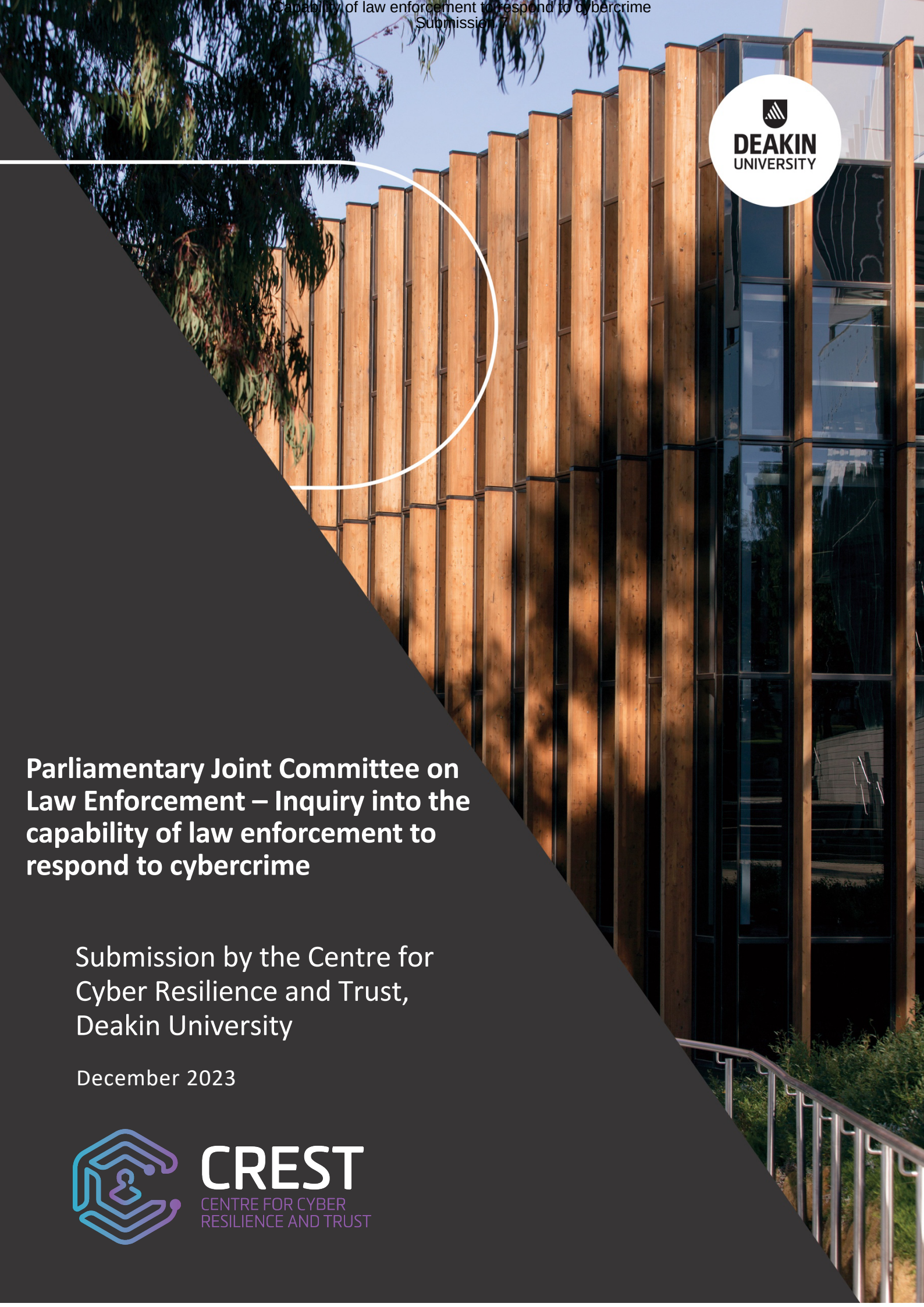

Parliamentary Joint Committee on Law Enforcement – Inquiry into the capability of law enforcement to respond to cybercrime

Submission by the Centre for Cyber Resilience and Trust, Deakin University

December 2023

CREST
CENTRE FOR CYBER RESILIENCE AND TRUST

Parliamentary Joint Committee on Law Enforcement – Inquiry into the capability of law enforcement to respond to cybercrime

