AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Australian Government
Australian Institute of Criminology

Parliamentary Joint Committee on Law Enforcement

Inquiry into the impact of new and emerging information and communications technology

Australian Criminal Intelligence Commission and
Australian Institute of Criminology submissions

February 2018

ACIC Ref: 17/258949

Table of Contents

Introduction

1. The Australian Criminal Intelligence Commission (ACIC) and the Australian Institute of Criminology (AIC) welcome the opportunity to make a public submission to the Parliamentary Joint Committee on Law Enforcement (PJCLE) inquiry into the impacts of new and emerging information and communications technology (ICT). The contents of this submission are unclassified and suitable for public release.
2. On 18 October 2017, the PJCLE resolved to conduct an inquiry into the impact of new and emerging ICT with particular reference to:
    a. Challenges facing Australian law enforcement agencies arising from new and emerging ICT
    b. The ICT capabilities of Australian law enforcement agencies
    c. Engagement by Australian law enforcement agencies in our region
    d. The role and use of the dark web
    e. The role and use of encryption, encryption services and encrypted devices
    f. Other relevant matters.
3. This submission addresses the ACIC's assessment of the current threat landscape, including technology as an enabler for serious and organised crime and the barriers which inhibit law enforcement agencies' abilities to mitigate the impacts of new and emerging ICT.

Background

4. The ACIC commenced operations on 1 July 2016; bringing together the Australian Crime Commission (ACC) and CrimTrac as one agency. The ACIC CEO is also the Director of the AIC, and administrative arrangements are in place to ensure appropriate access to information between agencies so that ACIC and AIC staff can work collaboratively.
5. The mission of the ACIC is to make Australia safer through an improved national ability to discover, understand and respond to current and emerging crime threats and criminal justice issues, including the ability to connect police and law enforcement to essential policing knowledge and information.
6. The ACIC is Australia's national criminal intelligence agency, uniquely equipped with intelligence, investigative and information delivery functions. The agency works with partners on the serious and organised crime threats of most harm to Australians and the national interest, and provides national policing information systems and services.
7. The AIC's mission is to inform crime and justice policy and practice in Australia by undertaking, funding and disseminating policy-relevant research of national significance. One of the AIC's key priorities is to explore the future of crime and justice including the emergence of new technologies and potential impacts.

Current threat landscape

8. Transnational serious and organised criminal groups have had a substantial impact on crime markets in Australia in recent years, with technology and digital infrastructure presenting as key enablers across multiple crime types. Australia's borders face ongoing challenges from transnational organised crime and the movement of illicit goods, money and people. However, for some crime types, technology has dissolved borders that previously protected victims from offshore offenders.
9. The ready availability of technology to reduce law enforcement visibility of serious and organised crime groups' activities has had an impact on how law enforcement agencies undertake their work. The ubiquitous use of encrypted communication devices and applications will continue to challenge law enforcement in coming years, as will the uptake of new technology and capabilities.

Technology as an enabler for serious and organised crime

10. The majority of serious and organised crime activities are enabled, to a large extent, by the use of technology. Technology is attractive to criminals as it can provide anonymity, obfuscate activities and locations, and increase their global reach by connecting them to potential victims, markets and information around the world. Using technology to commit crime is also significantly more efficient and less resource intensive than traditional methods of perpetrating crime.
11. The use of technology and digital infrastructure by serious and organised crime is considered a key determinant of significant changes in the criminal landscape into the future. The impact of the availability of technology can already be seen in multiple crime types, with a growth in technology-enabled fraud in the areas of online banking, trade, superannuation and identity crime.
12. The ability to target a range of victims remotely from any location in the world is attractive to serious and organised crime groups, who actively use technology to exploit the financial sector, to undertake online trading of illicit goods via the darknet, and to commit acts of child sexual exploitation through online grooming and distribution of child exploitation material. The growing availability and usage of the internet has also increased access by organised crime to vulnerable individuals.
13. Increasingly, criminal activities are committed with the assistance of technology either via the online environment or through advances in technological capabilities, such as secure communications which include but are not limited to communication devices with military grade encryption, remote wipe capabilities, duress passwords and secure cloud-based services.
14. The online environment enables crime to be committed with relative anonymity, a characteristic that is attractive to serious and organised crime groups and other motivated individuals, making the identification and prosecution of offenders more difficult.
15. The commercial availability of secure communication platforms and surveillance equipment, such as tracking devices, provides serious and organised crime groups with the means to conceal their criminal activities from law enforcement. Serious and organised crime groups also engage the services of professional facilitators with specialist ICT knowledge and skills to assist in the commission of technology enabled crimes.

