Chapter 5

Operational challenges and vulnerabilities

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

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

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

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

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

---

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

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

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

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

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

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

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

Geographical and jurisdictional constraints

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

Workforce skills and capabilities

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

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

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

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

Specialist staff

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

---

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

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

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

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

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

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

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

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

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

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

21 CSRC, *Submission 8*, pp. 11−12.

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

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

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

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

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

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

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

22 CSRC, *Submission 8*, pp. 11−12.

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

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

25 CSRC, *Submission 8*, pp. 13−14.

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

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

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

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

5.28 NCA Specials:

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Specialist training

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

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

5.37 DHA, AGD and ABF stated that:

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

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

---

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

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

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

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

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

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

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

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

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

ICT capabilities

Rapidly changing technologies

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

5.41 The CSRC noted, for example, that:

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

---

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

Financial constraints

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

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

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

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

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

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

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

---

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

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

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

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

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

Ageing and inconsistent systems

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

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

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

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

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

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

---

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

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

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

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

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

Securing electronic evidence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Data management

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

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

---

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

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

64 Dr John Coyne, *Submission 4*, pp. 8−9.

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

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

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

Increasing volume and complexity of data

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

- a Hybrid Cloud Strategy using a mixture of public and private cloud storage services that allows sharing of data and applications;

---

70 Ms Tania Churchill, Director, Enterprise Analytics, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 11 May 2018, p. 54.

71 CSRC, *Submission 8*, p. 10.

72 D2D CRC, *Submission 7*, pp. 4−8.

- machine learning to sort and filter significant volumes of data for human analysis; and
- artificial intelligence and other advanced analytics techniques.[73]

Accountability and privacy issues

5.67 Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia, and Future Wise expressed concern that the expansion of data collection and information sharing by law enforcement and security agencies has not been matched with an expansion in independent oversight of policing activity.[74]

5.68 They argued that the new data-driven approaches to policing, involving the widespread collection of information, implementation of data-led decision making, and the use of algorithmic profiling, have had unintended consequences for human and due process rights. They contended that, in policing contexts, law enforcement agencies require greater accountability and regulation involving digital data collection and information sharing, such as has occurred in the European Union through the new General Data Protection Regulation:

> These processes are not neutral, and there is the potential for bias and discrimination to become inscrutable and incontestable with increased barriers to transparency via a potentially false veil of objectivity provided by computerisation…In striving for increased efficiency through automation, procedural and due process safeguards may be undercut. New forms of 'automatic justice' are challenging the traditional model of criminal justice where divisions between surveillance, adjudication and punishment are eroding with new forms of surveillance and automated decision-making that remove humans entirely. Here, 'black-box' decision-making creates a lack of transparency in how policing decisions are being made by machines.[75]

5.69 Dr Molnar stated that the obligation to store metadata that may indicate sensitive personal information should be subject to the same judicial authorisation requirements as content.[76] Dr Mann added that the European Union had ceased data retention schemes because they were found to present 'a disproportionate interference with individual human rights'.[77]

---

73 Confidential, *Submission 33*, p. 7–8.

74 Drs Monique Mann, Adam Molnar, Ian Warren and Angela Daly, Australian Privacy Foundation, Digital Rights Watch Australia, Electronic Frontiers Australia, and Future Wise, *Submission 23*, p. 18.

75 Dr Monique Mann et al, *Submission 23*, pp. 15−16.

76 Dr Adam Molnar, Vice-Chair, Australian Privacy Foundation, *Committee Hansard*, 29 March 2018, p. 17.

77 Dr Monique Mann, Co-Chair, Surveillance Committee, Board of Directors, Australian Privacy Foundation, *Committee Hansard*, 29 March 2018, p. 17.

5.70 Drs Mann, Molnar, Warren and Daly recommended that new rules should be developed for digital evidence collection and exchange to assist prosecutions whilst preserving due process and human rights. For example, a judicial warrant should be required to enable law enforcement to access telecommunications information, on the basis that the current data retention scheme is 'at odds with international precedent'.[78]

5.71 In this context, Ms Churchill noted the challenge of combining data lawfully:

> …if you're going to use a specific piece of data in an administrative decision, an investigation or a prosecution, you've got to have complete visibility of the provenance of the data—in a legal sense—how was the data collected? And was there a lawful reason to use the data?...[T]hat's a real challenge for our legislative frameworks.[79]

5.72 Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, D2D CRC, highlighted the importance of having a common data governance framework across jurisdictions, and the need for greater public awareness of how data is collected and used by law enforcement:

