ACDA Response to the Australian Cyber Security Strategy Discussion Paper

15th April 2023

Active Cyber Defence Alliance

Overview

Cyber-attacks are doing untold harm at all levels of the Australian society and economy.

Cyber threat actors who perpetrate these attacks act without regard for sovereign boundaries, and cause harm to individuals, organisations, enterprises, and governments without any regard for ethical, moral, or legal considerations. Some of this harm has been mitigated, but not totally avoided, by each Australian entity spending significant amounts on often piecemeal passive-protection, patchy detection of and limited response to cyber-attacks, often following compliance-led prescriptions. Demonstrably and undeniably, existing and potential Australian cyber victims need different approaches. Victims, and potential victims, can also be unclear as to the scope of actions they can perform in defence of their digital property, due to outdated and sometimes conflicting legislation.

The Active Cyber Defence Alliance Inc (ACDA) is a focused think tank committed to lifting Australia's cyber resilience through greater awareness, capability, and adoption in active cyber defence. We draw together leading cyber professionals from government, industry (both supply and demand side) along with academic, legal and regulatory stakeholders – so this submission is based on lived experience.

The ACDA believes there is an urgent need for an Australian Cyber Security Strategy (CSS) to lead and sustain a cohesive legislative and regulatory regime so that governments, industry, and individuals can collectively and individually reduce risk through the clarification of the scope of lawful actions that can be performed by an Australian entity in the defence of their digital property. We believe that a large part of the gap can be addressed by:

- Clarifying the application of law in the cyber realm, proposing safe guardrails for lawful practice and collaboration with law enforcement and national security to shape, deter and respond to cyber-attacks.
- Encouraging potential victims to look beyond compliance-based security and consider methods that provide practical and lawful deterrence and raise cyber criminal's cost and risk.

While cyber criminals are not limited by boundaries, our response is. Our current legal and regulatory frameworks – few of which envisaged the current global information environment – leave well-meaning enterprises and agencies loath to act due to uncertainty about:

- their direct liabilities from such action,
- breaches of privacy, including those of the criminals,
- the lawfulness of their metadata collection in the process of detecting a crime,
- whether they will be exposed to charges of criminal behaviour, or
- the possibility that they could be sued for causing harm inadvertently.

This requires clarification of criminality about engaging with attackers, new models of trust to optimise re-use of capabilities via shared national and regional frameworks and promulgation of resilient, cyber-secure behaviours against increased threat actor capabilities.

To that end ACDA has already initiated two working groups:

- The **ACDA Lawful Countermeasures Working Group** will research how cyber is already or needs to be incorporated into Australia's current legislation and regulatory environment. *This body of research addresses 8 of the questions raised for discussion.*
- **The ACDA Frameworks Working Group** will work with Australian and international cyber frameworks including MITRE to add cyber threat actor behavioural attributes and patterns that are Key Risk Indicators of pending attacks and support active defence. *This work addresses 10 of the questions raised for discussion.*

Only when the cost of attacking Australian and regional data, infrastructure and services is greater than the reward, will the cyber security challenge we face today – and every day – be met, making Australia the most cyber secure nation in the world by 2030.

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?

Large, mature organisations in the private sector should be empowered to use the resources and capabilities that they already have, in order to protect themselves and their information eco-systems against cyber-attacks, including by using Active Cyber Defence.

"Private sector entities operate today on the front lines of cyber conflict, targeted by a variety of hostile actors that seek to steal and misappropriate their intellectual property, degrade their infrastructure, and disrupt their business activities. Despite this reality, the options available within the private sector for responding to cyber threats are outdated and constrained. The status quo is reactive in nature and advantages the attacker". [1]

These organisations need legal certainty on what responses are lawful. Currently, the risks attached to taking action where there is no legal certainty results in a failure to act and leaves Australia vulnerable.

The strategy should:

- Lead the evolution of the Australian legal and regulatory environment to recognise cyber within current legislation before creating new laws.
- consider adopting industry accepted language described by thought leaders, such as the MITRE Corporation, which advocate options that extend a controls-based defence to include deterrence strategies provided through adversary engagement.

