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.

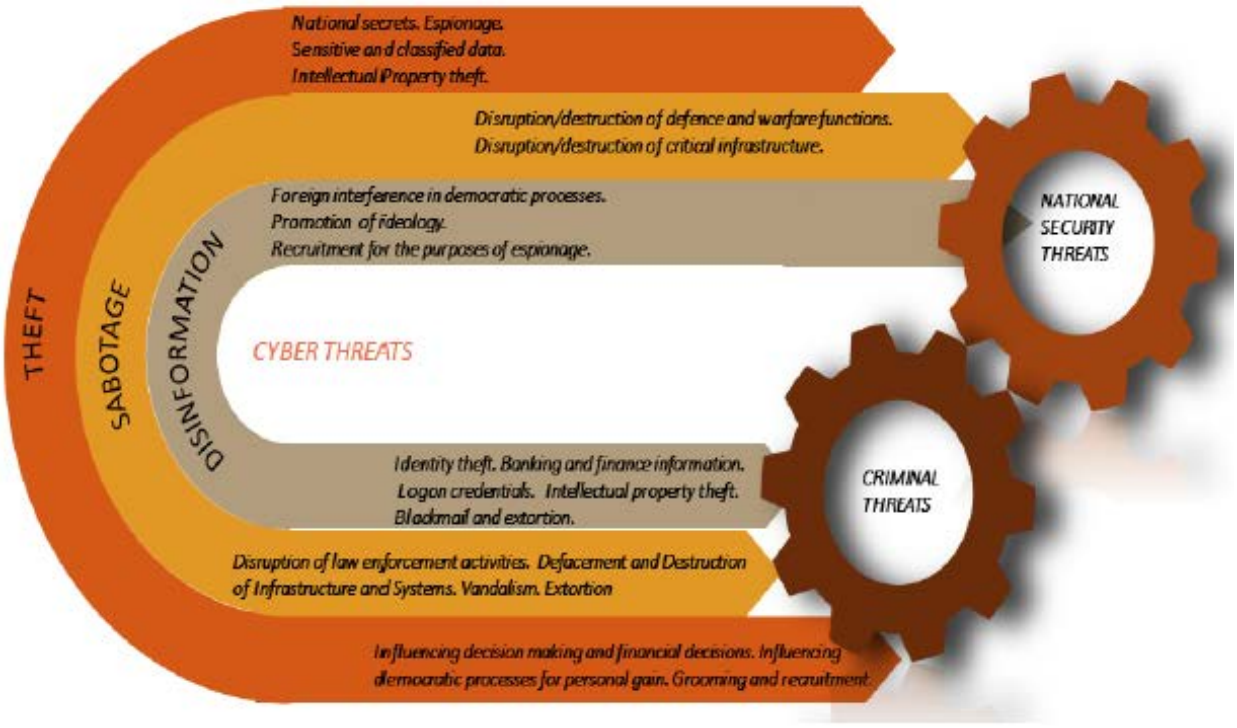
3 CSRC, *Submission 8*, pp. 6−7.

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]



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.

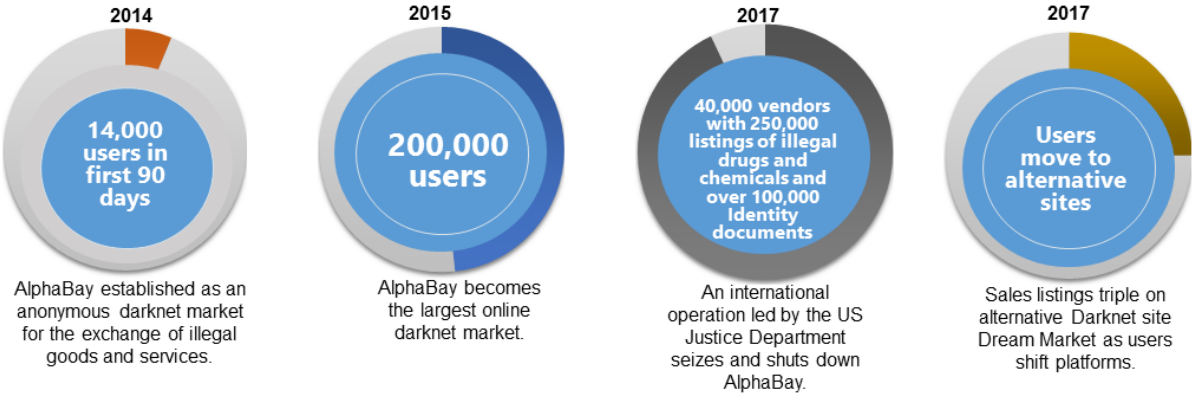
43 CSRC, *Submission 8*, p. 6.

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]



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.**