2023-2030 Australian Security Cyber Strategy - Public Submission

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

April 2023

CREST
CENTRE FOR CYBER RESILIENCE AND TRUST

2023-2030 Australian Security Cyber Strategy - Public Submission

Submission by the Centre for Cyber Resilience and Trust, Deakin University
15 April 2023

Co-authors

Associate Professor Lennon Yao-Chung Chang

Dr James Martin

Professor Chad Whelan

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

In our view, the revised Cyber Security Strategy should include:

- Mandates for the adoption of robust cyber security standards across private industry where appropriate, and incentives for small-to-medium sized enterprises (SMEs) to meet these standards in ways commensurate with their resources and business models.
- Measures to strengthen regional and international collaboration on cybercrime investigation and enhancing cyber resilience in the region. Cyberattacks and cybercrime are without borders and Australia cannot combat these issues alone. Strengthening developing countries' cyber capacity and maturity will also contribute to Australia's cyber security.
- Expansion of bilateral and multilateral security partnerships to incorporate 'cyber' amongst traditional security domains (air, sea, land and space).
- Regular review of Australia's cyber maturity and capacity.
- Enhancing trust and collaboration between the public and private sectors, as well as with individuals, to build cyber resilience. There needs to be greater community awareness of how to respond to cyberattacks, who to call and what help is available.
- Stronger platforms and incentives for collaborative research between government, industry, and researchers across numerous disciplines. This should include dedicated programs of government funding and procedures for promoting trust and removing barriers (e.g., facilitating researchers to obtain necessary security clearances). In Australia, collaboration between government and academia is a long way from the ideal state – several countries are far more advanced in this domain.

Further to these aims, we recommend the development of a national Australian Cyber Doctrine that would articulate the principles, rationale and strategies underpinning the government's approach to both defensive and offensive cyber operations.

The Cyber Doctrine would:

- assist in informing whole of government responses to cyber threats.
- ensure that government cyber operations are optimally calibrated to achieve national security aims.
- ensure that government's cyber operations remain consistent with our values, foreign policy objectives as well as with domestic and international laws.

Given the diversity and novelty of state, semi-state and private criminal threats that are prevalent and emerging in the cyber domain, coupled with the significant strategic and geo-political implications associated with offensive cyber operations in particular, the Cyber Doctrine should be informed by experts in defence,

cybersecurity, security studies, criminology and international relations across government, private industry and academia.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

We recommend that the government include additional infrastructure such as screens and monitors used for public broadcasting purposes in the Act or other Acts to cover attacks on these system during an election or other important events to disseminate unwanted messages and/or dis/misinformation. While the Security of Critical Infrastructure Act provided a clear definition of critical infrastructure, it excluded some types of attacks that may target non-critical infrastructure but that may still result in national security concerns and cause alarm amongst the public. For example, during US House Speaker Pelosi's recent visit to Taiwan, TV billboards at train stations and convenience stores came under mass and organised cyberattack, replacing the usual content of the screens with dis/misinformation. Such attacks against important but non-critical infrastructure carry the potential to cause panic and spread harmful content, especially during times of geo-political tension or conflict.

2.d. Should Australia consider a Cyber Security Act, and what should this include?

Cyber security is a broad area involving both technology and human behavior, whilst also carrying implications for national security, criminal justice, politics, and economics. It would therefore be difficult to have an Act that refers to all of these issues in detail. Rather, we suggest that an Australian Cyber Security Act include high level principles and policy on cyber security. Similar approaches can be seen in Japan (the Basic Act on Cybersecurity[1]), the People's Republic of China (Cybersecurity Law of the People's Republic of China[2]) and Taiwan (draft Technology Basic Law).

2.f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:
(a) victims of cybercrime; and/or
(b) insurers? If so, under what circumstances?

While prohibiting payment of ransom and extortion demands by cyber-criminals has considerable appeal, this is likely to have significant risks and unintended consequences that, on balance, would make this approach unviable at the current time. A far preferable pathway would be to focus on compulsory reporting of such incidents and incentivise ways to improve cyber security across the economy and society. We elaborate on this below.

2.i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

A strict prohibition would introduce several risks and unintended consequences.

Some victims and companies, particularly SMEs, may suffer attacks that have devastating human, economic, and social consequences that could mean they have little choice but to pay a ransom. Prohibiting payment of

[1] See https://www.japaneselawtranslation.go.jp/en/laws/view/2760 for the translation. (Last accessed 10 April 2023)

[2] See https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ for the translation (Last accessed 10 April 2023)

ransoms and extortion demands by larger corporations only risks displacing targeting to SMEs and those not captured under such a regime. This could foreseeably result in more ransomware / extortion campaigns overall.