This Strategy update provides the opportunity to expand the range of Australia's lawful cyber defence activities to change the balance of power in the cyber realm in favour of the defender thus reversing the current asymmetric advantage of the attacker which is creating so much loss, risk and harm for legitimate organisations.

Significant progress towards this recognition can be accomplished by adopting the approaches proposed in the charter of the Active Cyber Defence Alliance

[1] George Washington University Center for Cyber and Homeland security, "Into the Gray Zone," (2016) https://cchs.gwu.edu/gray-zone-active-defense-private-sector-against-cyber-threats.

Inc[2] and being incorporated into the MITRE frameworks MITRE ATT&CK, ENGAGE, & Caldera[3].

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

Australia already has substantive regulatory reform underway (surveillance, privacy, critical infrastructure and more) and **before new laws are promulgated**, the existing laws should be reviewed for application to the cyber realm.

The review should ideally be funded by government and take the form of a body of research with the specific purpose of researching the application of Australian national law to cyberspace.

A similar review was undertaken in Estonia and produced the Tallinn Manuals 1 and 2 (international law which applies in cyberspace and to cyber operations).

This research is already being planned by the ACDA Lawful Countermeasures Group - A working group to explore and clarify the application of law in the cyber realm, proposing safe guardrails for lawful practice and collaboration with law enforcement and national security. The working group recognises the need for wide consultation and the significant effort involved.

As the research is completed, amendments to current laws and regulatory codes can be proposed. This approach is pragmatic and will result in much faster and more effective enhancement of cyber resilience across the digital economy with lower barriers to adoption.

Why is this research critical?

For example, the legal defences under the *Criminal Code Act 1995* (Cth) (Division 10 - Circumstances involving external factors) to the offence of damage and harm caused, as a result of action taken in response to:

- Self-Defence;
- Intervening conduct or event;

[2] https://acda.group
[3] https://mitre.com

- Sudden or extraordinary emergency; and
- Duress

have not yet specifically been recognised to apply in the cyber realm. To do so would empower (suitably qualified) organisations to better protect themselves and Australia more broadly.

This right has not yet specifically been recognised to apply to cyberspace.

The ACDA working group will analyse potential cyber countermeasure scenarios and seek to answer the question:

What freedom do we have to act and what are the consequences when we don't act?

The working group will:

- Identify a set of typical scenarios that occur in cyber incidents from theft of personal private information, intellectual property through to threats to human safety and operational reliability of critical infrastructure and services.
- Map out guidelines for lawful countermeasures in Cyber Defence for each scenario by answering the questions.
  - What actions are available?
  - Risks if we act
  - Risks if we don't act
- Consider the context of Australian State and Federal law but potentially also selected regional and other international jurisdictions.

This is how it works:

In Australia self-defence is provided for in section 10.4 of the *Criminal Code Act 1995* (Cth)[4] as follows:

> *(1) A person is not criminally responsible for an offence if he or she carries out the conduct constituting the offence in self-defence.*

[4] The Criminal Code Schedule. General principles of criminal responsibility. Chapter 2. Circumstances in which there is no criminal responsibility. Part 2.3. Circumstances involving external factors Division 10. Only relevant provisions are quoted.

(2) A person carries out conduct in self-defence if and only if he or she believes the conduct is necessary:

(a) to defend himself or herself or another person; or

(b) to prevent or terminate the unlawful imprisonment of himself or herself or another person; or

(c) to protect property from unlawful appropriation, destruction, damage or interference; or

(d) to prevent criminal trespass to any land or premises; or

(e) to remove from any land or premises a person who is committing criminal trespass; and, the conduct is a reasonable response in the circumstances as he or she perceives them. [5]

Given that "Property" is defined in section 4 of the Criminal Code to include real property, personal property, money, and other intangible property, and "Person" includes a body corporate, the only re-interpretation required is in relation to (2)(e): *" to remove …"*

References to "*criminal trespass to any land or premises"* have already been re-interpreted to mean unauthorised access to computers and networks[6] (criminal trespass).

