purposes in this country, there are three pieces of work that are acceptable in a court of law to identify someone: DNA, fingerprints and eyewitness testimony. Facial recognition is not at that stage, so it's important that we actually have a doctrine about how you're going to use facial recognition—whether it's going to be used for forensic purposes, whether it's going to be used by police officers at the coalface, whether it's going to be used by detectives, whether it's going to be used in the intelligence area. I would submit that all of that needs to be worked out before we spend any money on a system. That's the process we're going through collectively with law enforcement at the moment.[85]

[82] Council of Australian Governments, Special Meeting of the Council of Australian Governments on Counter-Terrorism Communique, 5 October 2017, https://www.coag.gov.au/meeting-outcomes/special-meeting-council-australian-governments-counter-terrorism-communique (accessed 12 December 2018). The agreement included the signing of an Intergovernmental Agreement on Identity Matching Services.

[83] Dr Monique Mann et al, *Submission 23*, pp. 16–17.

[84] Dr Monique Mann et al, *Submission 23*, p. 15.

[85] The existing National Automated Fingerprint Identification System remains in use. Mr Michael Phelan, Chief Executive Officer, ACIC, Australian Criminal Intelligence Commission annual report 2016–17, PJCLE, *Committee Hansard*, 29 November 2018, p. 4.

5.78 The Law Council outlined the privacy and data security issues relating to the use of biometric data and facial recognition systems for law enforcement purposes, and recommended that the Australian government should consider the following when developing its future strategies in this area:

- the development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security;
- the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities; and
- publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.[86]

Obtaining information from banks

5.79 Law enforcement agencies commonly seek account holder information from an Internet Service Provider (ISP) or from a bank. Whilst the legal process for obtaining information from ISPs (authorised by telecommunications legislation) is effective, the process of obtaining information from banks (requiring the swearing of an Order to Produce or equivalent authorised by an external judicial authority) is not.

5.80 According to the WA Police, this is due to the increasing volume of investigations compounded by recent civil litigation that has resulted in the banking industry requiring an Order To Produce on every occasion:[87]

> Since the information obtained by both processes is essentially the same the WA Police recommends legislative reform be conducted to harmonise the information supply laws of the financial industry with those of telecommunications industry. In the absence of this change police will require additional resources to meet the required volume of order to produce processes.[88]

Personal safety and the Internet of Things

5.81 As explained in Chapter 1, the Internet of Things (IoT) describes the networking of physical devices, vehicles, buildings and other items that use

[86] Law Council of Australia, *Submission 21*, pp. 12−13.

[87] WA Police, *Submission 31*, p. 8.

[88] WA Police, *Submission 31*, p. 8.

electronics, software, sensors, actuators and network connectivity to collect and exchange data.[89]

5.82 Cybercriminals are increasingly using the 'seemingly innocuous' IoT to deploy a range of devices and applications that hide the identity of the user by separating online identity from online activity. The CSRC noted that such devices often have weak security and permit access to an individual's or company's wider network.[90]

5.83 The South Eastern Centre Against Sexual Assault and Family Violence (South Eastern CASA) highlighted the implications that insecure IoT devices have for women and children who may be subject to violence:

> For those who do not have either direct physical access to a device or knowledge of passwords, IOT devices are notoriously insecure and easy to hack. The prevalence and severity of the use of technology like phones and computers for violence against women is well documented.[91]

5.84 The ACIC and AIC noted that IoT devices are created for automation and efficiency rather than security. They submitted that the lack of agreed security guidelines in creating IoT devices introduces significant risk to individuals and businesses targeted by organised and serious crime groups, particularly where connected devices can alter the real-world environment such as in medical devices, door locks, cars, central heating systems, air conditioners and refrigerators.[92]

Protecting privacy and preventing domestic abuse

5.85 A significant emerging challenge for law enforcement is that, whilst internet-enabled devices such as mobile phones are already being used to stalk and monitor current or ex-partners, the IoT offers the opportunity for a range of new devices designed for legitimate purposes to be used to perpetuate violence against others. South Eastern CASA, for example, submitted that such internet-enabled devices are 'notoriously insecure and easy to hack':

> While people are becoming more aware that spyware can be installed on things like computers or phones, who would think that someone could be monitored via their fridge?...Using these devices an abuser could gather knowledge of a victim's day to day activities and personal habits remotely. This could be a powerful tool for coercive control and emotional abuse.[93]

[89] 'The Internet of Things (IoT): An Overview', Internet Society, https://www.internetsociety.org/resources/doc/2015/iot-overview?gclid=EAIaIQobChMI9Zqf0siC4AIVFR4rCh3hPwVVEAAYAyAAEgL_gPD_BwE (accessed 23 January 2019).

[90] CSRC, *Submission 8*, p. 6; DHA, AGD and ABF, *Submission 28*, p. 16.

[91] South Eastern Centre Against Sexual Assault and Family Violence (South Eastern CASA), *Submission 18*, p. 3.

[92] ACIC and AIC, *Submission 29*, p. 7.

[93] South Eastern CASA, *Submission 18*, p. 2.

5.86 South Eastern CASA also pointed out that detecting and gathering evidence of such abuse requires a victim to have a sophisticated knowledge of technology in order for law enforcement agencies to act. In addition, most current options for law enforcement agencies, such as an Apprehended Violence Order (AVO), were created to protect the victim from physical contact but do not offer protection against monitoring or stalking using internet-enabled devices.[94]

5.87 DIGI similarly discussed the inadequacy of law enforcement options that were created and implemented before the invention and ubiquitous adoption of the internet. DIGI advised that its members conduct regular training and outreach with law enforcement agencies, but highlighted the need for more education and training that ensures law enforcement personnel understand that 'crimes committed online should be treated and investigated in the same way as physical crimes':[95]

> Recently, Instagram (a DIGI member) was alerted to advice given by a police officer to a distressed mother whose daughter was being told to kill herself via Instagram. A police officer at her local station informed her that there was nothing that could be done despite the facts that (a) there are criminal laws prohibiting the use of carriage service to threaten, intimate or harass a person, (b) this type of conduct clearly violates Instagram's policies and will be promptly removed when Instagram becomes aware of it, and (c) Instagram has a well established process for responding to authorised law enforcement requests for data.[96]

5.88 South Eastern CASA suggested a number of practical reforms that are required in order to make internet-enabled devices secure against technologically-facilitated violence, including:

- manufacturers adhering to regulation and accountability requirements that ensure the security of internet-enabled devices, including no default login encoded into devices; an automated way for security updates to be installed on devices; and a simple way for the device owner to check who has accessed the device;
- consumer education on how to protect privacy;
- free access to a helpdesk where a consumer can take an internet-enabled device to be checked if they suspect that it has been compromised;
- education of law enforcement personnel about technologically-facilitated violence and how to best respond, particularly in family violence situations;
- internet-connected vehicles should have advanced technologies to ensure that the integrity of the vehicle is intact;

[94] South Eastern CASA, *Submission 18*, p. 2.

[95] DIGI, *Submission 20*, p. 2.

[96] DIGI, *Submission 20*, p. 2.

- ongoing technology training for anti-domestic violence practitioners about how to respond to and prevent technologically-facilitated violence; and
- ensuring that legal protections keep pace with technological development and are meaningfully enforced.[97]

Public awareness

5.89 Ms Lizzie O'Shea and Ms Elise Thomas stated that 'consumers have a reasonable expectation that messaging platforms and storage systems for personal data will be kept secure, including through the use of strong encryption'.[98] However, there remain relatively low levels of public awareness about cybercrime.