16. Advances in Financial Technology, beginning with internet banking, through to the payments platforms and anonymous value-transfer systems we have today, have enabled serious organised criminal groups to move funds rapidly around the world, creating vast differences between the time it takes to move funds and the time it takes to identify and further investigate those movements.

17. Increased availability and ongoing advances in technology will continue to provide criminals with a diverse range of resources to conduct criminal activity and impede law enforcement investigations.

Darknet marketplaces

18. The darknet is a routed allocation of internet protocol address space that is not discoverable by usual means. The term can refer to a single private network or to the collective portion of internet address space that has been configured in that manner. Such networks are decentralised, routing traffic through a widespread system of servers, making it difficult to trace communications.

19. Darknet marketplaces such as Silk Road 3.0 and Valhalla Marketplace are used to facilitate the sale and trafficking of illicit drugs, firearms, precursor chemicals and child exploitation materials.

20. The use of darknet marketplaces by entities in Australia is expected to grow, given the increasing popularity of online trading and the perceived anonymity such marketplaces provide.

Anonymous value transfer mechanisms

21. Anonymising technologies, such as alternative banking services and virtual currencies, make it difficult to track financial transactions and to determine the origin and destination of illicit funds.

Alternative Banking Service

22. An Alternative Banking Service (ABS) facilitates low-cost international value transfers between clients, with a significant level of anonymity as client and company names are rarely connected with the movement of funds. An ABS acts as an online banking interface, which sits above and coordinates multiple bank accounts in various international locations. The ABS structure is underpinned by complex company structures designed to take advantage of inter-jurisdictional financial laws. Anonymity, along with ease of use, makes ABS attractive to criminal entities looking to engage in covert value movements.

Virtual currencies

23. Virtual currencies, more accurately known as cryptocurrencies[1] can be used by criminals for money laundering and to pay for illicit goods and services. Most darknet marketplaces exclusively accept virtual currencies for payments and they are commonly demanded as part of cyber-related extortion attempts.

24. Virtual currencies, such as bitcoin, are increasingly being used by serious and organised crime groups as they can be transacted anonymously online. They are also not reliant on regulated central banks and financial institution to facilitate transactions. The only regulated part of virtual currency transactions, the exchange of fiat currency for virtual currency, may be based in a country with little to no regulatory oversight.

[1] Cryptocurrencies exist in the online world. Transactions are most commonly recorded in public or private ledgers called *blockchains*. The transactions are considered 'pseudo- anonymous' as they are not directly attributable to one entity or person.

25. In December 2017, Parliament passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2017* (AML/CTF Bill) which will assist law enforcement to mitigate the criminal exploitation of virtual currencies through regulation of digital currency exchange businesses in Australia.

26. The Bill seeks to regulate digital currency[2] exchange businesses in Australia by requiring them to:

    - enrol with the Australian Transaction Reports and Analysis Centre (AUSTRAC) and register on the Digital Currency Exchange Register
    - adopt and maintain an Anti-Money Laundering and Counter-Terrorism Financing program to identify, mitigate and manage the risks they may face
    - identify and verify the identities of their customers
    - report suspicious matters, and transactions involving physical currency that exceed $10,000 or more to AUSTRAC,[3] and
    - keep certain records for seven years.[4]

27. Digital currency exchanges have been provided with 12 months from the date of passing to comply with the regulations set out in the AML/CTF Bill.