So, the question to be answered is what does "*to remove* …" from computers and networks a person who is committing criminal trespass mean? Physical and fault elements should be examined, and a determination made as to damage and proportionality.

The government (legislative, executive, and judicial branches) can then move quickly to resolve questions such as this.

The ACDA sees this as a typical example of the outcome of the Lawful Countermeasures working group and is actively seeking public and private funding.

[5] This section does not apply if the person uses force that involves the intentional infliction of death or really serious injury to achieve (c), (d) or (e), or if the person is responding to lawful conduct knowing that the conduct was lawful. Other countries have similar provisions e.g. Singapore, New Zealand, Hong Kong, India.

[6] *Criminal Code Act 1995* (Cth). Part 10.7 – Computer Offences.

2a. 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)?

Australia has thousands of laws, regulations and guidance. We need to properly understand and use what we have. Enforceability is what is lacking.

Mandating controls-based cyber security standards such as the global ISO:27000 series, the Australian Government's Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) operational security standards will never be adequate to secure the information in complex current, legacy and evolving information handling environments. Enforcement at this level alone will not be enough.

Similarly, mandatory adoption of cyber security constructs from global information ecosystems, such as Google, Apple or Microsoft that are not informed by local Australian legislative and regulatory environments equally fall short of being effective or appropriate.

Leadership by Commonwealth and State jurisdictions in assessing and recognising third party cyber risk and cyber risk in the supply chain, and costing these risks as liabilities during procurement, operation and sustainment can enforce improvements in operational cyber security standards for all parties providing products and services to government and industry (also addresses Q 18).

This is how it worked:

The high cyber risk from certain brands of telecommunication equipment being used in Australia's telecommunications networks was assessed by State and Commonwealth CISOs as a greater liability than the total costs that would be saved, effectively mandating telecommunications networks comply with the relevant / applicable cyber security standards.

Government procurement of networks that only use low cyber risk (cyber - compliant) equipment leads to multiple beneficial outcomes across the economy such as operational and service staff being trained in cyber compliance to maintain the networks.

2b. 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?

This is not necessary if purposive electronic interpretation is applied, and existing law is researched for application to cyberspace.

2c. Should the obligations of company directors specifically address cyber security risks and consequences?

The current requirements under the *Corporations Act 2001* (Cth) already render directors liable for cyber security - irrespective of whether the Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234[7] (Information Security) applies or not. Further work in this regard should fall under the research outlined above. Substantial penalties already exist, for example:

A director who fails to perform their duties, may:

- Have contravened a civil penalty provision such as the care and diligence requirements under section 181(1) of the Corporations Act (see section 1317E). The court may order the director to pay to the Commonwealth up to $200,000).
- Be personally liable to compensate the company or others for any loss or damage they suffer.
- Be prohibited from managing a company.

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

A separate Cyber Security Act would seem to ignore that cyber is – and has been for many years now – inherent in most economic and civil interactions.

[7] https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.

Whether any additional legislation is required can be decided based on the outcome of the research identified above.

2e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

Undertake the research described above.

Some 80 percent of the apparent complexity will be resolved through analysis and rationalisation even with respect to the Commonwealth – State and Territory Regulatory Universes. (This statement is founded on work already undertaken by ACDA members).

This is how it could work:

In the review of the Universal Service Obligation (USO) embedded in the Telecommunications (Consumer Protection and Service Standards) Act (1999)[8]

During 2021-22, Telstra introduced its "Cleaner Pipes" initiative. This halted many millions of calls and texts – two vectors used to perpetrate cyber-attacks across the Telstra network. By including cyber within the definitions of the legislation, the government could include "Cleaner Pipes" as part of a USO to ensure all Australian telecommunications networks provided the service or adopted Telstra's under a commercial arrangement.

This would recognise Telstra's investment in capability and leadership of Telstra staff including Jennifer Stockwell – now advisor to the Hon. Clare O'Neil, Minister for Cyber Security.