5.90 Detective Inspector John Manley, Officer in Charge of the Victorian Joint Anti-Child Exploitation Team, Victoria Police, noted that raising public awareness of the risks associated with cybercrime is important but takes time:

> I know there has been a lot done by the federal and state government agencies to educate people, but, at the end of the day, you just wonder how much of it sinks in. I think this is a generational thing. I think people will learn over time. A lot of the people that have been scammed are people who haven't grown up with a computer in their home—they're older people, in a lot of cases—and they trust people.[99]

5.91 ISACA reflected that the pace at which new technologies are introduced is part of the challenge and that public education plays an important role in resilience against cybercrimes:

> it's not necessarily the new technologies that are the ultimate challenge but the pace at which these technologies are being introduced. So what happens is that we, as societies, also have trouble keeping up with the necessary laws, policies and regulations to keep them in check. So while we try to figure that out, the cybercriminals are still advancing. I think that's why we have to do more on the education side to make sure that the stakeholders beyond the public sector take their accountabilities to supporting the safety of our society very seriously and do what they need to do to educate people and make sure that all enterprises are implementing the proper practices in order to ensure the maximum resilience against these cyber related crimes.[100]

[97] South Eastern CASA, *Submission 18*, p. 4.

[98] Ms Lizzie O'Shea and Ms Elise Thomas, *Submission 15,* p. 4.

[99] Detective Inspector John Manley, Officer in Charge of the Victorian Joint Anti-Child Exploitation Team, Victoria Police, *Committee Hansard*, 11 May 2018, p. 35.

[100] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 12.

Committee view

5.92 The committee acknowledges that there are significant and ongoing operational challenges and vulnerabilities for law enforcement agencies in relation to combating the criminal use of new and emerging ICTs. These include:

- geographic and jurisdictional constraints;
- workforce skills and capabilities;
- ICT capabilities and resources; and
- the dissemination, storage and management of, and access to, increasingly large volumes of data.

Geographic and jurisdictional constraints

5.93 A key feature of cybercrime is its international and borderless nature. For that reason, law enforcement agencies investigating cybercrime are routinely required to liaise and work with their international counterparts.

5.94 Throughout the course of the inquiry, the committee heard from a range of stakeholders, including law enforcement agencies and academics, that MLATs in their current form can be cumbersome, time consuming and not fit for purpose (see also discussion in Chapter 3).

5.95 The committee is aware that the MLAT process is not something Australia alone can resolve, and the committee acknowledges there have been some relevant changes in the US with the enactment of the CLOUD Act and subsequent moves to reach bilateral agreements in relation to accessing data.

5.96 However, the committee is of the view that the Australian government should evaluate the current MLAT process and identify how that process might be modified to better suit cybercrimes so that law enforcement investigations are not hindered by time delays or the inability to access data located outside Australia.

Recommendation 3

5.97 The committee recommends that the Australian government evaluates the current Mutual Legal Assistance Treaty process and identifies:

- **how the process might be modified to better suit the investigation of cybercrimes and the information and communications technology challenges facing law enforcement; and**
- **opportunities to implement those modifications with treaty partners.**

Workforce skills and capabilities

5.98 The committee is concerned by the evidence it received in relation to the challenges facing Australian law enforcement in recruiting and retaining sufficiently skilled staff with relevant ICT expertise. The ability of law enforcement agencies to offer pay and conditions comparable to those available in the private sector is one of those challenges.

5.99 The committee is attracted to the approach adopted in the UK by the NCA in employing NCA Specials (see paragraphs 5.27-5.29). The ability to engage contracted volunteers from the private sector with discrete expertise, subject to the same security vetting, confidentiality and code of conduct requirements as sworn personnel, and on a specific 'as needs' basis offers a dynamic and flexible means of addressing some of the workforce capability challenges facing Australian law enforcement. The committee also suggests that having such volunteer experts working side-by-side sworn officers would have the beneficial effect of simultaneously upskilling law enforcement personnel.

5.100 The committee agrees with the proposition put by the CSRC and others that there are significant benefits to be achieved from aggregating and concentrating cyber expertise. The committee believes that there is a need for a multi-agency approach to ICT workforce planning that builds a workforce with the necessary skills to respond and adapt to new and emerging technologies. The committee also welcomes the suggestion from Dr Coyne, reflecting on the ATO's approach, of recruiting ICT 'cadets' straight from university.

Recommendation 4

5.101 The committee recommends that the Australian government explores a range of approaches for improving the information and communications technology (ICT) skills and capabilities of the law enforcement workforce, including:

- **engaging volunteer experts, similar to the United Kingdom (UK) National Crime Agency Specials program;**
- **establishing 'single points of contact' within law enforcement agencies, similar to the approach adopted in the UK;**
- **implementing a single Commonwealth-led cooperative entity, providing expert cybercrime investigative support services to government, national security and law enforcement agencies; and**
- **establishing ICT cadetship programs for the recruitment of talented university students.**

ICT capabilities and resources

5.102 The committee heard evidence about the limited accessibility, search functionality and incompatibility of current Australian law enforcement ICT systems. It acknowledges that the ACIC's proposed National Criminal Intelligence System (NCIS), to be implemented over four years from 2018−19, aims to support collation and sharing of criminal intelligence and information across state, territory and Commonwealth law enforcement.

5.103 Whilst the NCIS seeks to address some of the challenges of establishing and maintaining ICT capabilities, the committee considers that dedicated agency funding may also be needed, in addition to existing annual agency appropriations, with sufficient flexibility to enable law enforcement agencies to respond to the escalating challenges of cybercrime.

5.104 In any event, it is evident to the committee that there will need to be ongoing government investment in ICT infrastructure if law enforcement agencies are to maintain connectivity and share data with their jurisdictional, intelligence and Five Eyes Alliance partners.

Recommendation 5

5.105 The committee recommends that the Australian government explores suggestions from law enforcement agencies and cybersecurity experts for improving information and communications technology (ICT) capabilities and resources, including:

- **dedicated agency funding with sufficient flexibility to enable law enforcement agencies to respond to the escalating challenges of cybercrime; and**
- **improving the model of ICT procurement and project management to promote new and emerging ICT for operational purposes.**

Data management

5.106 The committee heard that law enforcement agencies are facing challenges as a result of the rapidly increasing volume and complexity of digital data that they are required to collect, store, access, analyse and/or share.

5.107 The committee heard a range of suggestions from law enforcement agencies and cybersecurity and data experts about practical measures that could be implemented to improve data collection and management. Measures such as hybrid storage strategies and the use of AI and other advanced analytical techniques to sort and filter large volumes of data were proposed as possible solutions.

5.108 The committee considers that the use of these technologies will provide law enforcement agencies with necessary tools to address the challenges of big data. For this reason, the committee recommends that the Australian government considers the use of hybrid storage strategies, AI, and other advanced techniques for sorting, filtering and analysing large volumes of data.

Recommendation 6

5.109 The committee recommends the Australian government considers the use of hybrid storage strategies, artificial intelligence and other advanced techniques for sorting, filtering and analysing large volumes of data.

