ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008-3105, USA
Web Site: *www.isaca.org*

Telephone: +1.847.253.1545
Facsimile: +1.847.253.1443
E-mail: *info@isaca.org*

15 January 2018

Sophie Dunstone
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Ms. Dunstone:

On behalf of the approximately 4,000 ISACA members within Australia, and the nearly 160,000 professionals who are part of ISACA's global community, we are grateful for the opportunity to respond to the Parliamentary Joint Committee on Law Enforcement's inquiry regarding the impact of new and emerging information and communications technologies (ICT).

In the attached document, you will find our responses to the questions posed by the Joint Committee. Though your initial correspondence came to our international headquarters, I have taken the liberty of consulting with some of the leading members within ISACA's Australia community for their insights and perspectives. ISACA's Australia and global communities would be pleased to continue to be a part of this important conversation, and to contribute to the Committee's and the Australian Parliament's ongoing efforts in this area.

If you would like additional information regarding any of the elements contained in our submission, please do not hesitate to reach out to me at your convenience at , or to ISACA's Australia leadership at or . Additionally, ISACA would welcome the opportunity to have a broader and ongoing discussion on these issues, should Committee leadership wish to do so. Thank you in advance for your time and consideration.

Respectfully submitted,

Matt Loeb
ISACA CEO

Jo Stewart-Rattray
ISACA International Director

Adam Wood
ISACA Canberra President

About ISACA

ISACA helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association representing approximately 160,000 information and cybersecurity professionals throughout the world, including nearly 3,600 in Australia. As part of ISACA's efforts to support the global IT professional community, ISACA offers COBIT®, a business framework to govern enterprise technology, and the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource to assist organizations in developing skilled cyber workforces and enabling individuals to grow and advance their cyber careers.

ISACA®

Responses to Parliamentary Joint Committee on Law Enforcement Inquiry

What are the challenges facing Australian law enforcement agencies arising from new and emerging ICTs?

There is really only one primary challenge, but all other challenges flow from it: keeping pace with the advancement of new and emerging technologies, especially in areas such as ICT. Combatting crime in the digital realm does not require being 'adequate to the task'; it requires being exceptional in the face of that task. It is imperative that Australia's law enforcement community remain at the leading edge of ICT technologies, to ensure a safe, prosperous, and forward-focused Australia.

What will the impact of new and emerging ICTs have on the ICT capabilities of Australian law enforcement agencies?

Overall, the ICT capabilities of most Australian law enforcement agencies are fairly mature:

- The **Australian Criminal Intelligence Commission** provides the nation with a comprehensive national picture of criminality in Australia, while concurrently sharing that information through national information and intelligence sharing system and network.
- The **Australian Institute of Police Management** provides training programs to leaders within the emergency services, and serves as a repository for databases and educational resources to current and former Institute students.
- The **Australian Commission for Law Enforcement Integrity** detects and deters corruption in the public sector and law enforcement, and are currently enhancing their cyber and data analytics capabilities to aid them in their efforts.
- The **Australian Cybercrime Online Reporting Network**, a national joint law enforcement initiative of the Commonwealth and state and territory governments, created as a result of the National Plan to Combat Cybercrime developed by the Attorney-General's Department in 2013,[1] provides information on how to identify cybercrime and methods of mitigating the risk of being affected by common cybercrime.
- The **Australian Federal Police (AFP)** play a pivotal role in enforcing federal criminal law and protecting the Australian national interests from crime by operating in the evolving digital and law enforcement landscape. The AFP Corporate Plan 2017-18 lists a key focus of the AFP's capability development in continuously building on the ability to strengthen information on demand as well as detect, prevent and predict serious crime through deep data exploration. Other key focuses identified in the Corporate Plan include the ongoing partnerships with industry to invest in innovation to combat serious and organised crime. [2]
- The **Prime Minister** launched Australia's Cyber Security Strategy in 2016 as a roadmap for creating a 'cyber smart nation', and keeping Australia safe and competitive in our digital world. Several of the Strategy's objectives are of importance to Australia's law enforcement community. These include, but are not limited to: the creation of jointly operated cyber threat sharing centers and an online threat sharing portal; partnering internationally to prevent cybercrime and other malicious/nefarious cyber activity; and helping to build capacity and awareness within Australia's public and private sectors

[1] ttps://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx
[2] https://www.afp.gov.au/sites/default/files/PDF/AFPCorporatePlan2017.pdf

through the development of a highly-skilled workforce and the raising of citizens' awareness of the risks and benefits found in the cyber realm. [3]

All these organizations and initiatives have served to move Australia forward, have been of benefit to Australia's law enforcement community, and are playing a critical role in aiding that community as it addresses challenges arising from new and emerging ICTs. Even the Prime Minister's efforts to grow a 'cyber smart nation' aid the work of law enforcement.