[8] https://www.legislation.gov.au/Series/C2004A00441

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

This question highlights the complex interaction between the need to minimise harm from cyber-attack with national and international laws that aim to limit criminal activity.

The ACDA believes that payment of ransoms should be unlawful in all circumstances, however there should be an exception/legal defence for exigent circumstances such as life, public safety etc.

This is how it might work:

In the research and review of legislation, the ACDA Working Group would take into consideration the complex interaction with prohibition scenarios.

On one hand, in an opinion piece titled "Making cyber ransom payments unlawful would help boards" AFR, 21 November 2022, the author stated:

"Cyber criminals' aggression and sophistication, community expectations – and now, dramatically increased Privacy Act penalties – create a daunting and complex environment for company leaders, their stakeholders and for government. [9]

The need for mindful action was identified by the Hon. Clare O'Neil, Minister for Cyber Security, who was quoted in the SMH, 27 February 2023 about paying ransoms as saying:

"What I do know is that we can't continue as we are today."[10],.

As an example of the level of complexity, payment of ransom – almost always in cryptocurrency such as BitCoin – may or may not resolve a ransomware

[9] https://www.afr.com/technology/making-cyber-ransom-payments-unlawful-would-help-boards-20221120-p5bzp7

[10] https://www.smh.com.au/technology/australia-is-not-a-soft-target-cyber-ransom-payments-in-firing-line-20230227-p5cnxr.html

attack but may also impact a reporting organisation's own AML/CTF program risk.

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

Yes – through the research identified above.

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

Cyber criminals are not limited by sovereign National boundaries or international treaties.

Only consistent cyber security frameworks able to be adopted end to end of cross-border (international) data flows will build effective cyber resilience. ACDA has initiated a working group to address this issue.

The aim of the ACDA Framework working group is to augment the MITRE Engage framework and potentially create an integrated framework encompassing MITRE ATT&CK, Engage and Caldera.

The working group will identify what changes are required in frameworks such as the NIST CSF and Australia's ISM to enable a tactical shift from passive to active defence. It would also seek to embed threat intelligence and tactics based on the MITRE frameworks into the controls design and capabilities of each organisation mature enough to use this best practice taxonomy. This brings behavioural analysis into cyber, opening up opportunities to employ people with these skills and honouring the contribution that neuro-diverse staff can make.

Government participation in this ACDA Frameworks working group will contribute to redefining security standards to explicitly incorporate active defence/adversary engagement techniques. Government involvement will bring invaluable perspectives to this process and signal to industry and the

community at large the value of these acceptable and necessary techniques and approaches.

Basing these matters within a globally accepted framework (MITRE) allows inclusion of our neighbours, builds our regional cyber resilience and better respond to cyber incidents.

Behavioural predictors are slower to change than technologies, tactics and techniques – which apparently can even be obtained from Chat GPT!

This also addresses Q15, Q16, Q17, and Q19 as MITRE, NIST and ISM frameworks continue to evolve.

Funding is required for this activity and could be included in the Australian CSS.

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

Both ACDA working groups will take regional and key international aspects into consideration including FVEYS national contributing partners through collaboration with and involvement of Defence.

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?

The ACDA Framework working group addresses this specifically.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

Cyber security is a national security issue, not a standalone cyber domain issue.

The lived experience of many government and enterprise cyber practitioners informs us that cyber incidents cause harm with impacts including identity, access to entitlements and reputational damage.

We need to respond as a nation through uniform cybersecurity laws (Refer to 2 above) and rely upon the Legislative Powers of Parliament under section 51 of the Australian Constitution.

The ACDA working groups will collect evidence and supply working models that shift the “cyber” issue from a tech-heavy issue that has “investment” thrown at it, back to a risk-based set of good enough cyber behaviours that are supported by a cyber informed legislative and regulatory environment.

This is how it worked:

A significant data breach of customer identity records of a major telecommunications retailer was detected by calls to government agencies requesting re-issuing of identity credentials. The agency collaborated with the retailer’s incident response team and provided a notification script that was distributed to victims to fast track the re-issue of their government credentials.

