Submission to the Parliamentary Joint Committee on Law Enforcement Inquiry into the '*Impact of new and emerging information and communications technology*' — from Dr John Coyne

This submission does not reflect an Australian Strategic Policy perspective but is the opinion of the author Dr John Coyne, Head of Program, Border Security Program ASPI.

Overview

This submission addresses the Parliamentary Joint Committee on Law Enforcement (PJCLE) Inquiry terms of reference for the inquiry into the '*Impact of new and emerging information and communications technology*'. The submission is based on applied policy and academic research undertaken by the author over several years and is underpinned by over 20 years of field experience in law enforcement, intelligence and national security.

This submission will address five specific issues:

- Challenges facing Australian law enforcement agencies arising from new and emerging Information and Communication Technology (ICT);
- The ICT capabilities of Australian law enforcement agencies;
- Engagement by Australian law enforcement agencies in our region;
- The role and use of the dark web; and
- The role and use of encryption, encryption services and encrypted devices.

Challenges facing Australian law enforcement agencies arising from new and emerging ICT

In this section I will seek to unpack some of the assumptions that underpin our understanding of future ICT challenges to Australian law enforcement agencies. At the turn of the millennium, cutting edge computing capability was still being driven by governments. Arguably, since 2000, the speed at which technology is developed and deployed has accelerated exponentially: and governments' technological monopolies forever ended. These developments have been predominantly driven by private corporations with revenues that exceed that of some governments. The complex ownership, financial and geographic arrangements make regulating these companies difficult for most governments.

By the early 2000's our day-to-day life was, for the most part, viewed through two conceptual lenses: real and virtual. Government's policy responses to technology, at least in Australia, treated technology challenges through similarly divided silos. In launching the iPhone in 2007, Steve Jobs was embarking on a project that altered the way that many of us interact with each other and the world. Today, generation y and x Australians are unlikely to see their life or social interactions as real or virtual: it is just their life. Unsurprisingly then technological disruptions to how our world operates are become more frequent. Further, this observation highlights the need for law enforcement to re-examine many of its assumptions regarding cyber and technology enabled crime.

Acceleration in the development and use of technology has been matched by changes in the capability of those that would do us harm. State and non-state actors alike are actively leveraging technology to communicate, undertake information operations and conduct cyber-attacks. For instance the use of twitter and twitter bots by ISIS to organise and market its message broadly.

Australian law enforcement agencies face an increasing number of challenges from emergent technologies. It is possible to categories these challenges into four broad thematic classifications:

- implications of specific technological developments;
- encryption;
- the continued globalisation of organised crime; and
- declining impact of traditional policing responses.

These categories withstanding, the key policy challenge that underpins all of the issues relates to the limited capacity of law enforcement, whether in Australia or in other countries, to introduce disruptive strategies in response to disruptive technology. The nature of many parts of law enforcement are rapidly changing and becoming more global in nature, but at the same time this does not mean an end to investigations and response roles.

Implications of specific technological developments

In December 2016, ASPI and the SAP Institute for Digital Government hosted a roundtable to consider what the next 15 years of technology development might bring. Four key themes emerged during the roundtable:

- the growing use of drones;
- the changing nature of critical infrastructure;
- quantum computing and the rise of Artificial Intelligence (AI); and
- the changing nature of the internet.

Current experiments in the use of drones has moved from single drone activity to models that support Eusocial behaviours. Eusocial behaviours are best represented by ants, bees and other forms of insect life which are capable of supporting complex social behaviour and acting in a highly coordinated manner despite the limited intelligence of individual units within the colony. Those patterns of behaviour have been modelled for the purposes of allowing drones to perform complex tasks in a coordinated fashion. Such capabilities have a wide application that extend from construction to remote surveillance.

Perhaps in the next 15 years we will see a shift to true independence of action by drones, Leveraging elements of AI would allow individual drones to complete preprogramed actions without human interaction, but may also allow then to finish tasks when circumstances change. The growing capabilities of drones will provide significant benefits for emergency response scenarios, as well as a reduction in risk to responders. However, we may also see the hijacking of drones to undertake terrorist actions.

Critical national infrastructure is undergoing a change in definition and distribution. In the future some forms of critical infrastructure will be physically distributed but digitally concentrated. This physical distribution will, like the original ARPANET, reduce the value of physical attacks on a single point of failure. This withstanding, commercial update servers and peer-to-peer relationships between devices will allow for rapid dissemination of viruses and malware which may cripple such infrastructure. Commercial providers of devices and systems will need to significantly improve cyber security in light of the likely growth in our dependence on digitally distributed systems.