One challenge for law enforcement remains, however—and it will be a challenge that, unfortunately, may never go away: keeping pace with the advancement of technologies, particularly ICTs. Work such as the AFP's deep data exploration is not merely welcome, but necessary, as law enforcement strives to keep up with criminal and other actors. With advances in distributed ledger technologies, artificial intelligence and machine learning, quantum cryptography, and predictive analytics looming on the horizon, the question is not ***if*** Australia's law enforcement community will see a changing threat landscape, but ***when***.

With a global digital economy has come global digital criminality. As a result, Australia's law enforcement community must now devote its scrutiny to not only Australia, but the whole of the world. Though this is a daunting task, it is nonetheless one which the Australia law enforcement community has risen to. As we work to ensure adequate protection of Australia's citizenry, however, we must never forget that the progress of technology does not stop. Because of this, neither can our focus on ensuring that Australia's law enforcement community is up to addressing any and all challenges that arise from new or emerging ICTs. One way of doing so is continual monitoring and measuring of cybersecurity capability, and benchmarking against other law enforcement entities, both within Australia, and throughout the world. In this way, no law enforcement leader is left to wonder if their cybersecurity endeavors are up to the task; they will know if they are or are not.

It is also worth noting that advances in ICT affect personnel—specifically, the ability to retain trained, high-quality professionals. In late 2016, global job posting website Indeed released a study which compared the number of jobs posted to the 'clicks' received from job seekers searching for employment. Approximately 42% of those looking for cyber security positions in Australia searched the available posted jobs. The correct balance, in which the demand for candidates and the supply of professionals are equivalent, should be 100%.

Australia's law enforcement community is no different from the rest of Australia. There is a shortage of cyber security professionals within law enforcement's ranks as well, and ICT and cyber security professionals in law enforcement that show promise are often lured away by private sector enterprises. A 2016 survey by Australia's Information Security Association (AISA) indicated that state and local governments were two of the three largest industry segments most affected by the shortage of cyber security professionals.

What will the impact of new and emerging ICTs have on engagement by Australian law enforcement agencies in our region?

The regional cooperation and engagement of Australian law enforcement agencies focuses primarily on three areas: intelligence sharing; transnational crime prevention and detection operations; and extradition of criminals and the international transfer of prisoner casework.

[3] https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

International law enforcement cooperation relationships are typically facilitated by bilateral and multilateral treaties. However, in some cases, Australia has a non-treaty arrangement with particular countries.

In October, Australia's Foreign Minister launched the "International Cyber Engagement Strategy". The purpose of this is to foster relationships between Australia and Asia-Pacific nations, such as China, New Zealand, South Korea and India, and improve connectivity, collaboration, and access throughout the region, especially in areas such as cyber security and internet governance.

Australia exchanges cyber security information and capabilities to improve their understanding of international threats. There is also a collective ability to prevent, detect and mitigate cyber threats and risks. The Australian Cyber Security Centre (ACSC) in particular engages with various international cyber organizations. The Strategy has also led to the formation of the Asia Pacific Computer Emergency Response Team (APCERT), a combination of CERTs from several nations that monitor and protect cyberspace in the region. It is also anticipated that overall regional cyber security capability will be strengthened as a result of the establishment of the Pacific Cyber Security Operational Network (PaCSON) to provide operational points of contacts.

All these efforts—the recent launch of Australia's International Engagement Strategy; the regional and global engagement of ACSC; the synergistic protection efforts of APCERT's member CERTs, and the anticipated establishment of PaCSON—currently serve and will continue to serve to strengthen cybercrime prevention, prosecution and cooperation throughout Australia and the wider Asia-Pacific region. These collaborative transnational efforts improve our neighboring countries' ability to prevent and respond to cybercrime while concurrently underpinning economic growth and creating a safer digital environment for Australian businesses and citizens. This work also deepens Australia's bilateral, regional and global partnerships, collectively building mutual capabilities to combat the international issue of cybercrime.