> …the difficulty with the current legislative regime is that it's too complex for the public to understand. Even if you told the public everything about how the current law operates, I think you'd just confuse them. It's important…that the public understand. Because the legislation is complex and hard, it is not easy for the public to understand what's going on. In an earlier project…we spoke to agencies and asked them to identify the laws that were relevant to the use of big data for national security and law enforcement and we also asked civil society organisations and others the same question. What was really interesting was that they didn't give the same answers. These were often people who were in the area, but they still had a very different sense of what the laws were.[80]

5.73 Dr Bennett Moses pointed to the process in the UK in developing the *Investigatory Powers Act 2016* (UK) which involved 'extensive public engagement around what agencies should and shouldn't be allowed to do' (see Chapter 4 for discussion about the UK consultation process). She suggested that Australia needed to undertake a similar public engagement process.[81]

---

78 Dr Monique Mann et al, *Submission 23*, pp. 9, 11.

79 Ms Tania Churchill, Director, Enterprise Analytics, AUSTRAC, *Committee Hansard*, 11 May 2018, p. 55.

80 Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, D2D CRC, *Committee Hansard*, 11 May 2018, p. 13.

81 Dr Lyria Bennett Moses, Project Leader, Law and Policy Program, D2D CRC, *Committee Hansard*, 11 May 2018, p. 13.

Biometric data and facial recognition systems

5.74 In late 2015, the Council of Australian Governments announced that members had agreed to establish a National Facial Biometric Matching Capability as part of a package of legislative and practical measures to further strengthen Australia's nationally-consistent approach to 'countering the evolving terrorist threat and help make Australians safer'.[82]

5.75 Drs Mann, Molnar, Warren and Daly argued that this system represented an example of 'function creep', where information collected for one purpose (such as licences and passports) may be used for secondary purposes beyond the scope or conditions of its original collection, without individuals being aware of or consenting to these secondary uses.[83]

5.76 They noted that a study of this new approach to policing in the Los Angeles Police Department had indicated that widening the 'criminal justice dragnet' reinforced discrimination and disadvantage by targeting 'risky' individuals or groups already marginalised, and had resulted in individuals seeking to avoid surveillance by avoiding all contact with institutions, such as social services, that use such methods.[84]

5.77 In November 2018 Mr Michael Phelan, Chief Executive Officer, ACIC, advised the committee that the contract to develop the Biometric Identification Services (BIS) had been terminated in June 2018 based on a cost-benefit analysis of the project. Mr Phelan stated that:

> …for identification purposes in this country, there are three pieces of work that are acceptable in a court of law to identify someone: DNA, fingerprints and eyewitness testimony. Facial recognition is not at that stage, so it's important that we actually have a doctrine about how you're going to use facial recognition—whether it's going to be used for forensic purposes, whether it's going to be used by police officers at the coalface, whether it's going to be used by detectives, whether it's going to be used in the intelligence area. I would submit that all of that needs to be worked out before we spend any money on a system. That's the process we're going through collectively with law enforcement at the moment.[85]

---

82 Council of Australian Governments, Special Meeting of the Council of Australian Governments on Counter-Terrorism Communique, 5 October 2017, https://www.coag.gov.au/meeting-outcomes/special-meeting-council-australian-governments-counter-terrorism-communique (accessed 12 December 2018). The agreement included the signing of an Intergovernmental Agreement on Identity Matching Services.

83 Dr Monique Mann et al, *Submission 23*, pp. 16−17.

84 Dr Monique Mann et al, *Submission 23*, p. 15.

85 The existing National Automated Fingerprint Identification System remains in use. Mr Michael Phelan, Chief Executive Officer, ACIC, Australian Criminal Intelligence Commission annual report 2016−17, PJCLE, *Committee Hansard*, 29 November 2018, p. 4.

5.78 The Law Council outlined the privacy and data security issues relating to the use of biometric data and facial recognition systems for law enforcement purposes, and recommended that the Australian government should consider the following when developing its future strategies in this area:

- the development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security;
- the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities; and
- publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.[86]

Obtaining information from banks

5.79 Law enforcement agencies commonly seek account holder information from an Internet Service Provider (ISP) or from a bank. Whilst the legal process for obtaining information from ISPs (authorised by telecommunications legislation) is effective, the process of obtaining information from banks (requiring the swearing of an Order to Produce or equivalent authorised by an external judicial authority) is not.