A further risk in prohibiting such payments is that some victims / companies may be forced to decide whether to face the devasting consequences associated with cyber-attacks and the potential consequences of breaching such provisions prohibiting a payment to cyber-criminals. It is impossible to assess the likelihood of this occurring in the absence of the detail on any proposed prohibition, including the potential penalties for not complying. However, in our view, we could foresee at least some scenarios where victims may still elect to pay a ransom and/or extortion demand despite such provisions. Some criminal actors may also test this very scenario, making them potentially more ruthless in their endeavours at least in the short- to medium-term. This could risk pushing more of the problem underground.

Prohibiting payments of ransom and extortion demands by insurers has more merit. In general, cyber insurance represents a much smaller component of targets of ransomware and extortion campaigns. We also know that many sophisticated cyber-criminals target those entities with cyber insurance, resulting in much higher demands in terms of ransom requests. Entities with cyber insurance tend to have more resources available to pay a ransom should they feel compelled to do so. It is also possible that overall ransom and extortion demands would decrease should this intervention be implemented.

However, implementing such a prohibition may not be as practicable as first thought. Many cyber insurers – and indeed targets of ransom and/or extortion attacks – are multinational corporations. As such, questions of jurisdiction emerge. It serves little benefit should cyber insurers be able to facilitate a payment by doing so via another jurisdiction where such a prohibition is not in effect. This same issue of jurisdiction applies to multinational corporations – many of which are among the more prominent victims of ransomware campaigns. Careful consideration needs to be placed on whether any attempt to introduce a more restrictive legislative regime in Australia could risk multinational corporations migrating to other countries with more favourable legislative systems in place.

Overall, we suggest a consistent approach be adopted among as many nation-states as possible. This could be facilitated via the G8 / G20 and/or the International Counter Ransomware Task Force. It is worth emphasising, however, that should wealthy states be successful in introducing such a system, and that system prove effective in deterring cyber-criminals from targeting such states, it is unlikely that cyber-criminal groups would cease their campaigns altogether. A considerable risk is that such groups will shift their attention to others without such regimes in place. Therefore, a regional approach to potential legislative reform should be considered. Finally, any amendments should be carefully monitored for displacement effects and unintended consequences.

2.g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

The Australian Government should clarify its position with respect to payment or non-payment of ransoms by companies. Our understanding currently is that in the vast majority of cases payment of a ransom or extortion demand does not constitute a breach of Australian law. While official advice has consistently been to not pay any demand to cyber-criminal groups for several reasons – e.g., that it is no guarantee that access will be restored or that data be destroyed, that it may lead to further extortion, and that it risks encouraging further attacks – these decisions are left with victims. In our view, more information could be provided to victims by government to inform these decisions, which would be facilitated by a compulsory reporting regime. For example, case studies using de-identified data would be invaluable to provide further evidence to entities experiencing ransomware and extortion campaigns.

It is worth considering whether the Australian Government would benefit from additional tools such as those available to the United States (US). For example, in 2019, the US Treasury's Office of Foreign Assets Control (OFAC) intervened against a Russian group known as Evil Corp, placing it on the sanctioned list. One of the explicit goals of this sanctioning was to disrupt Evil Corp's business model by making it a strict liability offence for any person or entity subject to a US jurisdiction to facilitate any form of payment to Evil Corp. It is our understanding that cyber insurers currently undertake rigorous analysis in an effort to ensure they do not

facilitate payment of a ransom or extortion demand to an OFAC sanctioned group. However, it is always possible for cyber-criminal groups to evolve their tactics and rebrand in an effort to get around sanctioned lists.

Nonetheless, a similar approach could be explored in Australia, whereby the Australian Government considers introducing sanctions on select cyber-criminal entities. A targeting approach to prohibiting ransom and extortion payments may prove more practicable and successful than a strict, broad-based approach. The effectiveness of OFAC sanctions should be properly evaluated before considering such an intervention and appropriate monitoring should be put in place to evaluate the ongoing effectiveness of this regime.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Australia could do much more to build cyber resilience and response capability in the region. This is critical should Australia seek to make our environment more hostile for cyber-criminals to operate, including by prohibiting payments of ransom and extortion demands as well as by disrupting cyber-criminal groups via offensive operations, due to risks of displacing this problem to neighbouring countries. Any attempt for Australia to disrupt cyber-criminal groups targeting Australia could be extended to select countries in the region (we elaborate upon this in the subsequent section).