5.110 The committee is also interested in the Law Council of Australia's recommendations in relation to the use by law enforcement of biometric data and facial recognition systems, and considers that the Australian government should take these into account when developing its future strategies (noting the BIS project has been terminated):

- the development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security;
- the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities; and
- publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.[101]

Recommendation 7

5.111 The committee recommends that the Australian government takes the following into account when developing any future strategies for biometric data and facial recognition systems:

- **the development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security;**
- **the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities; and**
- **publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.**

Internet of Things, protecting privacy and preventing domestic abuse

5.112 The committee is concerned about the lack of agreed security guidelines in relation to the manufacture of IoT devices. Whilst such devices are designed for legitimate purposes, they are vulnerable to hacking by criminals and those who seek to perpetuate violence against others. The committee notes the evidence from the ACIC and AIC that the proliferation of such internet-enabled devices is putting all Australians at serious risk of being targeted by organised and serious crime groups.

5.113 The committee believes that legal protections in relation to internet-enabled devices and other consumer products should be subject to regular monitoring and

[101] Law Council of Australia, *Submission 21*, pp. 12−13.

review in order to ensure that they keep pace with technological development and are enforced.

Recommendation 8

5.114 The committee recommends that the Australian government reviews current consumer protection laws and regulations in relation to internet-enabled devices and identifies changes that may be required to provide adequate and timely consumer protection in relation to the risks they pose.

5.115 The committee is concerned that many mechanisms currently available intended to protect victims from a perpetrator, such as AVOs, do not offer victims protection against crimes perpetrated using internet-enabled devices.

5.116 While AVOs are legislated by the states and territories, the committee supports Australian governments reviewing legislation to ensure that current legal mechanisms afford adequate protection to victims of crime perpetrated via internet-enabled devices.

5.117 The committee also heard evidence indicating that there is a need for more education and training of law enforcement personnel about technologically-facilitated violence and how to best respond given the prevalence of IoT devices.

Recommendation 9

5.118 The committee recommends that Australian governments review legal mechanisms intended to protect victims, such as Apprehended Violence Orders, to ensure that they offer adequate protection to victims of crime facilitated by internet-enabled devices.

Recommendation 10

5.119 The committee recommends that the Australian government develops education materials to inform law enforcement agencies and personnel about new and emerging information and communications technologies that offenders may use to facilitate family and domestic abuse, and to provide guidance on appropriate strategies for responding to such situations.

5.120 The committee welcomes suggestions for practical reforms to improve regulation and accountability by manufacturers of internet-enabled devices and other consumer products, particularly in relation to IoT devices that may expose consumers to hacking, stalking, violence and other criminal activities. Such reforms could include, for example:

- ensuring that a default login is not encoded into devices;
- developing an automated way for security updates to be installed on devices; and
- providing a simple way for the device owner to check who has accessed the device.

5.121 The committee also welcomes suggestions for a public awareness and education program that informs consumers about the potential risks of internet-enabled devices, and other products and measures that they can take to protect their privacy. It also considers that the proposal for a consumer helpdesk has merit, offering device owners the means of having their devices checked if they suspect that it has been compromised.

Recommendation 11

5.122 The committee recommends that the Australian government develops and implements an Internet of Things (IoT) public awareness campaign that:

- **raises awareness about the potential vulnerabilities of internet-enabled devices and the IoT; and**
- **provides guidance to consumers about how to protect their privacy when using internet-enabled devices or the IoT, and information about how to access online help.**

Chapter 6

Strategic challenges and opportunities

6.1 The rapidly developing and changing cyber environment not only presents a range of strategic challenges, it also presents law enforcement with opportunities. Some of these are discussed in this chapter.

International law enforcement

6.2 Ms Esther George, Lead Cybercrime Consultant, International Association of Prosecutors (IAP), outlined a range of challenges that law enforcement agencies face worldwide in relation to bringing cybercriminals to justice, including:

- lack of expertise in using digital evidence amongst law enforcement agencies, prosecutors and judges;
- volume of cybercrime and the increasing professionalism of cybercriminals;
- under-reporting of cybercrime by businesses perhaps due to lack of awareness of the crime or the fear of commercial damage;
- integrity of electronic evidence and the increasing complexity of cybercrime; and
- gaps in law enforcement of cybercrime in some countries.[1]

6.3 Mr Matthew Loeb, Chief Executive Officer, ISACA, reflected on global efforts to keep people safe from cyberattacks, remarking:

> I've observed a more concerted effort and investment in collaboration of stakeholders…By collaboration, I mean across the board—local collaboration, statewide, region-wide, countrywide and even at the global level. I've been privileged to have the opportunity to see what key areas of the world are doing to keep their citizens safe.[2]

6.4 Mr Loeb also outlined strategic approaches that have been adopted in Europe, the United Kingdom (UK) and the United States (US) noting that they have been designed to ensure that law enforcement professionals are equipped to deal with cybercrime:

> The bottom line is that the future of law enforcement will realise the positive benefits of technology in its work. This means law enforcement professionals will increasingly need to be grounded in technology and possess a level of expertise that enables them to leverage these technologies

[1] Ms Esther George, Lead Cybercrime Consultant, International Association of Prosecutors (IAP), *Committee Hansard*, 29 March 2018, p. 40.

[2] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 10.

> to spot criminal activities—whether it occurs on the street, in smartphones or across T1 lines connected to the digital nerve centre of financial institutions or our critical infrastructures.

Europe

6.5 In 2004, European Union (EU) established the EU Agency for Network and Information Security (ENISA).[3] ENISA is a centre of expertise for cyber security in Europe. It works closely with EU member states and the private sector, to contribute to 'the development of a culture of [network and information security (NIS)] in society and in order to raise awareness of NIS'.[4]

6.6 ISACA told the committee that it supported a 'stronger role for ENISA' and increased cooperation with its stakeholders, stating:

> ISACA believes the framework for cybersecurity certification of ICT products and services should be regional rather than national and should leverage existing global standards and best practices. Moreover, it should be ensured that the design of products and services takes into account cybersecurity at the beginning of the design process in order to avoid creating new vulnerabilities. Finally, the EU recognised that addressing the cybersecurity skills gap is a major challenge, and ISACA staunchly supports the call on industry to step up cybersecurity related training for organisations and staff.[5]

United States

6.7 On 11 May 2017, President Trump issued an executive order designed to strengthen the cybersecurity of federal networks and critical infrastructure in order to establish 'a more cohesive approach on how the federal government addresses cyber risk'. The order requires all federal agencies to utilise a framework designed by the National Institute of Standards and Technology to improve critical cybersecurity.[6]

6.8 Mr Loeb stated:

> the executive order directs the Director of National Intelligence to ensure the development of a cybersecurity workforce in the US competitive with its foreign peers. Last summer, I had the opportunity to testify in Chicago on this particular piece of the order, and provide comments on how to

[3] European Union Agency for Network and Information Security (ENISA), 'ENISA: 15 years of building cybersecurity bridges together', *Press release*, 20 March 2019, available: https://www.enisa.europa.eu/news/enisa-news/enisa-15-years-of-building-cybersecurity-bridges-together (accessed 26 March 2019).

[4] ENISA, *About ENISA*, available: https://www.enisa.europa.eu/about-enisa (access 26 March 2019).

[5] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 10.

[6] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 9.