28. As regulation occurs at the point of intersection between the existing regulated financial system and unregulated virtual currencies, the new regulations may lead to information in regard to trends in the currencies used, potential links between currencies and darknet marketplaces and risks of emerging currencies.

29. The new regulations will be advantageous for law enforcement and intelligence agencies in the Australian context, however gaps may remain in the international picture due to differing or non-existent regulatory frameworks. There is also the possibility of criminals avoiding regulated digital currency exchange businesses by seeking out those in the black, or unregulated sector. Non-compliance with the regulated alternative remittance sector has already arisen in response to the AML-CTF regime, and it could be expected that this will also occur if virtual currency providers are brought within the regime. Tracking such non-compliance and investigating unregulated businesses may create challenges for regulators that would need to be addressed.

Encrypted communications

30. Encryption has both positive and negative impacts. Encryption provides government (including law enforcement and intelligence agencies), businesses and individuals with the ability to protect computer systems and data, as well as safely engage in online activities such as banking, shopping and communication. However, criminals are also employing encryption services to communicate and commit crimes outside of the visibility of law enforcement.

31. High-end encrypted smartphones continue to be preferred by serious and organised crime groups to reduce visibility of their activities to law enforcement. Multiple outlaw motorcycle gangs (OMCGs) and other serious and organised crime groups use encrypted communication devices and software applications as their primary means of communication, due to the content protection features available on these devices and applications.

[2] The ACIC uses the term 'virtual currency'. For the purpose of this submission, a virtual currency is a digital currency as defined by the Bill.
[3] Noting the only transactions visible to the exchanges are the exchange of fiat currency for virtual currency.
[4] Explanatory Memorandum, *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (Cth), p. 9.

32. Increased availability and ongoing advances in encryption technology will continue to provide criminals with a diverse range of resources to conduct criminal activity and impede law enforcement investigations.

New technologies entering the market

5G technology

33. New technologies entering the market, such as 5G, will give users greater anonymity and create challenges for law enforcement to lawfully access communications via traditional methods.

34. New 5G technology will allow devices to download data from multiple sources (such as WiFi, network towers and satellite) simultaneously. 5G will also replace the unique identifier associated with an electronic device with a temporary identifier which destructs once a connection with a tower is made. With current 4G technology law enforcement are able to use the unique identifier to attribute a device to an individual, whereas 5G technology and temporary identifiers will obfuscate this.

35. Further, 4G technology requires that communications data will eventually cross over a point on the provider network; the emergence of 5G may allow a person to restrict data travelling across telecommunication providers' networks entirely. This is a challenge for law enforcement as the current practices of intercepting communications may be void as less and less crosses the interception point.

36. A key issue with the introduction of 5G technology is that to provide lawful access, communications providers will need to assist law enforcement agencies to reconstruct data sessions from multiple sources to allow access to a single communication event. Whereas this is an occasional (but increasing) requirement for current 4G communications, this will almost certainly become the new normal for all data intercepted through 5G. Given 5G is slated to carry exponential increases in data, at far higher speeds, with far greater security that ever before, the impost and burden on both communications providers and law enforcement agencies to achieve lawful interception will be unprecedented.

Internet of Things

37. An increasing number of consumer devices are being developed with the capability to connect to the internet. Referred to as the Internet of Things (IoT) devices range from smart phones to CCTV cameras, lightbulbs, medical aids and household appliances. IoT devices are created with automation and efficiency in mind, however, security is not often prioritised during the design process.