Australia should continue supporting developing countries in the Indo-Pacific region to build cyber capacity and cyber security awareness. While countries in the region might all recognise the importance of building cyber resilience, not all counties have the capacity and resources to do this. This is especially the case in developing countries that might not perceive cyber security as a top priority in the development of the country. Designated aid support and resources will allow those countries to enhance their cyber resilience.

For an aid program like this to be successful, it is crucial that the Australian government carefully select partners that have at least minimal cyber capability and with whom we share an understanding of the local context, culture, and customs. A one-size-fits-all approach is not viable. It is conceivable that some countries, such as the micro-states, will never have the capacity to detect, prevent or recover from a cyberattack. Australia should consider entering into agreements with these states to allow Australian capabilities to be deployed when needed.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

There is significant scope for Australia to work with international partners to elevate cybersecurity partnerships, both multilaterally and bilaterally. Just as multilateral and bilateral partnerships were formed over the course of the previous century to address security threats across traditional domains of conflict (i.e., air, sea, land), we argue that similar cybersecurity arrangements should be developed now to address current and emerging cyber threats, including those posed by state actors, state-affiliated/tolerated criminal actors, and purely non-state criminal actors.

The recently formed International Counter Ransomware Taskforce provides a notable example and possible future template for how new multilateral frameworks can be used to tackle cyber threats to Australia in concert with friendly, cyber-capable states. We believe that this taskforce should also monitor emerging cybercrime trends and potentially broaden its scope of operations to address new cyber threats as and when they emerge.

In our view, Australia should also use its cyber-expertise to help protect more vulnerable states, particularly those in our region (see 3 above). Australia's use of offensive cyber capabilities to target foreign threat actors carries the risk of displacement, meaning that cybercriminals will likely be deterred from attacking Australia and instead will target more vulnerable states.

We further recommend that the joint ASD-AFP taskforce should consider broadening its remit to engage in offensive operations on behalf of select regional states, creating a regional 'cyber umbrella' that can be used to help deter cybercriminals from targeting vulnerable regional partners. Such an arrangement would not only help protect friendly states from cyber-attacks and mitigate against the displacement of cyber-attacks from Australia to more vulnerable states but would also boost Australia's diplomatic standing in the region. The

ASEAN Regional Forum and the Pacific Islands Forum (perhaps an expansion of the remit in the Biketawa Declaration) provide potential multilateral frameworks that could be used to raise such an idea amongst regional partners.

With regards to internet governance, we believe it is essential for Australia to continue playing a role in international organisations including the Internet Governance Forum (IGF) and the Asia Pacific Internet Governance Forum (APrIGF), as well as Forum of Incident Response and Security Teams (FIRST) and the Asia Pacific Emergency Response Team (APCERT).

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

Acknowledging that a new UN convention on cybercrime is under negotiation, Australia should continue to play a leading role advocating for broader ratification of the Budapest Convention on Cybercrime. The Budapest Convention is currently the most well-developed international treaty regarding state responses to cybercrime.

The Australian government should actively engage in discussion for a new UN convention on cybercrime, putting fundamentals rights upfront and making sure the new convention is aligned with Australia's goal to build an open, free and secure internet.

In the meantime, we recommend that Australia take the lead in harmonising laws and regulations, as well as capacities, in facilitating cybercrime investigation, especially in the Indo-Pacific region. A way to start this might be Australian government funding research to map, review and develop cyber capacity in the region, including regularly mapping laws of the Indo-Pacific countries against the Budapest Convention and provide recommendations.

7. What can government do to improve information sharing with industry on cyber threats?

The Security of Critical Infrastructure Act 2018 establishes a good set of guidelines for computer incident reporting. However, there might still be concerns with reporting, including whether a reported case will be made public or not. It is crucial that the Department of Home Affairs make it clear to critical infrastructure entities how reporting data will be used and how to protect the any incident from being publicised unnecessarily.

Currently, the Australian Cyber Security Centre (ACSC) is the designated organisation to receive incident reports and a report will be shared with the Department of Home Affairs only with the reporting organisation's consent. However, given that the ACSC is a government organisation, there may still be concerns from reporting entities that their data might be shared with industry regulatory authorities. A clear guideline on how the data will be shared and an explicit obligation of confidentiality upon the Australian Signals Directorate and ACSC should be enforced to encourage incident reporting (in response to Question 8).

We suggest the ACSC continue build trust with critical infrastructure entities. It can be done by designating the ACSC as the organisation responsible to not only to receive reports but also to provide necessary support to reporting entities to tackle incidents. Also, regular surveys on concerns and issues in incident reporting should be conducted with regulated entities to understand any difficulties or obstacles to reporting and to enhance reporting by eliminating concerns that entities might have.