> improve the federal and private cybersecurity workforce in the US. Similar to our positions with cyber regulations in the EU and UK, ISACA is supportive of a highly trained cybersecurity workforce in the US as well as in other regions of the globe, and we are spearheading efforts, using performance based testing and credentialing, to help ensure the whole workforce remains well-positioned to meet the security challenges of the future.[7]

6.9 As discussed in Chapter 3, the US Congress has also passed the controversial *Clarifying Lawful Overseas Use of Data Act 2018* (CLOUD Act).

United Kingdom

6.10 The UK's National Cyber Security Strategy 2016–21 includes plans for threats and vulnerabilities as 'defend, deter and develop'. The Strategy is centred on keeping pace with new and emerging technologies and maintaining international collaborations.[8]

6.11 Mr Loeb stated that the UK government is focused on safeguarding traditional technologies as well as addressing security issues associated with the development of the Internet of Things and the 'growing omnipresence' of artificial intelligence that creates both opportunities and threats:

> This is all underpinned by an approach that drives forward cyber skills at all levels of the education system to ensure that the UK has the pool of talent it needs to respond to challenges in the future. The talent issue, which I've referenced twice, is a global issue. In all of our engagements with the UK, we've emphasised the importance of international collaboration and cybersecurity within both the European context and the wider Five Eyes grouping. The government gets this, and we are pleased to support them on a number of initiatives in our own professional community.[9]

Australian law enforcement initiatives

6.12 A number of initiatives have been established in Australia aimed at improving information and intelligence-sharing across jurisdictions. These initiatives include Australian Cybercrime Online Reporting Network (ACORN); the National Criminal Intelligence System (NCIS); and projects developed through the Data to Decisions Cooperative Research Centre (D2D CRC).

[7] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p.10.

[8] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 9.

[9] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 9.

Australian Cybercrime Online Reporting Network

6.13 A key initiative of the 2013 National Plan to Combat Cybercrime (outlined in Chapter 3) was the establishment of ACORN.

6.14 ACORN is:

> a national policing initiative of the Commonwealth, State and Territory governments. It is a national online system that allows the public to securely report instances of cybercrime. It will also provide advice to help people recognise and avoid common types of cybercrime.[10]

6.15 ACORN provides information to the public on how to identify and avoid common forms of cybercrime ('such as hacking, online scams, online fraud, identity theft and attacks on computer systems'); advice for victims of cybercrime; and a system for reporting cybercrime online.[11]

6.16 ACORN was designed and delivered in collaboration with all Australian police agencies; the Attorney-General's Department (AGD); the Australian Communications and Media Authority (ACMA); the Australian Competition and Consumer Commission (ACCC); the Australian New Zealand Policing Advisory Agency; and the Australian Criminal Intelligence Commission (ACIC).[12]

6.17 According to Mr Michael Phelan, APM, Chief Executive Officer, ACIC and Director, Australian Institute of Criminology (AIC):

> The national ACORN system, where all reports come in through the ACIC and back out to state jurisdictions, has the ability inside it to do analysis and see where the trends are and in which direction we can point jurisdictions.[13]

6.18 Detective Inspector Tim Thomas, Assistant Divisional Officer for Technology Crime Services, Western Australian Police, noted the importance of ACORN for Australia's law enforcement agencies. He argued that, whilst it needed some refinement, it remained largely effective because it aggregates data to enable law enforcement to identify offenders where the victims may be in a different jurisdiction:

> It is essential for law enforcement. What the metadata essentially stores is the identity information of the participants in criminal events. If we don't

[10] Australian Government, *About the ACORN*, available: https://www.acorn.gov.au/about-acorn (accessed 22 March 2019).

[11] Australian Government, *About the ACORN*, available: https://www.acorn.gov.au/about-acorn (accessed 22 March 2019).

[12] Department of Home Affair (DHA), 'Cybercrime', https://archive.homeaffairs.gov.au/about/crime/cybercrime (accessed 5 December 2018).

[13] Mr Michael Phelan, APM, Chief Executive Officer, Australian Criminal Intelligence Commission (ACIC) and Director, Australian Institute of Criminology, *Committee Hansard*, 11 May 2018, p. 44.

> have that information, we can't investigate the criminal events; it is as simple as that.[14]

6.19 A 2016 review by the AIC found that more than 65,000 reports had been submitted to the ACORN between November 2014 and June 2016. Online scams and fraud were the most common type of cybercrime reported (48 per cent) followed by issues buying and selling online (21 per cent). The AIC review also found that:

- there was little evidence that the ACORN had led to an increased prevalence among cybercrime victims to report to police;
- there had been little change in public awareness of where to report cybercrime, and awareness of the ACORN among the general public was relatively low;
- there were relatively high levels of satisfaction with the process of reporting to the ACORN;
- the number of investigations into cybercrime offences had increased, with an associated increase in resourcing for such investigations; and
- there was a high level of engagement with the prevention advice available from the ACORN among those who submitted a report of cybercrime.[15]

National Criminal Intelligence System

6.20 In 2015 the Australian government allocated $9.8 million over two years from the Proceeds of Crime Fund to pilot the National Criminal Intelligence System (NCIS), designed to enable the sharing of criminal intelligence and information across all Australian jurisdictions in real-time. Twenty Commonwealth, state and territory partner organisations participated in the pilot program; the results included:

- more informed risk assessments and enhanced officer safety;
- improved efficiency in discovering information and intelligence;
- de-confliction and greater collaboration across agencies;
- improved access to and awareness of existing and new criminal intelligence and information;
- better understanding of criminality and associations for persons of interest; and
- new lines of inquiry for investigators.[16]

[14] Detective Inspector Tim Thomas, Assistant Divisional Officer for Technology Crime Services, Western Australian Police (WA Police), *Committee Hansard*, 29 March 2018, pp. 29, 32.

[15] A Morgan, C Dowling, R Brown et al, *Evaluation of the Australian Cybercrime Online Reporting Network*, Australian Institute of Criminology, October 2016, pp. 9−14, https://aic.gov.au/sites/default/files/2018/08/acorn_evaluation_report_.pdf (accessed 6 December 2018).

[16] 'National Criminal Intelligence System', ACIC.

6.21 The pilot was completed in June 2017 and, as part of the 2018−19 Budget process, the ACIC was allocated an additional $59.1 million to develop tranche 1 of the system, which is being built with technological expertise from the Department of Home Affairs (DHA).[17]

6.22 The NCIS is intended to give Australia's law enforcement and intelligence agencies the first 'truly national and unified picture of criminal activity'.

> The objective is to deliver a future state where Australia’s law enforcement, law compliance and national security agencies leverage new services that facilitate the efficient and effective sharing of criminal information and intelligence, and collaborate in the management of cross-agency activities.[18]

6.23 The ACIC and AIC explained that the NCIS will be a whole of government capability providing a 'federated intelligence and information sharing platform' with improved analytical tools, near real-time monitoring, de-confliction, alerts and indicators, and effective management tools:

> The aim is to satisfy common, critical needs of intelligence analysts, investigators, front line officers and community policing stakeholders. By providing a clearer and more complete picture of criminal intelligence holdings, and ensuring the right people are able to access the right information when they need it, decision making and responses to crime will be faster and more accurate; improving our ability to prevent, detect and disrupt criminal threats.[19]

6.24 Mr Phelan explained that the development of the NCIS involved mapping the legislation in each jurisdiction and identifying any legislative impediments that needed to be addressed.[20]

6.25 According to Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, Data to Decisions Cooperative Research Centre (D2D CRC):

> The NCIS data platform was conceived as an ICT solution to remedy the data-sharing problem among law enforcement agencies. Essentially it would enable data from the different state databases to be searched from a common platform by a properly authorised officer with search outputs tailored based not only on the search terms but also on issues like security level, agency, and data-level permissions. This would essentially automate

[17] Mr Michael Phelan, ACIC, PJCLE, ACIC annual report 2016−17, *Committee Hansard*, 29 November 2018, p. 3. Tranche 1 is focused on connecting the states and territories with real-time information enabling the ACIC to do the analytics.