Our understanding of how we will leverage AI and how it will impact on our society are limited. The development of AI will have impacts on law enforcement. And there is a real possibility that AI will disrupt employment and social cohesion. The largest IT companies—including Facebook, Google, IBM and Microsoft—are in the front seat to develop AI. The benchmark for AI is technology that is emulative of the human condition, rather than one that will deliver improvement in the human condition. As such, there is a real possibility that someone will produce a machine intelligent enough to achieve a single goal, without any ability to understand the broader impact of its actions.

Contemporary approaches to software development cannot meet the needs of the exponentially growing computing power used to support AI-based systems. To support new capabilities we may see a move to intelligent systems that are decoupled from underlying infrastructure. In this construct, AI may exist across multiple pieces of hardware rather than being developed in a single stand alone or networked piece of hardware infrastructure.

In the future, programs may become independent consumers of resources, intelligently negotiating with other programs for resources across all domains, including but not limited to mobile devices, traditional server farms and mainframes. Those programs would follow biological models of behaviour: being born, reproducing as required, and dying when they are no longer required. This kind of model isn't without risks. A program could potentially become a pandemic in the digital world, propagating like a bacteria and consuming all available resources. In the future, cybersecurity incidents like the May 2017 ransomware attack against the United Kingdom National Health Service might be even more devastating in terms of their real world impact. Robust protocols around system behaviour and investment in policing programs to ensure fair use will be required to manage the risks arising from those programs.

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 development structures to support rapid innovation to protect citizens in a constantly changing landscape

Encryption

In many law enforcement and policy circles 'encryption' has become an increasingly complex operational and legislative challenge. This section provides the inquiry with a critical analysis of how and why law enforcement is challenged by encryption. However, before any analysis of this law enforcement conundrum can be undertaken, or even considered, a more contextual understanding of encryption is required.

To be very clear, encryption is a central contributor to the health of the global economy and business competition. It is not a necessary evil but an essential 21st century societal hygiene factor. In order to analyse the implications of encryption today, you need to understand the historical significance of telecommunications interceptions (TI) to police and their operations.

For law enforcement agencies, the late 1970s were a formative period for TI methodologies. By 1973 there was a telephone in almost three quarters of Australian homes. By 1976, Australians had international subscriber dialling allowing global communications without having to access a switchboard operator: providing a new degree of privacy—a point not lost on criminals.

With new interception technologies in place in the 1970s, law enforcement agencies had access to a wealth of intelligence and evidence. But importantly there was a low likelihood of authorities being detected collecting this evidence. In comparison to human source, undercover and surveillance operations, TI were a low risk activity. The use of covert telecommunications meant no police were required to be deployed to the field so the risk of physical injury to officers was non-existent.

The threats to privacy posed by TI operations were recognised in Australia by the late 1970s, leading to the passage of the *Telecommunications (Interception and Access) Act 1979*. With the arrival of mobile phone technology in the 1980s and 1990s the collection of intelligence by TI had become the default intelligence source for collection managers and police investigators alike. And naturally so: it provided, cheap, easy and low risk intelligence in real time.

Queensland's Fitzgerald Inquiry (Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct) and the Woods Royal Commission (Royal Commission into the New South Wales Police Service) rang the death knell for other covert evidence collection techniques. Both reports highlighted how covert relationships and actions by law enforcement, however well intentioned, can create a slippery slope for corruption. Unsurprisingly, the commissions have left a deep legacy in Australian law enforcement. This legacy has seen an increased application of TI powers and a substantial decline in covert policing capabilities.

Customers, from the halls of government to investigators in local police stations, have over time become voracious consumers of raw intercept reporting. This has led to a devaluation of human source intelligence which often has less direct access, is prone to interpretation and is less timely.

For law enforcement the problems started occurring with the arrival of Blackberry and Viber. But the operational challenges of decrypting these particular platforms were symptomatic of a wider strategic reality.

The Snowden leaks revealed that the US Government were using a patchwork of tools, backdoors and behind closed door relationships to counter encryption—including efforts allegedly focused on undermining the further development of the technology. Despite these efforts governments can no longer develop decryption technologies fast enough to keep pace with the technology markets. And the evolving forms of internet based communication (such

as telegram[1], Chatsecure, Cyrptocat, jitisi) have consistently outpaced the available and emerging interception technology.

Federal Bureau of Investigation director, James Comey, has described this new operational reality in terms of interception intelligence sources 'going dark'. Alleged criminal and terrorist targets are now using increasingly sophisticated encryption services which prevent law enforcement and police agencies from intercepting their communications. The interception intelligence sources are no longer shining a light on the covert activities of these targets.

Encryption is rightfully here to stay and will continue to rapidly improve. And law enforcement must continue to invest in research and development of technology solutions that are legal, affordable and practical. But such investments will continuously fall well short of resolving the encryption challenge.