5.80 According to the WA Police, this is due to the increasing volume of investigations compounded by recent civil litigation that has resulted in the banking industry requiring an Order To Produce on every occasion:[87]

> Since the information obtained by both processes is essentially the same the WA Police recommends legislative reform be conducted to harmonise the information supply laws of the financial industry with those of telecommunications industry. In the absence of this change police will require additional resources to meet the required volume of order to produce processes.[88]

Personal safety and the Internet of Things

5.81 As explained in Chapter 1, the Internet of Things (IoT) describes the networking of physical devices, vehicles, buildings and other items that use

86 Law Council of Australia, *Submission 21*, pp. 12−13.

87 WA Police, *Submission 31*, p. 8.

88 WA Police, *Submission 31*, p. 8.

electronics, software, sensors, actuators and network connectivity to collect and exchange data.[89]

5.82 Cybercriminals are increasingly using the 'seemingly innocuous' IoT to deploy a range of devices and applications that hide the identity of the user by separating online identity from online activity. The CSRC noted that such devices often have weak security and permit access to an individual's or company's wider network.[90]

5.83 The South Eastern Centre Against Sexual Assault and Family Violence (South Eastern CASA) highlighted the implications that insecure IoT devices have for women and children who may be subject to violence:

> For those who do not have either direct physical access to a device or knowledge of passwords, IOT devices are notoriously insecure and easy to hack. The prevalence and severity of the use of technology like phones and computers for violence against women is well documented.[91]

5.84 The ACIC and AIC noted that IoT devices are created for automation and efficiency rather than security. They submitted that the lack of agreed security guidelines in creating IoT devices introduces significant risk to individuals and businesses targeted by organised and serious crime groups, particularly where connected devices can alter the real-world environment such as in medical devices, door locks, cars, central heating systems, air conditioners and refrigerators.[92]

Protecting privacy and preventing domestic abuse

5.85 A significant emerging challenge for law enforcement is that, whilst internet-enabled devices such as mobile phones are already being used to stalk and monitor current or ex-partners, the IoT offers the opportunity for a range of new devices designed for legitimate purposes to be used to perpetuate violence against others. South Eastern CASA, for example, submitted that such internet-enabled devices are 'notoriously insecure and easy to hack':

> While people are becoming more aware that spyware can be installed on things like computers or phones, who would think that someone could be monitored via their fridge?...Using these devices an abuser could gather knowledge of a victim's day to day activities and personal habits remotely. This could be a powerful tool for coercive control and emotional abuse.[93]

---

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

90 CSRC, *Submission 8*, p. 6; DHA, AGD and ABF, *Submission 28*, p. 16.

91 South Eastern Centre Against Sexual Assault and Family Violence (South Eastern CASA), *Submission 18*, p. 3.

92 ACIC and AIC, *Submission 29*, p. 7.

93 South Eastern CASA, *Submission 18*, p. 2.

5.86 South Eastern CASA also pointed out that detecting and gathering evidence of such abuse requires a victim to have a sophisticated knowledge of technology in order for law enforcement agencies to act. In addition, most current options for law enforcement agencies, such as an Apprehended Violence Order (AVO), were created to protect the victim from physical contact but do not offer protection against monitoring or stalking using internet-enabled devices.[94]

5.87 DIGI similarly discussed the inadequacy of law enforcement options that were created and implemented before the invention and ubiquitous adoption of the internet. DIGI advised that its members conduct regular training and outreach with law enforcement agencies, but highlighted the need for more education and training that ensures law enforcement personnel understand that 'crimes committed online should be treated and investigated in the same way as physical crimes':[95]

> Recently, Instagram (a DIGI member) was alerted to advice given by a police officer to a distressed mother whose daughter was being told to kill herself via Instagram. A police officer at her local station informed her that there was nothing that could be done despite the facts that (a) there are criminal laws prohibiting the use of carriage service to threaten, intimate or harass a person, (b) this type of conduct clearly violates Instagram's policies and will be promptly removed when Instagram becomes aware of it, and (c) Instagram has a well established process for responding to authorised law enforcement requests for data.[96]

5.88 South Eastern CASA suggested a number of practical reforms that are required in order to make internet-enabled devices secure against technologically-facilitated violence, including:

- manufacturers adhering to regulation and accountability requirements that ensure the security of internet-enabled devices, including no default login encoded into devices; an automated way for security updates to be installed on devices; and a simple way for the device owner to check who has accessed the device;
- consumer education on how to protect privacy;
- free access to a helpdesk where a consumer can take an internet-enabled device to be checked if they suspect that it has been compromised;
- education of law enforcement personnel about technologically-facilitated violence and how to best respond, particularly in family violence situations;
- internet-connected vehicles should have advanced technologies to ensure that the integrity of the vehicle is intact;

94 South Eastern CASA, *Submission 18*, p. 2.

95 DIGI, *Submission 20*, p. 2.

96 DIGI, *Submission 20*, p. 2.

- ongoing technology training for anti-domestic violence practitioners about how to respond to and prevent technologically-facilitated violence; and
- ensuring that legal protections keep pace with technological development and are meaningfully enforced.[97]

Public awareness

5.89 Ms Lizzie O'Shea and Ms Elise Thomas stated that 'consumers have a reasonable expectation that messaging platforms and storage systems for personal data will be kept secure, including through the use of strong encryption'.[98] However, there remain relatively low levels of public awareness about cybercrime.