38. It is predicted that by 2020 around 25 billion objects will be connected to the internet.[5] A lack of agreed security guidelines in the creation of IoT devices means their proliferation introduces significant risks as serious and organised crime groups are provided with numerous new avenues to target individuals and businesses. The risk is particularly substantial where connected devices can alter the real-world environment, for example medical devices, door locks, cars, central heating systems, air conditioners and fridges.[6]

[5] UK Government, *The Internet of Things,* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/410117/Internet_of_things_-_FINAL.pdf
[6] Australian Cyber Security Centre, *ACSC Threat Report,* 2017, p. 40-42, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

Offshore storage of data

39. ACIC intelligence indicates up to 70 per cent of Australia's serious and organised crime threats are based offshore or have strong offshore links.[7] As visibility of criminal activities becomes increasingly obscured through new technologies and sophisticated methods, it is clear that a connected, informed and collaborative response to the threat is required.

40. The increasing reach of the global communications supply chain means that more Australians are using services provided by offshore entities. This has implications for law enforcement in accessing communications as part of criminal investigations.

41. Law enforcement agencies may lawfully access stored communications and telecommunications data held by Australian carriers and carriage service providers using the powers of the *Telecommunications (Interception and Access) Act 1979* (TIA Act). However, if stored communications and telecommunications data are held offshore, agencies are required to engage in the Mutual Legal Assistance Treaty (MLAT) process. The MLAT process is not only lengthy and complex but can only be engaged in for evidentiary purposes meaning that the ACIC is unable to fulfil its intelligence functions, or to advance real time investigations, through this process.

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

[7] Australian Criminal Intelligence Commission, *Organised Crime in Australia,* 2017, p. 2, https://www.acic.gov.au/sites/g/files/net1491/f/2017/08/oca_2017_230817_1830.pdf.

Barriers which impact on and challenge the operating environment

43. The ACIC and AIC's investigative, research and information delivery services aim to work with our law enforcement partners to stop criminals exploiting emerging opportunities and perceived gaps in law enforcement information.

44. It is the ACIC's priority to fill cross-agency IT gaps, replacing previously incompatible IT systems with better, more integrated platforms that will save resources and time. The more responsive our systems, the more quickly our police and national security agencies can act to prevent, detect and disrupt significant threats.

45. The barriers identified below impact the ACIC's ability to fulfil its mandated functions to deliver information and services to frontline policing and law enforcement.

Personnel recruitment and retention

46. Challenges arise in recruiting and retaining personnel trained in cyber-forensics and who able to use the latest hardware and software for cyber investigations. Similarly, there is a need to employ trained cyber criminologists who are knowledgeable about the threat environment and familiar with the most recent theoretical and applied prevention and control approaches internationally. Expenditure on hardware and software will be required to enable law enforcement personnel to undertake investigations into criminality that makes use of the latest ICT systems, and to stay ahead of new and emerging threats.

47. The ACIC notes the Government's recent announcement to introduce two new tertiary qualifications to help protect businesses from cyber crime and drive a national industry of cyber security professionals.

48. A challenge experienced by not only the ACIC, but many agencies across government, is the length of time taken for staff to gain security clearances, particularly Top Secret (Positive Vetting) clearances. This leaves a limited pool of staff that are able to access and process information of high classifications, which can be a challenge for the ACIC in collaboration with Commonwealth, state and territory partners. This point is made to illustrate the challenge, not to say that security clearances are not required.

Access to information

49. As a service delivery agency, the ACIC has a responsibility to provide its partners with data, information and intelligence in support of decision-making. In particular there is an increasing need to do so in a timely manner, so that the right people have access to the right information to make the right decisions at the right time.

50. The ACIC has a legislated mandate to maintain a national database of criminal information and intelligence. The principal means of meeting this legislative function is currently through the ageing Australian Criminal Intelligence Database (ACID) and Australian Law Enforcement Intelligence Network (ALEIN), which are bespoke systems that are no longer fit for purpose and do not meet the

contemporary business needs of law enforcement and intelligence agencies, as highlighted in the 2013 PJCLE Inquiry into the gathering and use of criminal intelligence.