Government ought to consider the following in response to this challenging operating context:

- 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; and

- Law enforcement and policy makers need to shape public and government expectations of what can be realistically achieved in response to technology disruptions.

The *Telecommunications (Interception and Access) Act 1979* needs to be rewritten in light of the over 40 years of technology disruptions to telecommunications. A number of dated assumptions underpin the *Act.*

- The Australian government had a technological edge over the private sector and could arguably adopt technology rapidly (at least by the standards of the day) to any foreseeable change in the operating environment. However, that's no longer the case.
- Many Australians trusted their government to self-regulate its use of intrusive powers.
- The government would maintain its monopoly control over the telecommunications industry. Deregulation and privatisation have, for better or worse, dramatically changed that arrangement.
- Law enforcement's physical access to telephone communications was a relatively simple affair—a point made particularly clear by Andrew.

While successive governments have progressively amended the Act, they have at various stages failed to engage holistically with the 21st Century's seismic technological paradigm shifts: for example encryption. While many will likely be tempted to continue to tinker with this legislation using minor amendments, the evidence is clear that policy and legislation requires a 'technology' driven disruption.

[1] 1Telegram was created in 2013 by Nikolai and Pavel Durov, the founders of VK (ВКонта́кте or VKontakte), Russia's largest online social network. It is a free, cross-platform, messaging application that offers secure messaging that requires access through an invitation link and is more private than other platforms, such as WhatsApp. The uniqueness of Telegram is that, when a message is deleted at one end, it is also deleted at the other end, thus ensuring that there's no trace of the message. Telegram also allows for a 'self-destruct' mechanism to be added to the message, which effectively means that a timer is in operation for the message.

These will be challenging times for our police and there will be limited time for lamenting what was. Encryption will be one of the most weighty policy challenges for long term Home Affairs capability development and there will be no simple solution.

Further globalisation of crime and declining impact of traditional policing responses

With the rising threat to domestic security from non-state actors, law enforcement agencies face a broad family of threats which are increasingly untouchable using extant police capabilities and legislative powers. The range of transnational untouchables, exploiting the vulnerabilities of international legal regimes, safe havens, and corruption is increasing. Successive Australian Crime Intelligence Commission (ACIC) reports have assessed that non-state actors may represent an existential threat to Australia, Australians and their interests. While such assessments are bleak, and arguably difficult to quantify, it is a truism that these threats do put Australia's rule of law, community safety and economic well-being at peril.

The ability of law enforcement to collect admissible evidence and prosecute these emergent transnational non-state actors is limited in terms of legal jurisdictions. While criminal organisations can cross a border in seconds, the collection of evidence from a foreign jurisdiction using mutual legal assistance treaty arrangements, where they exist, can take weeks or months. While a non-state actor can operate from anywhere at any time, our law enforcement agencies' operational freedom of movement is limited by the geographic borders established in domestic and international law.

Often even with the support of another country, disrupting transnational threats using law enforcement methodologies is challenging. This point is illustrated by the 2017 Sydney plane terrorist plot. In late July 2017 the AFP uncovered a suspected Islamic State plot to blow up an Etihad flight to Abu Dhabi. In this alleged case the IS coordinated in Syria, mailed a bomb kit from Turkey to a terror cell in Sydney.

The detection of transnational criminals is going to become increasingly difficult. In a physical sense proactively identifying deviant financial transactions, people and cargo crossing borders is being made ever more difficult by the exponential growing number of legitimate transactions. 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.

This point is not lost on Australian law enforcement officials and policy makers. While the majority of the Australian government's law enforcement efforts are focussed on arrests and seizures, a very small yet incredibly successful number of enforcement officers are focussed on the disruption of threats—especially organised crime–using soft power including capacity development. Such efforts are not easy, and should not be viewed as an easy solution to the problem of resilient criminal targets.

The ICT capabilities of Australian law enforcement agencies

Given the classified nature of law enforcement ICT systems it is impractical for an external observer to make specific comments on extant arrangements. This withstanding, the following general observations are provide for the committee's consideration based on my experiences as an intelligence executive:

- As highlighted earlier in this submission the frequency of technology disruptions is increasing exponentially. The implications of the current trajectory of technological developments is the life cycle of ICT investments will be drastically reduced. So while the AFP's current case management system might be decades old, the next one will not have the same usable life.
- Current acquisition requirements, as outlined within relevant Department of Finance guidelines, no longer meet law enforcement needs. And under certain circumstances may impeded 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.

Engagement by Australian law enforcement agencies in our region

International engagement, including cooperation and capacity development, has become a central pillar in AFP, ACIC and ABF strategies for most crime types. This cooperation is just as important in terms of technology as traditional law enforcement. These networks are increasingly under financial pressures, with the AFP's international footprint continuously shrinking over recent years.