5.90 Detective Inspector John Manley, Officer in Charge of the Victorian Joint Anti-Child Exploitation Team, Victoria Police, noted that raising public awareness of the risks associated with cybercrime is important but takes time:

> I know there has been a lot done by the federal and state government agencies to educate people, but, at the end of the day, you just wonder how much of it sinks in. I think this is a generational thing. I think people will learn over time. A lot of the people that have been scammed are people who haven't grown up with a computer in their home—they're older people, in a lot of cases—and they trust people.[99]

5.91 ISACA reflected that the pace at which new technologies are introduced is part of the challenge and that public education plays an important role in resilience against cybercrimes:

> it's not necessarily the new technologies that are the ultimate challenge but the pace at which these technologies are being introduced. So what happens is that we, as societies, also have trouble keeping up with the necessary laws, policies and regulations to keep them in check. So while we try to figure that out, the cybercriminals are still advancing. I think that's why we have to do more on the education side to make sure that the stakeholders beyond the public sector take their accountabilities to supporting the safety of our society very seriously and do what they need to do to educate people and make sure that all enterprises are implementing the proper practices in order to ensure the maximum resilience against these cyber related crimes.[100]

97 South Eastern CASA, *Submission 18*, p. 4.

98 Ms Lizzie O'Shea and Ms Elise Thomas, *Submission 15*, p. 4.

99 Detective Inspector John Manley, Officer in Charge of the Victorian Joint Anti-Child Exploitation Team, Victoria Police, *Committee Hansard*, 11 May 2018, p. 35.

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

Committee view

5.92 The committee acknowledges that there are significant and ongoing operational challenges and vulnerabilities for law enforcement agencies in relation to combating the criminal use of new and emerging ICTs. These include:

- geographic and jurisdictional constraints;
- workforce skills and capabilities;
- ICT capabilities and resources; and
- the dissemination, storage and management of, and access to, increasingly large volumes of data.

Geographic and jurisdictional constraints

5.93 A key feature of cybercrime is its international and borderless nature. For that reason, law enforcement agencies investigating cybercrime are routinely required to liaise and work with their international counterparts.

5.94 Throughout the course of the inquiry, the committee heard from a range of stakeholders, including law enforcement agencies and academics, that MLATs in their current form can be cumbersome, time consuming and not fit for purpose (see also discussion in Chapter 3).

5.95 The committee is aware that the MLAT process is not something Australia alone can resolve, and the committee acknowledges there have been some relevant changes in the US with the enactment of the CLOUD Act and subsequent moves to reach bilateral agreements in relation to accessing data.

5.96 However, the committee is of the view that the Australian government should evaluate the current MLAT process and identify how that process might be modified to better suit cybercrimes so that law enforcement investigations are not hindered by time delays or the inability to access data located outside Australia.

Recommendation 3

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

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

Workforce skills and capabilities

5.98 The committee is concerned by the evidence it received in relation to the challenges facing Australian law enforcement in recruiting and retaining sufficiently skilled staff with relevant ICT expertise. The ability of law enforcement agencies to

offer pay and conditions comparable to those available in the private sector is one of those challenges.

5.99 The committee is attracted to the approach adopted in the UK by the NCA in employing NCA Specials (see paragraphs 5.27-5.29). The ability to engage contracted volunteers from the private sector with discrete expertise, subject to the same security vetting, confidentiality and code of conduct requirements as sworn personnel, and on a specific 'as needs' basis offers a dynamic and flexible means of addressing some of the workforce capability challenges facing Australian law enforcement. The committee also suggests that having such volunteer experts working side-by-side sworn officers would have the beneficial effect of simultaneously upskilling law enforcement personnel.

5.100 The committee agrees with the proposition put by the CSRC and others that there are significant benefits to be achieved from aggregating and concentrating cyber expertise. The committee believes that there is a need for a multi-agency approach to ICT workforce planning that builds a workforce with the necessary skills to respond and adapt to new and emerging technologies. The committee also welcomes the suggestion from Dr Coyne, reflecting on the ATO's approach, of recruiting ICT 'cadets' straight from university.

