Active Cyber Defence Alliance

Cyber Security Legislative Package 2024

Submission to the Parliamentary Joint Committee on Intelligence and Security

Authors

Brendan Walker-Munro
Andrew Cox
Sascha Dov-Bachmann
Philipp Moore
Grant Haroway
Joe Otway
Michelle Price
Duncan Unwin

Disclaimer: The views expressed in this paper are those of the individual authors and the Active Cyber Defence Alliance, and may not represent the views of any other institution, agency or government despite the affiliations of the authors.

Introduction & Context

The Active Cyber Defence Alliance Inc (ACDA) is a dedicated Australian industry think tank with membership across sectors of the economy, including the legal fraternity, committed to advancing active cyber defence practices for bolstering Australia's cyber resilience. The ACDA welcomes the opportunity to make a submission to the public consultation on the proposed Review of the Cyber Security Legislative Package 2024 ("the Package"), comprising of the Cyber Security Bill 2024 (Cth), the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024, and the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024.

The civilian cyber defence landscape has largely concentrated, to date, on the passive defence of information systems (i.e., antivirus programs, scanning software, firewalls, etc.) while defence and law enforcement have been given a mandate to use cyber offence to disrupt those who would do harm to Australian systems or interests (i.e., by "hack backs", network disruption warrants, and similar). However, there is a significant space between these zones of passive defence and offence that the ACDA believes should be used by civilian organisations to monitor the actions of, and even engage with, these malicious actors to gather cyber threat intelligence that would help to repel the actions of these actors and build better defences. However, the legal framework in Australia does not protect civilians or civilian organisations adequately from potential prosecution or civil liability for trying to protect their information and intellectual property, or their privacy of their staff, contractors and customers.

In that space, we adopt the definition of 'active cyber defence' used by the US National Institute of Science and Technology (NIST) that describes any capability, tool or technique which offers '[s]ynchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities',[1] with a particular emphasis on the production of cyber threat intelligence. Active cyber defence thus incorporates activities such as use of tracers, teasers, honeypots and honey tokens (described further below) to actively – rather than passively – detect, expose and potentially disrupt a cyber-attacker during a cybersecurity incident. To be clear, we do not (and never will) accept that active cyber defence should involve activities by civilians designed to "hack back",[2] which remains the sole and proper domain of agencies operating under the imprimatur of Executive government and/or the supervision of the courts.

To see where the punches are coming from gives us the opportunity to duck and weave. A boxer with a blindfold on is bereft of half their arsenal and is confined to an unfair fight. The ACDA is committed to exploring the lawful use of active defence techniques that remove the blindfold from the boxer and provide a view of the malicious intent toward an organisation and respond to resist the threat.

[1] NIST Computer Security Resource Center, *Glossary* (online, 2024) <https://csrc.nist.gov/glossary/term/active_cyber_defense>.
[2] Brendan Walker-Munro, David Mount, Ruby Ioannou, "The Hacker Strikes Back: Examining the Lawfulness of "Offensive Cyber" under the Laws of Australia' (2022) 94 *Computers & Law* 5.

Summary

Cyber-attacks pose a serious threat to the security and integrity of corporate entities, especially when they involve insiders who have access to sensitive data and systems. By using active cyber defence techniques, organisations can increase their chances of preventing and identifying cyber-attacks, as well as collecting evidence for legal action. However, this submission also acknowledges that there are some challenges and risks associated with the use of active cyber defence in the context of the specific reforms proposed in the Cyber Security Legislative Package 2024.

Therefore, this submission examines three areas of the Legislative Package which pose specific risks with respect to the use of active cyber defence tools and techniques:

- The establishment of the Cyber Incident Review Board (CIRB), and the scope of matters under review (which should include whether the impacted entity had deployed or was deploying any forms of active cyber defence);
- The Minister's power to "approve" terms of reference for any CIRB review, which we consider an unnecessary and dangerous form of Ministerial control of an otherwise independent entity; and
- The limitation of the currently proposed "limited use" information provisions, which we argue does not provide clarity in cybersecurity practices and refer to the current legal dilemmas surrounding use of active cyber defence tools.

This submission addresses only these three areas of the Package; however, this should not be read as an endorsement or rejection of any of those other parts of the Package.

The Cyber Incident Review Board (CIRB)

One of the most significant changes in the Package is the introduction of the new Cyber Incident Review Board (CIRB). This CIRB would be made up of Ministerial appointees, assisted by a specific group of experts chosen from industry. Appointments to the Expert Panel would be made by the CIRB themselves without Ministerial involvement.