[18] ACIC and Australian Institute of Criminology (AIC), *Submission 29*, p. 13.

[19] ACIC and AIC, *Submission 29*, p. 10.

[20] Mr Michael Phelan, Chief Executive Officer, ACIC, *Committee Hansard*, 29 November 2018, p. 3.

> the current manual process while providing an appropriate data governance framework…[21]

Data to Decisions Cooperative Research Centre

6.26 The Data to Decisions Cooperative Research Centre (D2D CRC) was established in 2014 to address some of the big data challenges within the national security sector. D2D CRC submitted that law enforcement agencies and the national security community:

> …must be open to agile and collaborative capability development approaches where partner agencies with common needs collaborate with a network of trusted national and international public and private partners.[22]

6.27 It reported that it is currently working with several agencies and researchers to harmonise national security needs and develop a range of capabilities including:

- advanced data analytics;
- big data architectures, platforms and technologies;
- big data collection, processing, analysis and reporting;
- augmented and mixed reality technologies for interacting with and understanding data;
- information sharing and entity linkage;
- understanding contemporary societal and psychological drivers and motivations for crime including extremism;
- law and policy development and implementation; and
- big data workforce development.[23]

6.28 D2D CRC has also proposed a new Cooperative Research Centre (INdata CRC) to build on this work of addressing the common big data and information sharing needs across national security and law enforcement agencies:

> The INdata CRC will build on the capabilities that we've established in D2D to help the agencies enable effective sharing and coordination of common capability requirements in data analytics, to support the development of innovative solutions to common capability needs, to develop a coordinated approach to address current and emerging technology and workforce gaps, to try and forecast relevant technology advancements

[21] Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, Data to Decisions Cooperative Research Centre (D2D CRC), *Committee Hansard*, 11 May 2018, p. 9.

[22] D2D CRC, *Submission 7*, p. 4.

[23] Data to Decisions Cooperative Research Centre (D2D CRC), *Submission 7*, p. 3. The issue of big data is discussed further in Chapter 6.

> and to implement a coordinated approach to legislative and policy changes.[24]

Strategic issues in Australian law enforcement

6.29 The speed at which Australians are adopting new technologies is increasing exponentially, as is the speed with which criminals are exploiting these technologies for unlawful purposes. However, as the DHA, AGD and Australian Border Force (ABF) noted:

> This is not solely a technology challenge. Domestic and international legal frameworks must also keep pace with rapid changes and technology and organisational cultures, policy and procedures must enable agencies to adapt more rapidly to changes in criminal behaviour.[25]

6.30 Several submitters suggested strategies that could enhance the effectiveness of law enforcement in dealing with these challenges. The Western Australia Police Force (WA Police) advocated the development of a national model of service delivery, supported by management frameworks, to enable state and territory law enforcement agencies to effectively manage cybercrime across jurisdictions:

> Managing this environment effectively requires practical, connected and rationalised frameworks which span the nation…Forming practical, effective linkages between state and federal entities is essential to evolutionary process, and has the potential to deliver reduced costs and greater efficiencies to all stakeholders.[26]

6.31 The Victorian Police highlighted key areas that it considers need to be addressed, including: ensuring that law enforcement has the capability to keep pace with technological advances; knowledge is maximised through information sharing and data management; and the national and international legal and ICT policy frameworks are harmonised.[27]

6.32 Dr John Coyne proposed a number of broader strategic changes to address the law enforcement challenges posed by new and emerging ICTs, noting that '[w]hat we can do is not try to match those technologies but look for opportunities where we can observe and act quicker'.[28] He suggested:

- building an innovation and risk-taking culture within law enforcement with regard to new and emerging technologies;

[24] Dr Sanjay Mazumdar, Chief Executive Officer, D2D CRC, *Committee Hansard*, 11 May 2018, p. 8.

[25] DHA, Attorney-General's Department (AGD) and Australian Border Force (ABF), *Submission 28*, p. 6.

[26] WA Police, *Submission 31*, pp. 1−2.

[27] Victoria Police, *Submission 35*, [pp. 1−2].

[28] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 1.

- developing new strategies and approaches that close the gap between the time taken for newer technologies to emerge and the ability of law enforcement to deal with them;
- introducing new 'breakthrough financing' to enable law enforcement to deal with sudden changes and disruptions in the ICT and law enforcement environments; and
- forward-looking legislation to address future challenges.[29]

Telecommunications interception laws

6.33 Telecommunications interception (TI) has become a fundamental building block for lawful interception in law enforcement investigations, but the increasing use of ICT means that governments are faced with the challenge of developing interception policy and technology fast enough to keep pace with new developments in internet-based communications.[30]

6.34 DHA, AGD and ABF acknowledged the importance of legislative frameworks keeping pace with community expectations in the rapidly changing ICT environment, including balancing the 'legitimate needs of law enforcement with the privacy, rights and freedoms of individuals'.[31]

6.35 DHA, AGD and ABF noted that telecommunications interception under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and electronic surveillance under the *Surveillance Devices Act 2004* (SD Act) are vital tools for agencies in their investigations of a range of criminal offences, both online and offline.[32]

6.36 The TIA Act and SD Act recognise that law enforcement and intelligence agencies should have access to communications where certain preconditions are met. However, changes in the technological environment are undermining that access and, although the TIA Act has been subject to a number of legislative changes, it is nevertheless largely anchored to the technological environment that existed in 1979 when it was enacted. According to DHA, AGD and ABF '[k]ey issues include streamlining and reducing complexity across the TIA Act, as well as reforming the systems of warrants, oversight and accountability measures and information sharing provisions'.[33]

6.37 The AGD told the committee that, at the time the TIA Act was enacted:

[29] Dr John Coyne, *Committee Hansard*, 29 March 2018, p. 1.

[30] Dr John Coyne, *Submission 4*, p. 8.

[31] DHA, AGD and ABF, *Submission 28*, p. 9.

[32] DHA, AGD and ABF, *Submission 28*, p. 11.

[33] DHA, AGD and ABF, *Submission 28*, p. 11.