Recommendation 4

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

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

ICT capabilities and resources

5.102 The committee heard evidence about the limited accessibility, search functionality and incompatibility of current Australian law enforcement ICT systems. It acknowledges that the ACIC's proposed National Criminal Intelligence System (NCIS), to be implemented over four years from 2018−19, aims to support collation and sharing of criminal intelligence and information across state, territory and Commonwealth law enforcement.

5.103 Whilst the NCIS seeks to address some of the challenges of establishing and maintaining ICT capabilities, the committee considers that dedicated agency funding may also be needed, in addition to existing annual agency appropriations, with sufficient flexibility to enable law enforcement agencies to respond to the escalating challenges of cybercrime.

5.104 In any event, it is evident to the committee that there will need to be ongoing government investment in ICT infrastructure if law enforcement agencies are to maintain connectivity and share data with their jurisdictional, intelligence and Five Eyes Alliance partners.

Recommendation 5

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

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

Data management

5.106 The committee heard that law enforcement agencies are facing challenges as a result of the rapidly increasing volume and complexity of digital data that they are required to collect, store, access, analyse and/or share.

5.107 The committee heard a range of suggestions from law enforcement agencies and cybersecurity and data experts about practical measures that could be implemented to improve data collection and management. Measures such as hybrid storage strategies and the use of AI and other advanced analytical techniques to sort and filter large volumes of data were proposed as possible solutions.

5.108 The committee considers that the use of these technologies will provide law enforcement agencies with necessary tools to address the challenges of big data. For this reason, the committee recommends that the Australian government considers the use of hybrid storage strategies, AI, and other advanced techniques for sorting, filtering and analysing large volumes of data.

Recommendation 6

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

5.110 The committee is also interested in the Law Council of Australia's recommendations in relation to the use by law enforcement of biometric data and facial recognition systems, and considers that the Australian government should take these into account when developing its future strategies (noting the BIS project has been terminated):

- the development of an appropriate regime to detect, audit, report on, respond to and guard against events that may breach biometric data security;
- the use of methods for assessing the implications of any security breach and communicating the breach to both the general public and the technical, privacy and security communities; and
- publicly releasing additional technical information about the nature of the facial matching scheme, and the process for ensuring that there are not false matches, in order to inform the public about its operation and to allow informed debate about its use and future database links.[101]

Recommendation 7

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

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

Internet of Things, protecting privacy and preventing domestic abuse

5.112 The committee is concerned about the lack of agreed security guidelines in relation to the manufacture of IoT devices. Whilst such devices are designed for legitimate purposes, they are vulnerable to hacking by criminals and those who seek to perpetuate violence against others. The committee notes the evidence from the ACIC and AIC that the proliferation of such internet-enabled devices is putting all Australians at serious risk of being targeted by organised and serious crime groups.

5.113 The committee believes that legal protections in relation to internet-enabled devices and other consumer products should be subject to regular monitoring and

101 Law Council of Australia, *Submission 21*, pp. 12−13.

review in order to ensure that they keep pace with technological development and are enforced.

Recommendation 8

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

5.115 The committee is concerned that many mechanisms currently available intended to protect victims from a perpetrator, such as AVOs, do not offer victims protection against crimes perpetrated using internet-enabled devices.

5.116 While AVOs are legislated by the states and territories, the committee supports Australian governments reviewing legislation to ensure that current legal mechanisms afford adequate protection to victims of crime perpetrated via internet-enabled devices.

5.117 The committee also heard evidence indicating that there is a need for more education and training of law enforcement personnel about technologically-facilitated violence and how to best respond given the prevalence of IoT devices.

Recommendation 9

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

Recommendation 10

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

5.120 The committee welcomes suggestions for practical reforms to improve regulation and accountability by manufacturers of internet-enabled devices and other consumer products, particularly in relation to IoT devices that may expose consumers to hacking, stalking, violence and other criminal activities. Such reforms could include, for example:

- ensuring that a default login is not encoded into devices;
- developing an automated way for security updates to be installed on devices; and
- providing a simple way for the device owner to check who has accessed the device.

5.121 The committee also welcomes suggestions for a public awareness and education program that informs consumers about the potential risks of internet-enabled devices, and other products and measures that they can take to protect their privacy. It also considers that the proposal for a consumer helpdesk has merit, offering device owners the means of having their devices checked if they suspect that it has been compromised.

Recommendation 11

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

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