Of peculiar relevance to the ACDA is the proposed section 46(2)(a) of the Cyber Security Bill 2024, which limits the conduct of reviews by the CIRB to those where 'the Board is satisfied that the incident or series of incidents meets the criteria mentioned in subsection (3)'. Subsection (3) then lists a number of potential criteria for reviewable incidents, with section 46(3)(b) of the Cyber Security Bill 2024 permitting a review where 'the incident or series of incidents involved novel or complex methods or technologies, an understanding of which will significantly improve Australia's preparedness, resilience, or response to cyber security incidents of a similar nature'. The CIRB will also be permitted under section 62(1)(a)(ii) of the Cyber Security Bill 2024 to includes in its reports (which are publicly available) 'recommendations to government and industry about actions that could be taken to prevent, detect, respond to or minimise the impact of, incidents of a similar nature in the future', i.e., whether companies use active cyber defence tools or techniques or not.

Given the legal and regulatory minefield that currently comprises the field of active cyber defence in Australia, this section is of prime interest and importance to the ACDA and its members.

The relative novelty of active cyber defence in cybersecurity practice, and complexity of the legal landscape, provides a unique opportunity for the CIRB to contribute to a deeper and more nuanced understanding of active defence, with a view to informing Australian decision-makers on the provision of greater legal clarity to this domain. For example, the CIRB may be in a position – once it has been established and developed adequate standards of evidence arising from previous reviews – to observe differences in the first responses, detection likelihood, damage suffered, or risk mitigated by firms or corporations that employ active cyber defence techniques when compared to those that do not. That evidence base would be crucial in both Australian government legislation and policy settings, to examine whether Australian law could better support industry players in deploying deception or active defence tools into their network architecture.

The ACDA fully supports the implementation of the CIRB, and recommends no changes be made to its mandate, scope or powers (save for the issue of Ministerial intervention raised below). As part of the implementation of the CIRB, the ACDA looks forward to contributing to any additional discussion or consultation that occurs in determining the matters and recommendations which could form part of future reviews.

Ministerial Power over the CIRB

Another provision in the proposed Cyber Security Bill 2024 is of great concern to the ACDA; that is, the requirement that the CIRB may not undertake a review unless 'the Minister has approved the terms of reference for the review' (section 46(2)(c)). That provision cuts to the very heart of the CIRB, which is otherwise an independent body under section 63 of the Cyber Security Bill 2024: '[the Board] has complete discretion in the performance of the Board's functions and the exercise of the Board's powers'.

There are numerous reasons why this provision is an inappropriate inclusion in the Bill. The first is the obvious potential for adverse Ministerial intervention in the otherwise independent conduct of the CIRB's operations. It is neither impossible nor far-fetched to imagine a Minister – even one acting in good faith – holding up or delaying the conduct of a review that is required to be conducted expediently and efficiently. Even worse is the possibility of a Minister abusing this power to block or prevent a review being conducted into a particular incident or incidents, on the grounds of political or personal embarrassment or discomfort with potential findings.

Secondly, the Ministerial power over the approval of terms of reference will fetter the procedure of potential reviews by the CIRB. Hypothetically, the Minister might approve a Terms of Reference but only after certain grounds of inquiry or areas of review are deleted from the scope. Again, this may be motivated by the good faith execution of the Minister's office, but equally could be designed to avoid casting light on matters which the Minister (for whatever reason) deems politically expedient to shield. Further, as experts appointed from the Expert Panel must be appointed 'in accordance with the terms of reference for a review under section 46' (section 70(3) of the Cyber Security Bill 2024), the Minister will have an indirect capability to influence, ensure or block the appointment of certain experts to a review by either limiting or removing grounds from a given Terms of Reference.

Thirdly, Ministerial intervention in Australia has a wretched history. The decision by then-Prime Minister Scott Morrison to appoint himself to numerous Ministries to interfere with a petroleum permit decision was, whilst technically legal, largely viewed with scorn by the Australian public and described as '[inconsistent] with the convention of responsible government'.[3] Ministerial involvement in the award of sporting grants has resulted in a much-maligned system of "pork barrelling", where the award of grants is based not on merit but on political expediency and partisanship.[4] Indeed, former President of the Australian Human Rights Commission, Professor Gillian Triggs, wrote in 2017 that Ministerial interventions were fundamentally a 'distortion of democracy'.[5]

It is the ACDA's view that the provision requiring that the Minister "approve" Terms of Reference of an otherwise independent body is thoroughly inconsistent with the fundamental independence required of a body like the CIRB and recommends that subsection 46(2)(c) be removed from the Bill.