51. The ACIC is exploring avenues to provide a federated intelligence and information sharing platform for collaboration and intelligence sharing with partners. This will include common and improved analytical tools, near real-time monitoring, deconfliction, alerts and indicators, and effective management tools to support activities such as tasking and reporting. The aim is to satisfy common, critical needs of intelligence analysts, investigators, front line officers and community policing stakeholders.

52. 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.

53. The proposed National Criminal Intelligence System (NCIS) (discussed discretely under *ACIC priority for reform*) will give Australia's intelligence agencies and front-line law enforcement a national and unified picture of criminal activity.

54. NCIS will provide an innovative solution for meeting the challenges of cross-agency systems and access. Currently, if a user of a law enforcement system is employed by a new agency, their level of security clearance or prior use of that system is not transferrable or recognised. Therefore, they will face difficulties in accessing the same (or similar) system without going through new clearance or screening processes. NCIS will remedy this problem as agencies would be accessing the information held across many systems via one common login.

Interoperability of ICT systems and services

55. National systems and services are required to deconflict agency efforts and to ensure the most efficient and consistent means of communicating information. Historically there have been interoperability issues between systems and services developed by the Commonwealth for use by States and Territories or the private sector. Systems are often built in response to an event or incident which does not guarantee the optimum outcome sought in response to an issue.

56. 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.

Rate of adoption of emerging technology

57. Currently law enforcement is unable to maintain the same pace of technology adoption as serious and organised crime groups. Government processes and funding cycles can be time consuming and impact agencies' abilities to quickly procure the technology necessary to match and exceed the capabilities of criminal groups.

58. In order to keep pace with these practices, law enforcement agencies would benefit from investing in automation to supplement traditional law enforcement practices, such as surveillance or analytics. Automation and technology will provide agencies with additional tools to complement traditional investigative techniques and encourage the adoption of technology for a more agile workforce.

59. For example, financial platforms make funds transfers instantaneously when carried out online, however law enforcement agencies still receive this information in a paper-based format, which is significantly time consuming to analyse. The ACIC supports efforts to address this issue, such as the proposed ATO online portal.

60. For the ACIC, augmenting traditional methodologies with automated technologies would contribute to enhanced intelligence outcomes. The ability to connect the public and private sector data holdings, with appropriate access and privacy controls, would render significant time and cost savings to both government and industry.

61. The Budget Process Operational Rules and ICT Investment Approval process support Cabinet decision making and the successful implementation of ICT-enabled proposals and are critical to ensure accountability for significant government expenditure. However, the two pass staged approval processes can slow law enforcement agencies' abilities to implement ICT solutions in a timely manner.

62. 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.

63. As with the staged approval process required for funding of proposed government-funded ICT projects, the governance processes which determine decision making within agencies, departments and across government also slows the implementation of ICT solutions.

64. Serious and organised crime groups are utilising new technologies and making it difficult for law enforcement to investigate their activities simply as they are making and implementing decisions at a faster rate. New generations of technologies are adopted by criminals far more rapidly than it takes agencies to respond to the original technology challenge.

65. 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.

Outsourcing environment

66. As discussed in the most recent *State of the Service Report*, the pace of change and the complexity of services place a premium on recruiting and retaining the right people. The Australian Public Service (APS) operates in a competitive labour market when searching for talent. This means people strategies in the APS must be continuously reviewed and improved. The goal is to attract talented people and then equip them to embrace challenges and to perform competently.[8]

67. The ACIC's workforce includes investigators and intelligence analysts; professional human source case managers; financial profilers; operational and organisational psychologists; physical and technical surveillance operatives; technical and cyber analytics operatives; strategic and vulnerability assessment analysts; lawyers, specialist examinations staff; business and systems analysts; solution,

[8] Australian Public Service Commission, *State of the Service Report 2016-17, pg. 5,* http://www.apsc.gov.au/__data/assets/pdf_file/0004/101200/SoSR_web.pdf.

enterprise, security and information architects; projects managers; business changes managers; program delivery managers; and corporate services staff.

