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).

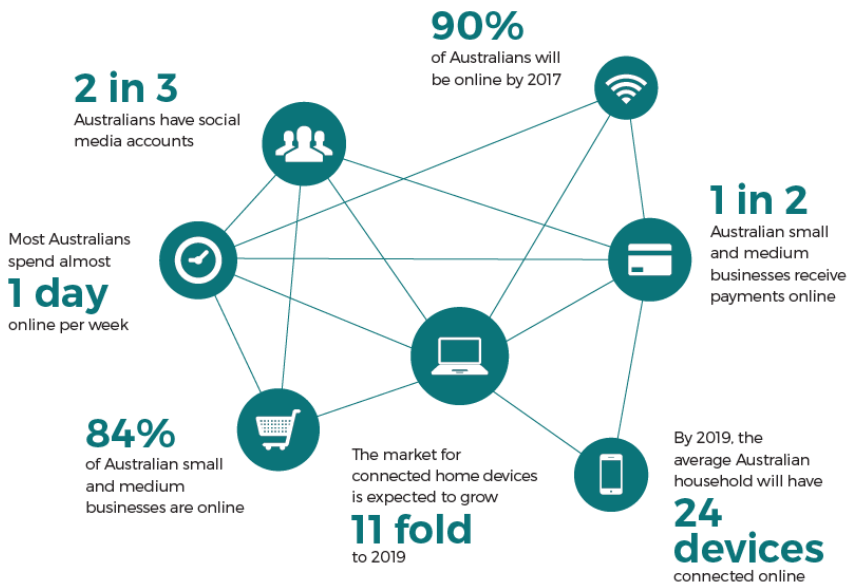
9 ABS, *8146.0 – Household Use of Information Technology, Australia, 2016–17*, available: http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0 (accessed 6 March 2019).

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]



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).