[3] Greg Carne, 'Improving the Future for Commonwealth Ministerial Responsibility and Responsible Government?: The Bell Inquiry and Beyond' (2024) 51(2) *University of Western Australia Law Review* 202-247.
[4] Yee-Fui Ng, 'Regulating the rorts: The legal governance of grants programs in Australia' (2023) 51(2) *Federal Law Review* 205-231.
[5] Gillian Triggs, 'Overreach of Executive and Ministerial Discretion: A Threat to Australian Democracy' (2017) 7 *Victoria University Law and Justice Journal* 9-14.

"Limited Use" Provisions and the Case of Active Cyber Defence

The provisions relating to the "limited use" of information provided to the National Cyber Security Coordinator (NCSC) have been the subject of a significant amount of public reporting. Relevantly, the ACDA notes that the provisions included in the Cyber Security Legislative Package do not amount to a "safe harbour", i.e., a complete blanket of immunity for entities that disclose information that might expose them to a penalty. The Government has made clear in the Explanatory Memorandum the difference between "limited use" and "safe harbour", such that entities that supply information to the NCSC may still incur potential legal liability for their conduct.[6]

As an opening point, the ACDA fully supports the "limited use" approach endorsed by government and does not seek to advocate for a safe harbour regime in Australian law. Individuals, directors, and boards of companies must be held accountable if their conduct is sufficiently malicious or negligent to warrant criminal prosecution – that option should never be taken away from the relevant regulatory bodies, and ought to encourage a stronger standard of diligence around cybersecurity protections in medium- and large-scale companies.

However, the debate around "limited use" and "safe harbour" surfaces – in the context of active cyber defence – several interconnected issues with the legality of using active cyber defence tools. In that context, active cyber defence involves the use of the following (non-exhaustive) list of techniques:

- Teasers: Falsified files and user credentials which appear genuine to an external actor but alert the Incident Response team when accessed (as the files and credentials themselves are falsified, there is no genuine need for those files to be accessed).
- Tracers: Cookies or similar programs attached to genuine trading information, which periodically transmit their network transmission and movement information back to the Incident Response team.
- Honey Pot: A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. A system or collection of systems created to look like a real system, which is configured to alert when an attempt is made to access it. Typically, these are deployed within the boundaries of an organisations.
- Honey Tokens: A subset of honeypots, such as a document, database credentials or other secrets made attractive to attackers, but when accessed or downloaded to an external system or device will activate an alert or execute code to transmit its IP address, physical location and/or other data from the browser context allowing that system or device, location, or user to be identified.

[6] Explanatory Memorandum to the Cyber Security Bill 2024, at 7, 54, 68 and Attachment B.

Each of these technologies and techniques is currently being tested, developed and even deployed in networks by Australian companies to better protect their internal networks from hackers and unauthorised intruders. However, the legal framework for criminal liability for computer-based offences in this country does not adequately protect the "good faith" conduct of active cyber defence, and risks criminalising the conduct of good practice cybersecurity. There are three discrete but overlapping challenges from the criminal law perspective:

- Computer offences in the *Criminal Code* (Cth) could apply: the use of teasers, tracers, honey pots and honey tokens could all ground liability for a computer offence in Part 10.7 of the Code. This is because the mere use of these technologies could result in 'unauthorised modification of data'[7] (even if that data belongs to a hacker or cyber-attacker), 'unauthorised impairment in their electronic communication'[8] (if it blocks the attackers access to the network), in any other way 'accesses, modifies, or impairs the reliability, security, or operation of data'.[9]
- State laws could also apply: the patchwork of State and Territory criminal offences could also be charged as 'State offences with a Federal aspect',[10] given that telecommunications is the *domaine reserve* of the Commonwealth (*Australian Constitution*, s 51(v)). Thus, where the relevant State nexus has been met, a company using active cyber defence to access the computer of a cyber-attacker could be prosecuted under Northern Territory law for 'unlawful access to data'[11] or ACT law for 'unauthorised modification of data to cause impairment'.[12]
- The lack of the protection of self-defence: Under the *Criminal Code* (Cth), a person is not criminally responsible for any act constituting self-defence.[13] However, the provisions of what constitutes self-defence are difficult to apply in the digital world, where computer data is not considered "property" and the notion of "criminal trespass" does not extend to digital networks.[14]