9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

In our view the existing regime for notification of cyber security incidents should be expanded to include mandatory reporting of all breaches as well as ransomware and extortion demands for all victims (including SMEs). Of course, should a system for prohibiting payments of ransom and extortion demands be introduced, an accompanying mandatory reporting regime would be essential. However, even in the absence of legal approaches to strictly prohibit such payments, a mandatory reporting regime has considerable public good benefits for improving situational awareness of cybercrime incidents.

Mandatory reporting should work alongside other initiatives to promote a more mature and resilient cyber security culture. A key component of such a culture is to avoid victim blaming and shaming – one of the key reasons underpinning a reluctance to report among many corporations. While victim shaming may serve to make executives and boardrooms take cyber security more seriously, it equally makes victims of cyber security incidents more reluctant to report. We are also a long way, in our view, from having a more sophisticated understanding of cyber security among the general public insofar as understanding when victims have taken reasonable precautions but still suffered a breach (which will happen) and when insufficient investment in cyber security protocols was the likely cause of such incidents in the first place.

It is possible for research to inform the potential impacts of a mandatory reporting regime on improving the understanding of cyber security incidents. For example, existing reports could be cross-referenced with known cyber security breaches as reported via extortion websites of cyber-criminal groups. Initial access sales, which typically do not mention entity names but do mention countries, could also be monitored and compared with both extortion sites (to gather a potential overall understanding of the true size of cybercrime incidents – many of which may be undetected by victims) and existing reports to gather a more holistic picture of the potential gap between actual incidents and reported incidents.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

As a multi-cultural nation, we have a significant number of migrants who are not native English speakers or English users. These groups are often targeted by special types of cybercrime (e.g., online and telecommunication fraud such as virtual kidnapping) and might be particularly vulnerable to dis/misinformation campaigns that are launched using their native language.

We strongly suggest that the design of awareness-raising programs should take into account different cultures and languages. While we now see advertisements using different languages to enhance public awareness, these need to be not just translated but designed to better fit different cultural contexts. Also, it is important to select different platforms, such as Line, Facebook and WhatsApp, to properly disseminate government messages so that people from different background can receive the message more easily.

For example, to prevent students from falling into virtual kidnapping scams, government messaging needs to be tailored to international student groups and conveyed in a medium that they use. Governments might consider working with NGOs or organisations that have connections with international students or with people with knowledge of the relevant culture and language to design an effective communication strategy.

15.a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

The Australian Government could facilitate procurement of cyber security technologies to maximise value for money across all public sector entities in Australia. In addition, as stated above, this procurement could be coordinated to support small and medium sized business with affordable cyber security technologies and the adoption of standards commensurate with their overall level of risk. These technologies and standards could be rolled out over a set timeframe, with explicit increases in maturity each year.

What is most important is that Australia has access to the most effective and affordable security systems. While efforts should be made to support and encourage the Australian cyber security ecosystem, including supporting start-ups and existing businesses to thrive, measures to privilege Australia firms in procurement decisions will compromise these objectives. Government procurement can be used to set minimum standards that can be

adopted by large corporates and cyber security firms. The Australian Government should also support Australian firms in producing better security systems and products.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

The Australian Government could facilitate procurement of cyber security technologies to maximise value for money across all public sector entities in Australia. In addition, as stated above, this procurement could be coordinated to support small and medium sized business with affordable cyber security technologies and the adoption of standards commensurate with their overall level of risk. These technologies and standards could be rolled out over a set timeframe, with explicit increases in maturity each year.

What is most important is that Australia has access to the most effective and affordable security systems. While efforts should be made to support and encourage the Australian cyber security ecosystem, including supporting start-ups and existing businesses to thrive, measures to privilege Australia firms in procurement decisions will compromise these objectives. Government procurement can be used to set minimum standards that can be adopted by large corporates and cyber security firms.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

In our view, ongoing evaluation measures are critical to assess the effectiveness of the Strategy. While the general numbers of cyber security reports are currently disclosed, this does not necessarily improve the overall picture of cyber security incidents.

There is currently no reporting of how many incidents are resolved in some way. Careful consideration should be directed toward reporting the number of cyber incidents resolved by police nationally, and in each jurisdiction. There are risks associated with publicly disclosing these data, particularly if they reveal very low rates of resolution (as is likely to currently be the case), which could energise cyber-criminal groups and undermine trust in public institutions. On the other hand, however, disclosing these data could encourage greater investment in responding to cyber incidents. Importantly, by resolution, we do not mean arrest and prosecution – these would also extend to some form of disruption.