The lead government agency will now be notified for all future significant breaches of their identity credentials by all the Telco and its retailers.

In this case, harm minimisation was achieved by appropriate, nuanced information sharing and collaborative behaviours.

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

As well as the above example, partner with and support the ACDA working groups, which in turn will partner with government and industry to deliver pragmatic, usable outcomes.

The ACDA supports the concept of ISAC – and specifically the CI-ISAC as a trusted third party (NFP).

Taking an Active Cyber Defence approach including deception networks creates the opportunity to share adversary Tactics, Techniques and Procedures (TTP) from the deception network rather than from the "Production" network allows the enterprise to share observed attacker TTP directly without compromising details of its own secure ICT configurations.

Much work has been completed on intelligence sharing protocols, however, both legislative clarity and active defence capabilities are required to create the trust for incident information to be shared. Hence the ACDA initiation of the working groups outlined above.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

No. That level of trust does not yet exist. See Q7 above.

The ACDA Framework working group address this in extending current best practice.

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 the context of cyber, asking for a ransom/extortion is an offence because it involves unauthorised access to a computer/computer system and is punishable by imprisonment of 5 years. Paying a ransom/extortion fee which creates a market for criminality should likewise be a criminal offence. The ACDA Lawful Countermeasures working group addresses this. See 2 f. above.

10. What best practice models are available for automated threat-blocking at scale?

Telstra and its international partners already implement this.

The ACDA Framework working group addresses this in extending current best practice.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Recognition that a broader range of disciplines including behavioural observation and analysis are inherently part of cyber will result in increased intelligence analysts and hence more usable cyber intelligence.

The ACDA Framework working group addresses this.

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

Both ACDA working groups will identify opportunities.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

The ACDA Lawful Countermeasures working group addresses this. See 2 f. above.

13a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The ACDA Lawful Countermeasures working group addresses this. See 2 f. above.

14. What would an effective post-incident review and consequence management model with industry involve?

The ACDA Framework working group addresses this.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Clarification of laws and regulations as they apply to cyber is a key pre-requisite for each party to understand their accountabilities and responsibilities (as per 2 above)

Until this is done, additional guidance will have low credibility.

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

Clarification of laws and regulations as they apply to cyber is a key pre-requisite for each party to understand their accountabilities and responsibilities (as per 2 above)

Until this is done, additional guidance will have low credibility.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

For government to support the evolution, application and adoption of active cyber defence – engaging with attackers before harm is caused. The ACDA sees this as part of our purpose and a major beneficial outcome from our work.

As a volunteer organisation, we are currently constrained in our resources and are actively attracting private and public funding.

17. How should we approach future proofing for cyber security technologies out to 2030?

Ongoing evolution of Frameworks and promulgation of experience and best practice is addressed by the ACDA Framework working group.

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?

This is addressed at Q2 (a) with an example. When Government applies its own mandatory standards in its procurement, this creates a positive feedback loop and a viable path to market for Australian Cyber Security firms.

This requires the body of research proposed as outcome from the ACDA Lawful Countermeasures working group.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

Focus on cyber secure behaviours as these are transferrable and adversary behaviours as these tend to be consistent regardless of technology.

Ongoing evolution of Frameworks and promulgation of experience and best practice is addressed by the ACDA Framework working group.

20. How should government measure its impact in uplifting national cyber resilience?

Currently cyber-crime is the third largest economic movement of value globally. Maintaining or reducing how much Australia and Australians contribute to this is a high-level measure, however metrics to track progress at even an industry level are missing or immature.

The ACDA Framework working group – by adding best practice cyber behaviours to recognised and accepted frameworks such as MITRE, will encourage resilience by adoption of (often simple) behaviours.

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

The ACDA working groups plan to consult widely. If performed as a part of the CSS, this consultation demonstrates transparency, gains recognition for and credibility of the CSS.

The key evaluation measure needs to be one of involvement – similar to the approach being taken by the ACSC.