Submission by the Centre for Cyber Resilience and Trust, Deakin University
14 December 2023

Co-authors

Contact Email:

About Us

CREST brings a multi-disciplinary focus to the changing landscape of cyber harms and the extent to which people, organisations, and communities are dependent on the growing digital economy. The term 'cyber resilience' encompasses but extends beyond the notion of conventional understandings of 'cyber security'. Our focus on cyber resilience exists at individual, organisational, and societal levels, and emphasises a need to move beyond a singular focus on preventing cyber security incidents to also anticipating, protecting, detecting, mitigating, disrupting, and recovering from them. CREST seeks to analyse the role of trust in the design of systems, cyber security technologies, and the capabilities of users. We examine mechanisms of trust in both technology and humans – how these are created and what they can achieve – in advancing cyber resilience.

CREST aims to utilise multi-disciplinary expertise to design state-of-the-art cybersecurity solutions by responsibly leveraging emerging technologies such as artificial intelligence, blockchain and quantum computing whilst also enabling a comprehensive understanding of the role played by the human factor and governance in cyber security. We employ the term 'human factor' to consider a broad suite of attributes relevant to cyber resilience at the individual, institutional, and societal levels. This conceptualisation includes individual human behaviours, as well as the social structures that enable collective action by groups and communities of various sizes, and the diverse public and private interventions that shape societal responses. We also seek to directly extend our focus to the diverse actors responsible for cyber harms, and the institutions and regulatory approaches necessary to prevent, minimise, and recover from such harms. Our focus on the human factor also extends to the notion of 'usable security' – ensuring that cyber security technologies are designed to be user-centric, inclusive, and affordable.

CREST adopts multi-disciplinary approach to these critically important knowledge gaps through five interrelated areas of impact:

- Advancing cyber security technologies
- Securing data and infrastructure
- Promoting cybersafe behaviours
- Disrupting cyber harms
- Harmonising cyber governance

a) Existing law enforcement capabilities in the detection, investigation and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes

Response:

While there is limited research on the existing capabilities of law enforcement in an operational sense, the Australian and international literature continues to highlight the growing challenges cybercrimes present for law enforcement capabilities. With the exception of child exploitation offences, which law enforcement tended to prioritise early in most developed economies, research suggests that current law enforcement capabilities are largely inadequate to deal with the growing volume and complexity of cybercrimes, including cyber-enabled and cyber-dependent crimes. We make this observation based on two interrelated points.

First, police organisations tend to view cybercrimes as a 'specialist' domain, yet they largely maintain a 'generalist' ethos to policing. This is understandable given the unique properties of cybercrime relative to other police priorities. However, cybercrimes – certainly cyber-enabled crimes – are not only 'volume' crimes but traditional crimes increasingly involve cyber components. The notion of 'cyber-enabled' is therefore becoming less and less pertinent in a digital society and economy. Given most police cybercrime units are relatively small compared with most other specialist areas or commands of police organisations, there is an increasing necessity for cyber units to become more selective regarding the cases they take on. This leaves a significant – and growing – gap in the number of cases reported relative to those that are investigated, especially those traditional crimes facilitated by technology.

Second, while some knowledge and skills pertaining to investigations are transferable across many crime types, it is undoubtedly the case that cybercrime is the most unique – and therefore least transferable – crime type in terms of investigative capabilities. Investigating cybercrimes requires technical expertise that takes a long time to acquire and demands particular investment from police organisations regarding education and training. To date, police organisations have approached this challenge in different ways, including a) recruiting people (sworn and unsworn) into police organisations that have these skills, b) educating and training people in these skills internally, and c) providing external education and training opportunities for staff. In our view, significantly greater investment in all three (and more) of these strategies is required.