> you had a very small number of telecommunications providers through which communications transited. In actual fact, going back some way, you might have had only one you had to deal with, and they were government owned. That's obviously changed significantly now. The obligations that sit under the Telecommunications Act 1997 under section 313 for reasonable assistance to law enforcement only applies now to the subset of telecommunications providers that are on the carriers and not to the over-the-top providers, the social media platforms and things.[34]

6.38 The ACIC explained the challenges arising from legislation that 'is still framed around a device and person':

> whereas very much the submissions that were put forward and are still valid today are around attributes. We're after parts and pieces of information, regardless of the medium over which it travels. We want to have legislation that just says, 'I want to intercept communications between Mike Phelan and Dr Aly.' How those communications travel; what form those communications take, whether they are data or voice; and whether they are on a device or on a computer—we want the legislation to be technology agnostic. I say that because the technology goes too quick for the legislation to keep up with. Having it more agnostic to the technology and more focussed on the problem that you're trying to treat, which is essentially communications, would be better for us.[35]

6.39 The question of the technological neutrality of legislation and the ways in which the existing legislation hampers law enforcement is not new. In 2015, the Senate Legal and Constitutional Affairs References Committee heard calls from the law enforcement community for reform to the TIA Act so that it adapted to technological advances.[36]

6.40 In May 2013, the Parliamentary Joint Committee on Intelligence and Security recommended 'that interception be conducted on the basis of specific attributes of communications' based on 'the existing named person interception warrants'.[37]

Coordinating cybercrime and cyber security frameworks

6.41 WA Police pointed out that cybercrime and cyber security frameworks, both locally and internationally, are not integrated in an effective manner.[38] On the one hand, law enforcement agencies are responsible for dealing with cybercrime. On the

[34] Mr Andrew Warnes, Assistant Secretary, Communications Security and Intelligence Branch, AGD, *Committee Hansard*, 11 May 2018, pp. 48–49.

[35] Mr Michael Phelan, Chief Executive Officer, ACIC, *Committee Hansard*, 11 May 2018, p. 49.

[36] Senate Legal and Constitutional Affairs References Committee, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, March 2015, p. 11.

[37] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. xxv.

[38] WA Police, *Submission 31*, p. 8.

other hand, cyber security matters relating to terrorism and national security or attacks on private entities may be dealt with by the Computer Emergency Response Team (CERT) based in the Australian Cyber Security Centre (ACSC) rather than law enforcement agencies.[39]

6.42 In part, this fragmentation is the result of historical factors whereby the cyber security industry initially assumed responsibility for making law enforcement decisions. In addition, the cyber security industry has tended to focus on securing an ICT system affected by a security breach, rather than dealing with the offence, resulting in an 'offender-friendly environment where there is little risk of police action'.[40]

Public-private partnerships

6.43 Mr Loeb regarded collaborations between the public and private sectors as the 'Holy Grail':

> the need to nurture that relationship is critical. It's also the biggest challenge because of the concerns about information sharing and privacy. I believe that there is a lot more work to be done to have government and industry come together and talk about these opportunities to work together—because we're all stakeholders in thwarting the threats of cybercrime and, frankly, cybercrimes links to issues around physical security as well.[41]

6.44 Mr Loeb went on to describe the work ISACA has undertaken to bring the public and private sectors closer together:

> [W]e're positioning ourselves as honest brokers and protectorates of that data so that industry and governments can come closer together on the best practices and the information sharing that they're doing in order to increase efforts to maintain security.[42]

6.45 He also noted that there is a global issue regarding retention of cybersecurity skills in the public sector, and argued that more attention needs to be given to ensure that skilled cybersecurity professionals have the ability to transfer their expertise across the public and private sectors to ensure that the public sector workforce can be more agile in responding to the challenges.[43]

[39] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy*, 2016, pp. 2–3. See Chapter 3 for further details about CERT.

[40] WA Police, *Submission 31*, p. 8.

[41] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 10.

[42] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 10.

[43] Mr Matthew Loeb, Chief Executive Officer, ISACA, *Committee Hansard*, 29 March 2018, p. 11.

6.46 Ms George also highlighted the importance of bringing the expertise in the public and private sectors together in order to address the complex nature of cybercrime and the need to better protect critical national infrastructure:

> There needs to be more of a team approach. So, you don't just look at it as cybercrime; you look at the fact that there are various elements of other crimes going on with it. Just because the person is a cybercrime specialist does not necessarily mean that they're going to know about online money laundering or how to adapt it or know all the powers that come with online money laundering. You wouldn't need to have them as permanent members of your team because that's a money/resource issue, but you could actually take up some of their time and bring them along for certain meetings so that they can add ideas and influence how you can actually deal with these crimes.[44]

6.47 Mr Phelan stressed the importance of public-private partnerships, not only because of the economies of scale that can be achieved, but also because of the exchange of expertise that occurs:

> …the ACIC's view is that working with partners is paramount, particularly in the private sector because there are economies of scale that we don't have. I won't go into the details of some of the large companies that we work with; suffice to say that we've got arrangements with corporations that deal with transactions, whether they be financial transactions or otherwise, and we're working with them not just for the exchange of data but, more importantly, for the exchange of expertise…there is a desire among most of the regulated companies who deal with data in this country to get information from law enforcement so they can better target harden their own systems…[45]

Committee view

6.48 The committee heard compelling evidence that the most effective way to counter cybercrime in Australia is to ensure that:

- Australia's legislative and regulatory frameworks and mechanisms are coordinated and harmonised on a national basis;
- the legislative and regulatory framework and mechanisms are sufficiently flexible to enable agencies to be nimble and 'ahead of the curve' in this constantly evolving environment; and
- agencies responsible for combatting cybercrime have the capacity to draw on the skills and capabilities of specialist expertise from the private sector via public-private partnerships.

[44] Ms Esther George, Lead Cybercrime Consultant, IAP, *Committee Hansard*, 29 March 2018, p. 45.

[45] Mr Michael Phelan, Chief Executive Officer, ACIC, *Committee Hansard*, 11 May 2018, p. 52.

6.49 In this context, the committee welcomes the development of a new National Plan to Combat Cybercrime, and recommends that the National Plan prioritises ways of better coordinating intelligence gathering, data analytics, data management and investigative support services across Australian jurisdictions and agencies in order to ensure that law enforcement in Australia is able to keep pace with the rapid technological change in digital communications.

Recommendation 12

6.50 The committee recommends that the National Plan includes, as a key priority area, ways to better coordinate intelligence gathering, data analytics, data management and investigative support services across Australian jurisdictions and agencies in order to ensure that law enforcement in Australia is able to keep pace with the rapid pace of technological change in digital communications.

6.51 The committee acknowledges the significant work already undertaken by Australian law enforcement agencies to improve information and intelligence-sharing across jurisdictions. The ACORN and NCIS are examples of this.

6.52 The committee heard that the ACORN could be further refined, and the NCIS is in its implementation phase. The committee urges the Australian government to continue providing these projects with appropriate resourcing, and to review them into the future to ensure that they are meeting the needs of law enforcement and keeping pace with technological advances. The committee welcomes the D2D CRC proposal for the INdata CRC to address the common big data and information sharing needs of law enforcement agencies. The committee recommends that the Australian government considers implementing the INdata CRC and otherwise continues exploring opportunities for further improving information and intelligence-sharing between Australian jurisdictions.

Recommendation 13

6.53 The committee recommends that the Australian government considers implementing the INdata Cooperative Research Centre to address the common big data and information data sharing needs of law enforcement agencies and explores other opportunities for improving information and intelligence-sharing between law enforcement agencies in all Australian jurisdictions.

6.54 Mobile devices such as smartphones and tablets are now effectively mobile computers. The committee was told by law enforcement agencies that legislation, such as the TIA Act, is not sufficiently technology agnostic.

6.55 It is imperative that the legislation empowering law enforcement to intercept telecommunications keeps pace with technological advances and remains relevant irrespective of such advances.

6.56 To that end, the committee considers there is merit in reviewing the TIA Act and SD Act through the lens of technology neutrality. The committee recommends that the Australian government considers reviewing the TIA Act and SD Act, in light other legislative reform such as the implementation of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, and amending them as necessary to ensure that they are technology neutral and an effective legal mechanism for meeting the telecommunications interception needs of law enforcement agencies.

