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