Overall, we make the following observations for consideration in this inquiry:

1. Police organisations should approach cyber-dependent crimes as a properly constituted specialist function. This requires moving away from a generalist ethos to policing, which suggests that police knowledge and skills are transferable, to recognising that cybercrime, especially cyber-dependent crime, is a distinct crime type that requires career specialists in that domain. This means cybercrime should be an area where police are able to specialise as well as achieve career advancement opportunities (including promotion and higher remuneration) within that area.
2. Police should carefully define and continually calibrate the workload of specialist cybercrime units. It should be clear that specialist units are unable to manage all cybercrime. Cybercrime is a broad concept that can encompass an increasing number and volume of crime types. We believe that the only realistic scenario is for police to plan for most cyber-enabled crimes to become business-as-usual policing. Essentially, this means specialised units will deal with the more complex and harmful cybercrimes – including cyber-dependent (e.g., ransomware and hacking) and sophisticated enabled crimes (e.g., transnational organised cybercrime such as online child exploitation and complex online scams) – within their respective jurisdictions, as well as provide services such as education and professional development for the wider organisation. However, we suggest that basic, foundational knowledge and skills regarding technology and cybercrime should be provided as part of the general training at the Academy and reiterated in ongoing training thereafter.
3. Police organisations need to become more diverse in design and composition, particularly regarding embedding non-police expertise. For example, in our view, one of the most promising strategies for enhancing police cybercrime capability is by harnessing (unsworn) civilian expertise. This is already underway to varying degrees in Australian policing (as it is elsewhere), but international research would suggest continual effort is required to understand clearly how civilians fit structurally and culturally in police organisations, and how to make civilians essentially equal partners in contemporary police organisations.

Police organisations can likely better utilise civilian expertise from numerous disciplines, including criminology, cybersecurity, data science, mathematics, and so on.

On top of these three broad observations, there are overarching philosophical components that we believe need to be considered, as well as practical challenges that need to be addressed. In responding to the philosophical first, these include embracing specialisation *as well as* a broader concept that police organisations should prioritise becoming more technically sophisticated and diverse organisations rather than necessarily larger organisations. For example, it is possible to employ people such as data scientists who can develop creative, technical solutions to workload that would mean an organisation can be more effective and productive with fewer staff. Prioritising education and development of current staff may also be more productive than seeking to recruit new members and may also assist with retention in this area.

Practically, we recognise this approach is quite unique and challenging for police organisations on a number of levels. In addition to points we have already mentioned, we would note:

- *Resourcing*: Significantly more resourcing is likely needed in cybercrime units in all jurisdictions and more capabilities to deal with less harmful and sophisticated cybercrimes outside of cyber units. It is likely that cybercrimes will demand a similar level of resourcing to other crime types (e.g., drugs, organised crime) from police organisations over the next decade.
- *Industrial Relations*: Engagement with all stakeholders would be necessary to negotiate the above points we have mentioned, including the potential for more flexible workplace agreements regarding salary and opportunities for career advancement (as most promotions are tied to managerial responsibilities which may not be reflective of where cyber specialists may wish to go and can result in cyber units losing critical expertise).
- *Education and training*: It is axiomatic that more education and training is needed. We fully appreciate the curriculum for police training at the Academy is already very crowded, with essentially little to no room to add further components without taking others away. In our view, police organisations need to plan for cybercrime and emerging technologies broadly taking up more space in training at the Academy. This means assessing what can be delivered in other ways. Furthermore, police could think about ongoing training in this area at all levels, with customised training for those in different roles: e.g., frontline officers, investigators, cyber specialists, and those at different levels of management. In addition to initial training, opportunities for ongoing training and development will be key. In our view, a much higher proportion of budgets would need to be allocated to ongoing professional development. We comment on this again later in this submission.
- *Recruitment and retention*: People with cyber expertise are in high demand not only across the economy but also in other public sector agencies. Retaining these people is likely a challenge for law enforcement. The benefits of working for law enforcement can be better articulated to potential recruits, including a sense of career satisfaction that people may acquire from their work. Together with enhanced career prospects, this could assist with law enforcement recruitment and retention efforts.

b) International, federal and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats

Response:

Our understanding is that there have been considerable improvements in relation to international, federal, and inter-state jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats.

Nationally, there are various (formal and informal) mechanisms for law enforcement and other government stakeholders (e.g., Australian Cyber Security Centre (ACSC), Australian Signals Directorate (ASD)) to share information. We comment on some of these below.