Since 1987, the efficiency dividend has been a central principle in successive Australian budgets. The efficiency dividend initially resulted in reductions to inefficient expenditure in non-operational areas within national security agencies, which was long overdue. As the number of non-operational efficiencies available to decision-makers decreased, cuts to operational expenditure became inevitable and, finally, commonplace.

To address the effects of reductions in expenditure, national security agencies developed new policy initiatives to obtain sufficient funding to offset risks to national security. For 10 or so years, a delicate equilibrium of cuts and 'just in time' policy initiatives was maintained. The budget of the last three years has seen a drastic reduction in the availability of new funding—which is resulting in incremental reductions in Australia's national security capability.

Further complicating and undermining the funding arrangements of organisations such as the AFP is the new policy initiative offset methodology adopted by successive federal governments since 2008. In this approach, departments that submit new policy proposals to government must offset the expenditure from within their existing budget. The end result is a continuous erosion of funding for existing programs of work, such as the highly regarded AFP international network. Careful consideration must also be given to the removal of the efficiency dividend from all Home Affairs agencies.

The role and use of the dark web

Much has been written in the media about the dark web and dark markets: a large percentage of which verges on moral panic. In the process there has been conflation of these two issues into one problem. To be clear the internet is comprised of two parts: the part that is indexed by search engines and that which isn't (the deep web). A small portion of this deep web is comprised of what has become known as the 'dark web'. In these areas of the internet exist secure networks of various sizes. These networks, and their data, are protected by a range of

technology including encryption. Within some of these dark web networks are buyers and sellers who combine to create dark markets: more often than not dealing in illicit commodities.

With this conceptual model it becomes clear that the World Wide Web, deep web, dark web and dark markets all provide law enforcement with particularly complex problems. More often than not, the main focus of the public policy dialogue in this area has been on specific dark markets. While law enforcement has experienced significant success in shutting down specific dark web networks, like Silk Road, they are yet to be prepared for the potential disruptive effect of these networks going mainstream.

Contemporary case categorisation and prioritisation for western law enforcement agencies is focussed on identifying and disrupting large shipments of illicit commodities. Or as an alternative identifying and prosecuting senior members of organised crime syndicates as a means of disruption. The dark markets, should they be engaged by larger numbers of drug consumers, could render contemporary policing models all but useless. Instead of large shipments of illicit drugs or weapons crossing the border, organised crime groups could completely decentralise the market: in the process increasing their profits. Australia's mail and cargo systems could be swamped with small imports that under current models would not reach the threshold for law enforcement action. Already senior law enforcement officers in the Northern Territory report their belief that the majority of meth amphetamines are already imported this way.

In response to these challenges the PJCLE ought to consider recommending:

- As a matter of priority, the Australian Criminal Intelligence Commission establish an Indicators and Warning (I&W) solution for this problem. The I&W solution needs to be developed in such a way as to be able to identify disruptive changes in the global supply illicit chains that impact on Australia's market.
- An independent entity, like ASPI, ought to be engaged to review current case categorisation and prioritisation models used by agencies within the Home Affairs Portfolio.
- The Home Affairs Portfolio, in conjunction with its portfolio agencies, consider how existing network focussed strategies, such as that used to close Silk Road, can be further enhanced.

The role and use of encryption, encryption services and encrypted devices

In June 2017, ASPI Senior Analyst Dr Andrew Davies painted a rather bleak picture of the future of TI: '[T]he access to data through lawful intercept that our security agencies once enjoyed will never be possible again.' The loss of TI effectiveness will hit the Australian law enforcement community particularly hard: it's the fundamental building block for complex investigations.

Collection management is an often overlooked, yet critical, component of any successful intelligence endeavour. For law enforcement agencies, greater emphasis needs to be placed on adequately developing intelligence professionals who can approach the problem of collecting intelligence and evidence in an imaginative manner, using a combination of intelligence disciplines. There can be no doubt that in the emerging law enforcement operating environment the collection of evidence and information will be riskier and more difficult. But there appear to be few other options.

While collection management will provide a roadmap for where to go next, the loss of TIs will necessitate greater investment in alternative collection disciplines, which will be costly. At the very least, physical surveillance and undercover and human source capabilities will become

increasingly important in our future TI-dark world. The Home Affairs Portfolio, including the ACIC and the AFP seek to further enhance the Commonwealth's online undercover capabilities.

While the decryption communications, we should not turn our back on technical intelligence or the exploitation of the electromagnetic spectrum. Through the study of communications using tried and tested techniques such as traffic analysis, intelligence value can still be drawn from identifying communication patterns.