Recommendation 14

6.57 The committee recommends that the Australian government considers reviewing the *Telecommunications (Interception and Access) Act 1979* and *Surveillance Devices Act 2004* and amending them as necessary to ensure that they are technology neutral and an effective legal mechanism for meeting the telecommunications interception needs of law enforcement agencies.

6.58 The committee is supportive of partnerships between the Australian government and the private sector as a means of fostering and developing ICT expertise and novel approaches to tackling cybercrime. Therefore, in conjunction with Recommendation 4, the committee recommends that the Australian government explores opportunities for greater engagement and partnerships with the private sector to facilitate the exchange of expertise and collaboration in addressing cybercrime.

Recommendation 15

6.59 The committee recommends that the Australian government explores opportunities for greater engagement and partnerships with the private sector to facilitate the exchange of information and communications technology expertise and the development of novel approaches to tackling cybercrime.

Mr Craig Kelly MP

Chair

Appendix 1

Public submissions

1 Australian Commission for Law Enforcement Integrity (ACLEI)

2 Dr Vanessa Teague

3 Professor Dan Svantesson

4 Dr John Coyne

5 Scram Software Pty Ltd

6 Mr Todd Hubers

7 Data to Decisions Cooperative Research Centre

8 Cyber Security Research Centre

9 Dr James Martin

10 Law and Policy Program, Data to Decisions Cooperative Research Centre, UNSW Law

11 Australian Securities and Investments Commission

12 Cortex I.T. Labs Pty Ltd

13 ISACA

14 Access Now

15 Ms Lizzie O'Shea and Ms Elise Thomas

16 Pirate Party Australia

17 Wireless Internet Service Provider Association of Australia (WISPAU)

18 South Eastern Centre Against Sexual Assault and Family Violence

19 International Association of Prosecutors - Global Prosecutors E-Crime Network (GPEN)

20 Digital Industry Group Incorporated (DIGI)

21 Law Council of Australia

22 Mr Timothy Holborn

23 Drs Mann, Molnar, Warren and Daly - Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia and Future Wise

24 Confidential

25 Confidential

26 Confidential

27 Nyman Gibson Miralis Defence Lawyers and Advisors

28	Department of Home Affairs, Attorney-General’s Department and Australian Border Force
29	Australian Criminal Intelligence Commission and Australian Institute of Criminology
30	AUSTRAC
31	Western Australian Police Force
32	Mr Paul Templeton
33	Confidential
34	VeroGuard Systems
35	Victoria Police

Appendix 2

Public hearings and witnesses

Thursday, 29 March 2018—Canberra

CARLISLE, Mr Guy, Chief Information Officer, Northern Territory Police, Fire and Emergency Services

COYNE, Dr John, Private capacity

GEORGE, Ms Esther, Lead Cybercrime Consultant, International Association of Prosecutors

IRVINE, Mr David, Chair, Cyber Security Research Institute

LOEB, Mr Matthew, Chief Executive Officer, ISACA

MANN, Dr Monique, Co-Chair, Surveillance Committee, Board of Directors, Australian Privacy Foundation

MOLNAR, Dr Adam, Vice-Chair, Australian Privacy Foundation

PANAIA, Commander Lawrence, Commander, Judicial Services, Western Australia Police Force

SVANTESSON, Professor Dan Jerker B, Private capacity

THOMAS, Detective Inspector Tim, Assistant Divisional Officer for Technology Crime Services, Western Australia Police Force

Friday, 11 May 2018—Canberra

BAILES, Mr Morry, President, Law Council of Australia

BENNETT MOSES, Dr Lyria, Project Leader, Law and Policy Program, Data to Decisions Cooperative Research Centre

CACIULOIU, Mr Alexandru, Cybercrime Project Coordinator, Southeast Asia and the Pacific, United Nations Office on Drugs and Crime Regional Office for Southeast Asia and the Pacific

CHURCHILL, Ms Tania, Director, Enterprise Analytics, Australian Transaction Reports & Analysis Centre

COPEMAN, Mr James, Commander, Enforcement Command, Australian Border Force

GANOPOLSKY, Ms Olga, Chair, Privacy Law Committee, Business Law Section, Law Council of Australia

HANSFORD, Mr Hamish, First Assistant Secretary, National Security & Law Enforcement Policy, Department of Home Affairs

JABBOUR, Deputy Commissioner Ramzi, Deputy Commissioner, Capability, Australian Federal Police

LEONARD, Mr Peter, Member, Media and Communications Committee, Business Law Section, Law Council of Australia

LOGAN, Dr Sarah, Postdoctoral Research Fellow, Law and Policy Program, Data to Decisions Cooperative Research Centre

MacGIBBON, Mr Alastair, Deputy Secretary, National Cyber Security Adviser, Department of Home Affairs

MANLEY, Detective Inspector Thomas John Shillito (John), Officer in Charge of the Victorian Joint Anti-Child Exploitation Team, Victoria Police

MAZUMDAR, Dr Sanjay, Chief Executive Officer, Data to Decisions Cooperative Research Centre

McNAUGHTON, Ms Sarah, SC, Director, Commonwealth Director of Public Prosecutions

MOLT, Dr Natasha, Deputy Director of Policy, Law Council of Australia

MOSS, Dr John, National Manager, Intelligence, Australian Transaction Reports & Analysis Centre

PHELAN, Mr Michael, APM, Chief Executive Officer, Australian Criminal Intelligence Commission; and Director, Australian Institute of Criminology

STEPANOVICH, Ms Amie, United States Policy Manager and Global Policy Counsel, Access Now

SUMMERS, Mr Miles, Programmer and Graphic Artist, Web Team, South Eastern Centre Against Sexual Assault

SUMMERS, Ms Juliet, Team Leader, Information Communication Technology, South Eastern Centre Against Sexual Assault

WARNES, Mr Andrew, Assistant Secretary, Communications Security and Intelligence Branch, Attorney-General's Department