Internationally, we also understand that there are effective mechanisms for sharing information and threat related intelligence, particularly across the Five Eyes. If there is any scope to improve these arrangements, it would likely be in non-Five Eyes countries. The International Counter Ransomware Taskforce, currently chaired by Australia, is an

ideal such forum to assist in coordinating collective responses to cybercrimes of international concern. It is also important to build stronger connections with like-minded countries/economies. The Global Cooperative and Training Framework which Australian Government is an official member could be a good platform for Australian Government to build network for exchanging threat intelligence with like-minded countries/economies.

Furthermore, current observations regarding the capabilities of neighbouring countries, particularly the Asia-Pacific, would suggest there is a need for further investment in capacity-building and cyber security awareness raising elsewhere. We note that further investments in this area are outlined in the *2023-2030 Australian Cyber Security Strategy*, but these appear to be focused predominately on responding to cyber incidents rather than a) preventing them and/or b) enhancing the capacity of neighbouring countries to respond.

c) Coordination efforts across law enforcement, non-government and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime

Response:

Once again, our understanding is that several promising initiatives are underway in relation to coordination efforts across law enforcement, non-government, and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime. Some of these have been established for some time, others are more recent. Examples of the former include the Joint Cyber Security Centres in most jurisdictions. Examples of latter include the Joint Policing Cybercrime Coordination Centre (JPC3) based in Sydney. The JPC3 has much potential to improve coordination efforts across Australian – and international – law enforcement efforts to respond to cybercrime.

Nonetheless, it is likely that further improvements can be made when we consider coordination across law enforcement, non-government, and the private sector. While there are various mechanisms established by the ACSC and ASD more broadly, these appear to be more narrowly focused on cybersecurity professionals. We note that JPC3 has a prevention and community outreach function, which may help fill this gap, which seems particularly applicable to non-government and small-medium size enterprises (SMEs). It is, however, important that there is a nationally consistent approach to education and outreach activities, and that it is properly designed and evaluated. It is quite likely that different levels of messaging will be required for different audiences (a point we return to below).

We would note that there appear to be significant opportunities to enhance collaboration with education providers (TAFE providers and universities). This would only assist to improve education and training for existing and new recruits. Furthermore, law enforcement agencies could leverage strategies such as student internships and guest lectures, addressing security considerations as appropriate, which could also assist with their recruitment efforts. Finally, we believe that collaboration with universities in particular could be improved with regard to research. There are many countries – including those in the Five Eyes – that have much more integrated arrangements for meaningful research collaborations between academia and law enforcement.

d) Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians

Response:

Many of the current and emerging cybercrime threats and challenges affecting Australia are outlined in the *2023-2030 Australian Cyber Security Strategy*. Unfortunately, despite significant new investments domestically and increasing international attention, we can realistically expect that the volume and complexity of cybercrime will only accelerate. Increasing geo-political instability, and the fact that some states are not capable to deal with or appear (at the very least) to tolerate cybercrimes from within their borders, will continue to pose significant limitations on the opportunities available for Australian law enforcement. We comment on these last in this submission. In addition, and again as noted in the strategy, the growing risks posed by Artificial Intelligence (AI) and Internet of Things (IoT) need to be considered. AI may be used by cyber criminals to prepare and conduct various cyber attacks, ranging from

phishing emails to scams, and pose additional risks with regard to child exploitation offences, domestic violence, data breach, as well as the dissemination of fake news and disinformation campaigns. All of this necessitates, in our view, a more novel response from law enforcement agencies over the next decade.

Amongst these responses, we applaud the federal government's establishment of the Joint Standing Taskforce between the Australian Federal Police and Australian Signals Directorate. We believe that the remit of the taskforce in conducting offensive operations against foreign threat actors is an appropriate one given the geo-political challenges noted above. Despite the necessity in pivoting towards offensive, disruption interventions, there are a range of risks and challenges associated with this approach that require careful consideration and management. We comment on some of these issues in Section G of this submission.

e) Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime

Response:

In our view there is significant opportunity to prevent and reduce cybercrime through strategic initiatives that are properly designed, implemented, and evaluated. Regarding victimisation, significant investment has occurred in the public sector in all jurisdictions as well as most larger enterprises, many of which at the very least understand the ASD's published *Strategies to Mitigate Cyber Security Incidents*. As previously mentioned, there is a significant gap around SMEs as well as individuals vulnerable to various types of cybercrimes. We believe further research would be useful in terms of identifying the specific requirements of SME owners and operators as well as what strategies are most effective at reaching this (highly diverse) audience.