As was noted in an earlier response, the ever-swifter pace of advancing technology, particularly in ICTs, will necessitate a similar swift pace of evolution within Australia's law enforcement community. This need does not change once one considers Australia's law enforcement community on the broader international stage; in fact, if anything, this need intensifies. In the coming years, collaboration between national law enforcement communities will become increasingly vital in combatting cybercrime, and the nations at the forefront of these cooperative efforts will reap the benefits in enhanced capabilities.

What will the impact of new and emerging ICTs have on the role and use of the dark web?

Regrettably, 'advances' are not the sole purview of law enforcement; criminals and other bad actors are able to make use of them as well. Advances that we noted earlier, in areas such as cryptology, distributed ledger technologies, predictive analytics and quantum computing, can all be exploited by those who make use of the dark web.

The biggest threat of new and emerging ICTs, though, is that they could negate the need for a 'dark' web. If distributed ledger technologies make illicit transactions impenetrable to law enforcement, why must they remain hidden? If the quantum encryption used on a quantum computer can't be broken, is there a need for a bad actor to hide their efforts in the shadows?

When the 'dark' web no longer needs to hide, it becomes mainstream—as do its offerings. That is perhaps the most negative impact new and emerging ICTs could have on the dark web; the creation of Amazon- and Alibaba-esque companies as one-stop-shops for all things illicit, illegal, lethal and loathsome—on the same internet where the global community engages in digital commerce.

ISACA®

What will the impact of new and emerging ICTs have on the role and use of encryption, encryption services, and encrypted devices?

Encryption, encryption services, and encrypted devices currently pose a problem (and will continue to pose a problem) for Australia's law enforcement community—as they do for law enforcement entities around the world. As ICT technologies evolve, the encryption those technologies make possible will evolve as well. There is no easy answer to the encryption question: nations have been wrestling with it, from different perspectives, for several years now, and as technologies advance, there will be new issues that will require discussion. The discussion of encryption, encryption services and encrypted devices is a conversation all its own, for it touches upon issues of surveillance, personal information capture, and a wealth of additional concerns. Respectfully, it could, in fact, comprise the entirety of another inquiry.

Until an adequate answer to encryption and encryption-related issues is found, however, the best alternative might be to focus law enforcement-support on research and development (R&D) in these areas. It is possible that such R&D efforts could yield tools that Australia's law enforcement community could use in their work to address encryption and encryption-related issues. Regardless of the outcome of this R&D work, though, such tools will need to address the concerns of both law enforcement and the general public, and do so in a way that satisfies both groups.

What will the impact of new and emerging ICTs have in other relevant areas?

What has not yet been discussed in these responses is the impact new and emerging ICTs will have upon the law enforcement community as professionals, and this is an area worthy of focus. Law enforcement professionals will increasingly need to be grounded in technology, and possess a level of expertise that enables them to spot cybercrime, whether it occurs on smartphones on the street, or across T1 lines connected to the digital center of a financial institution.

Likewise, leadership in law enforcement will need to possess expertise in ICT technologies as well, to improve decision making, allocation of resources, strategic planning, and other undertakings. When the law enforcement community—from local officials to the national levels—are aligned in this manner, change becomes swifter, and the ability to anticipate and respond to technological advances improves.

These same professionals, however, will rely upon technology, and it is imperative that the tools designed for the law enforcement community have robust yet adaptable security and privacy built into them at the design and development stages. Crime does not take a holiday; the tools used to prevent it must be up meeting the challenges of an ever-present, ever-shifting threat landscape. Those tools must be strong enough to meet the task at hand, yet flexible enough to retain their inherent security over their lifecycle as products.

At a global level, it is also important to engage Australia's law enforcement community in international standards development efforts, as well as the crafting of multinational cyber norms, agreements, and similar pacts. As was pointed out earlier, cybercrime is borderless; the pursuit and thwarting of those engaged in criminal or malicious activities must be able to rely upon similar easy movement throughout the global digital realm. Transnational reciprocity, multinational sharing centers, and similar constructs are of vital assistance to ensure Australia's law enforcement community remains ahead of cyber criminals and other bad actors.