Other than these offences from the *Criminal Code* (Cth), there are other ancillary provisions which may be triggered using active cyber defence. The revelation of the "in-real-life" identity of a cyber attacker may breach the *Privacy Act 1988* (Cth)[15] or State-based human rights legislation.[16] The use of

[7] *Criminal Code* (Cth), s 477.2(1).
[8] Ibid, s 477.3(1).
[9] Ibid, s 478.2.
[10] *Crimes Act 1914* (Cth), s 3AA.
[11] *Criminal Code 1983* (NT), Sch 1, s 276B.
[12] *Criminal Code 2002* (ACT), s 416.
[13] *Criminal Code* (Cth), s 10.4(1).
[14] For example, in *Director of Public Prosecutions v Murdoch* [1993] 1 VR 406, the respondent was charged with a specific "computer trespass" provision under the now-repealed section 9A of the *Summary Offences Act 1966* (Vic). In applying *Barker v R* (1983) 153 CLR 338 the Supreme Court held that the provision 'requires attention to whether the particular entry in question was an entry that was made without lawful authority'. That said, no authoritative case since has considered whether the provisions of the *Criminal Code* (Cth) relating to computer offences could amount to criminal trespass.
[15] Because the information collected on the individual was not consented to, was gathered in a covert manner and/or was not in accordance with a company's privacy policy, or is disclosed in a manner not consistent with, or a for a purpose not recognised by, Australian law or court proceedings (*Privacy Act 1988* (Cth), APPs 3.1-3.3, 5 and 6).
[16] Such as the right to privacy (*Human Rights Act 2019* (Qld), s 25).

"deceptive" network architecture like tokens may open the door for a company to be found to have engaged in 'false or misleading conduct in trade or commerce' under Australian consumer law.[17]

Because the "limited use" provisions in the Cyber Security Legislative Package do not excuse conduct (or protect information that may constitute evidence) of any form of criminal offence, these provisions do not provide any legal clarity or certainty to the issues currently surrounding the use of active cyber defence in Australia. That is unfortunate, because the conduct of active cyber defence as a practice is broadly consistent with the Government's intention to be a leading cybersecurity nation by 2030 under the *2023-2030 Australian Cyber Security Strategy*.

The ACDA has developed a draft White Paper that more fulsomely discusses these issues and can supply that document to the PJCIS on request. Suffice to say, the scope of these issues is well beyond what the PJCIS has been asked to review. However, the ACDA welcomes the Government's commitment to addressing cybersecurity law as a priority and looks forward to being consulted on additional law reform which addresses the matters which have been raised above.

[17] *Competition and Consumer Act 2010* (Cth), Sch 2, s 18.

Conclusion

This submission has examined the proposed Cyber Security Legislative Package 2024, and how it might implicate active cyber defence measures and the legal defences that may be invoked by individuals or organisations who use active cyber defence measures to protect their networks and data from cyber-attacks. We have addressed our comments principally to the provisions relating to the institution of the Cyber Incident Review Board, the potential limitation of that Board's independence, and the "limited use" provisions. It has also discussed the limitations and challenges of applying these provisions in the context of active cyber defence, where the uncertainty of the law, the proportionality of the response, the attribution of the attacker, and the potential harm to third parties will still obligate the careful assessment of the legal risks and consequences.

Implementing and receiving the full value of ACD requires legal clarity. There is more law reform to be done, such as amendments that would resolve the current legal ambiguity to businesses, providing legal certainty so they can build and defend their organisation while operating within the bounds of the law. Without such clarity, businesses may inadvertently operate in legal grey areas, compromising their ability to protect themselves and their clients effectively.

To meet the Australian Government's vision of being a world leader in cyber security by 2030, the ACDA is promoting the use of active cyber defence technologies and techniques to better understand the actions and intent of cyber attackers and therefore better understand the threats to Australian organisations and citizens. Before we can encourage the use of these technologies and techniques, there needs to be legal clarity around the use of active cyber defence. The ACDA is calling on federal legislators to make the changes that will remove the legal grey areas and allow Australian organisations to be world leaders in cyber security by the end of this decade.

Active Cyber Defence Alliance

---------- END OF DOCUMENT ----------