68. The required breadth of specialised skills amongst the ACIC workforce highlights the need to have the right people with the right skills at the right time. However, it is often difficult to source people up skilled in the correct fields with the ability to match emerging technologies. There is a need to hire specialists for short term periods to ensure these gaps are filled. Further investment in the development and sustainment of these specialised skills and knowledge within law enforcement agencies would be beneficial.

69. Similarly, systems and services which have been purchased require investment to maintain pace with updates which agencies are unable to support due to lack of capability, skills and knowledge.

70. As technology progresses it becomes less likely that an 'off-the-shelf' product will satisfy the needs of law enforcement in combating serious and organised crime use of technology to obfuscate their activities. The law enforcement community will increasingly be required to work within more collaborative arrangements in response to technology and capability development.

Contemporary legislation

71. Legislation establishing or regulating law enforcement powers necessarily seeks to strike a balance between these powers and individual rights and freedoms that will best serve the needs of an open, democratic and safe society. This balance is achieved by restricting the types of powers that may be exercised, and the ways and circumstances in which they may be exercised.

72. Technological advancements can rapidly change the social and criminal environment in which legislation operates, making powers less effective or restrictions on their exercise more burdensome. The fundamental need for an appropriate balance between law enforcement powers and individual freedoms is constant but the details of what is appropriate may vary over time.

73. Accordingly, governments and legislatures need to keep this balance under review to ensure that it remains appropriate. In some cases such review may lead to the conclusion that powers once considered unduly intrusive are now justified by changes in society and in criminal methods, or that restrictions once considered reasonable now make a power effectively unusable and need to be relaxed.

74. The ACIC considers that that legislative frameworks need to be flexible and adaptable in order to allow agencies to respond to unforeseen emerging technologies while still providing agencies with clarity of their powers and obligations. This would allow law enforcement agencies to consistently maintain the ability to appropriately investigate criminal matters. Further, the process to amend legislation or enact new legislation can be time consuming; a Bill that seeks to address a specific technological advancement, may be redundant by the time it is passed, as the technology it addresses has been superseded by a new generation of technology.

75. The existence of multiple prescriptive information disclosure regimes at the Commonwealth level, including that in the *Australian Crime Commission Act 2002*, complicates, and in some cases prevents, the sharing of information among agencies for law enforcement and crime prevention purposes. While there may be sound reasons for some of these restrictions, the overall effect is to hinder information sharing generally and, in particular, efforts to harness new technologies to share information more quickly and effectively.

76. Variation in legislation between local and international jurisdictions creates difficulties in the creation and implementation of national systems and services. For example, spent conviction regimes differ between jurisdictions. In this case, creating an automated national system to flag specific spent convictions would be difficult due to the inconsistencies in state legislation. For example what offences may become spent, after what period and in what circumstances. Similarly, lack of uniformity in unexplained wealth laws and identity crime legislation leads to problems in using new legislative schemes.

ACIC priority for reform

National Criminal Intelligence System

77. The ACIC proposes to establish a NCIS which will be a whole of government capability. NCIS will give Australia's law enforcement and intelligence agencies the first truly national and unified picture of criminal activity and will assist to address some of the challenges highlighted above.

78. 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.

79. The enhanced services will address the current information sharing issues and process deficiencies, whilst meeting the evolving business needs of all partners through improved interoperability, enabling:

    - access to timely and relevant national criminal information and intelligence
    - awareness of emergent threats, crime and criminality
    - exploitation of national data to discover criminal and terrorist links, associations and patterns
    - collaboration on cross-agency intelligence activities
    - de-confliction across partner agencies
    - trust and confidence by partners to share their information and intelligence
    - trust and confidence by partners to use nationally sourced information and intelligence, and
    - compliance and accountability.

80. The ACIC welcomes the Australian Government's commitment to NCIS through providing funding for the Pilot Program. Following three successful releases to partner agencies to test the system's capability, a further two years funding was provided to deliver the NCIS Interim Solution.