WHITE, Mr Nathan, Senior Legislative Manager, Access Now

WORTH, Ms Carolyn, Manager, South Eastern Centre Against Sexual Assault

Appendix 3

Tabled documents, answers to questions on notice and additional information

Answers to questions on notice

Thursday, 29 March 2018—Canberra

1 Dr Adam Molnar, Australian Privacy Foundation (received 27 April 2018)

Friday, 11 May 2018—Canberra

2 Ms Amie Stepanovich & Mr Nathan White, Access Now (received 31 May 2018)

Additional information

1 Gabriel Weimann – New terrorism and new media (received 24 October 2019)

2 Gabriel Weimann – Terrorists turn social media into antisocial media (received 24 October 2017)

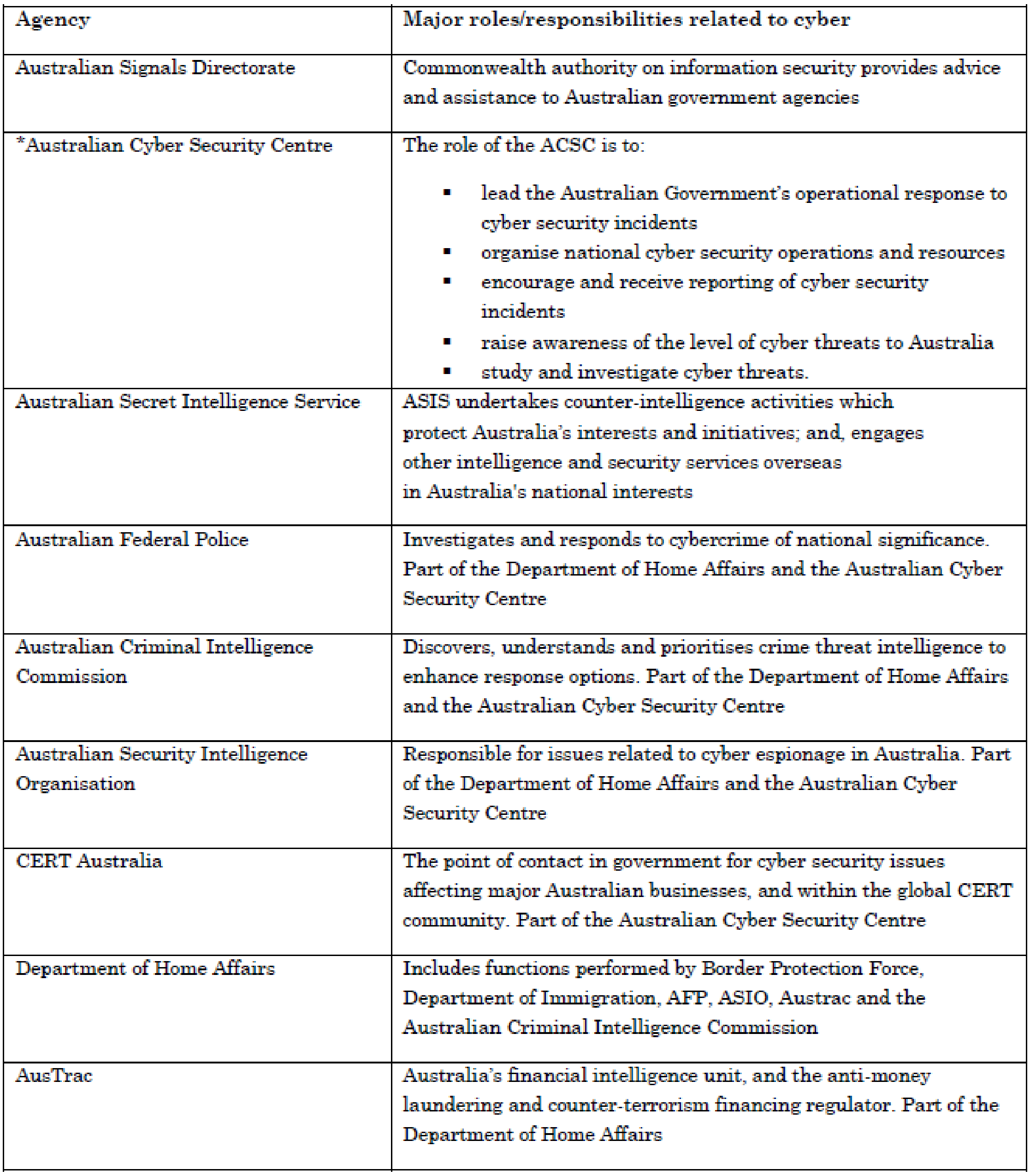
3 Gabriel Weimann – Terrorists migration to the dark web (received 24 October 2017)

4 Gabriel Weimann – Going dark: Terrorism on the dark web and terrorism in cyberspace. The next generation (received 24 October 2017)

5 Riana Pfefferkorn – The risk of "Responsible Encryption" (received 9 February 2018)

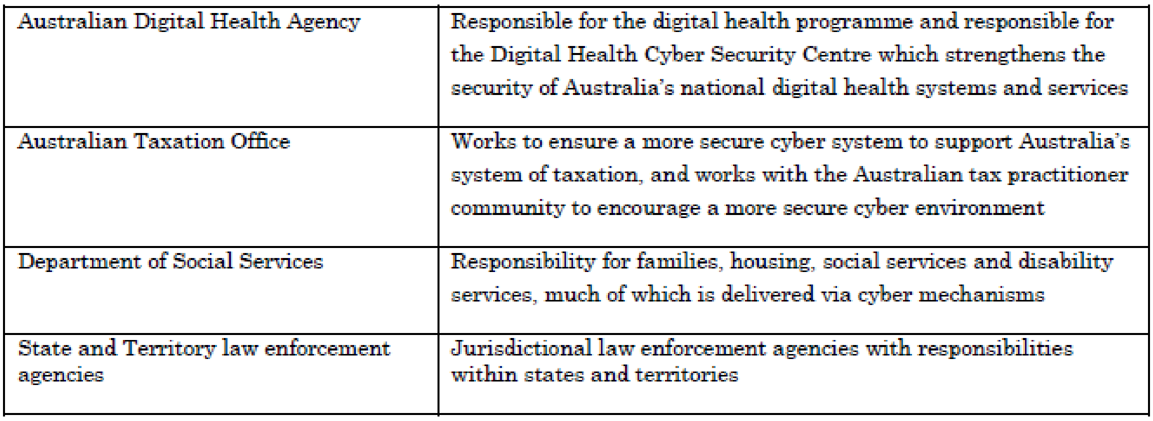
Appendix 4

Government agencies with existing cybercrime and cyber security responsibilities[1]



Agency	Major roles/responsibilities related to cyber
Australian Signals Directorate	Commonwealth authority on information security provides advice and assistance to Australian government agencies
*Australian Cyber Security Centre	The role of the ACSC is to: ▪ lead the Australian Government's operational response to cyber security incidents ▪ organise national cyber security operations and resources ▪ encourage and receive reporting of cyber security incidents ▪ raise awareness of the level of cyber threats to Australia ▪ study and investigate cyber threats.
Australian Secret Intelligence Service	ASIS undertakes counter-intelligence activities which protect Australia's interests and initiatives; and, engages other intelligence and security services overseas in Australia's national interests
Australian Federal Police	Investigates and responds to cybercrime of national significance. Part of the Department of Home Affairs and the Australian Cyber Security Centre
Australian Criminal Intelligence Commission	Discovers, understands and prioritises crime threat intelligence to enhance response options. Part of the Department of Home Affairs and the Australian Cyber Security Centre
Australian Security Intelligence Organisation	Responsible for issues related to cyber espionage in Australia. Part of the Department of Home Affairs and the Australian Cyber Security Centre
CERT Australia	The point of contact in government for cyber security issues affecting major Australian businesses, and within the global CERT community. Part of the Australian Cyber Security Centre
Department of Home Affairs	Includes functions performed by Border Protection Force, Department of Immigration, AFP, ASIO, Austrac and the Australian Criminal Intelligence Commission
AusTrac	Australia's financial intelligence unit, and the anti-money laundering and counter-terrorism financing regulator. Part of the Department of Home Affairs

[1] Cyber Security Research Centre, *Submission 8*, pp. 19–20.



Australian Digital Health Agency	Responsible for the digital health programme and responsible for the Digital Health Cyber Security Centre which strengthens the security of Australia's national digital health systems and services
Australian Taxation Office	Works to ensure a more secure cyber system to support Australia's system of taxation, and works with the Australian tax practitioner community to encourage a more secure cyber environment
Department of Social Services	Responsibility for families, housing, social services and disability services, much of which is delivered via cyber mechanisms
State and Territory law enforcement agencies	Jurisdictional law enforcement agencies with responsibilities within states and territories