It must also be recognised that prevention and education approaches is crowded territory. Careful consideration needs to be given about what role various bodies have in this domain, including (as examples): the Australian Cyber Security Centre, the Australian Federal Police (e.g., via JPC3 as well as the Australian Centre for Countering Child Exploitation), state and territory police, the eSafety Commissioner, and the various entities involved in business registration in each jurisdiction along with financial institutions, telecommunications providers, and so on.

f) other related matters

Response:

We wish to raise the following additional points for consideration by the inquiry.

1) Question A asks specifically about existing law enforcement capabilities in the detection, investigation, and prosecution of cybercrime. We note here that cybercrimes are rarely 'detected' by law enforcement. Indeed, in many instances, police are less likely to be first responders to many cybercrimes, certainly cyber-dependent crimes experienced by larger entities. These trends further underscore the unique properties of cybercrime relative to other crime types. In addition, given that a large proportion of cybercriminal offenders appear to be located in foreign jurisdictions, police investigations are less likely to result in prosecutions compared with most other crime types. Much of this has underpinned the Australian Government's recent focus on *disrupting* and *deterring* cybercriminals, as outlined in the *2023-2030 Australian Cyber Security Strategy.* We feel that more work is required in defining 'disruption'; what strategies and tactics need to be developed in this domain in order to be effective; and how disruption activities are coordinated with international partners.
2) A related point is that all law enforcement agencies need to carefully consider what success looks like given that a) many cybercrimes are likely to grow no matter what law enforcement do about them (noting, however, there is a lot that can be done to reduce the extent to which they do continue to increase); and b) many traditional metrics police use to communicate and evaluate outcomes (arrests, prosecutions, seizures, etc.) are less available in the domain of cybercrime. Due consideration needs to be afforded regarding how

novel disruption interventions are internally monitored and evaluated, such that effective programs are rewarded and expanded. How successes in this area are to be communicated to the Australian public also requires careful management. This will require inevitable trade-offs between needs for operational secrecy and for visible policing to reassure the Australian community that law enforcement and the government more broadly are doing all they can to ensure their security.

3) Much more consideration should be given to improving the experience for victims of cybercrime. We are pleased to see this recognised in the *2023-2030 Australian Cyber Security Strategy*; however, the strategy seems to focus predominately on victim entities and/or victims of identity crime. There is, in our view, important consideration required as to what the role of law enforcement is and should be in relation to supporting a wide array of cybercrime victims. At present, research would suggest many victims are unsatisfied with their experience of reporting cybercrimes. There is also a growing risk of 'victim-blaming'. In our view, if these problems are left unaddressed, they risk undermining the legitimacy of the police and government more broadly.
4) Australia has significant number of immigrants and indigenous communities. It is important that all governments take into consideration of the cultural and language differences while designing preventative programs and raising awareness. We see certain cybercrimes appear to be intentionally targeting migrant groups and international students. There is a need to design innovative ways to effectively disseminate messages relating to cybercrime prevention to these groups.
5) In addition to victimisation, we see opportunity for Australia to focus on domestic cyber offender prevention programs. We are aware of work being undertaken in the United Kingdom and the Netherlands in this regard, which has significant potential to prevent and reduce cybercrime. We also see merit in properly designed and evaluated early detection programs as well as offender rehabilitation programs.
6) The 2023-2030 Strategy re-emphasises Australia's determination to support and promote the Council of Europe's Convention on Cybercrime (Budapest Convention). However, it is crucial for Australia to be a gatekeeper and closely watch and contribute to the development of the United Nations (UN) Convention on Cybercrime, to make sure it will not have adverse implications for freedom of speech and basic human rights. It is also crucial for the Australian Government to work closely with democratic economies that are not members of UN or other international organisations such as Interpol through a 1.5 track or 2 track, if 1 track is not possible.