Supplementary Submission
Security Amendment (Critical Infrastructure) Bill 2020 Inquiry

A document developed by the Active Cyber Defence Alliance

Written by John Powell & Helaine Leggat

Final version release on 28 July 2021

Security Amendment (Critical Infrastructure) Bill 2020 – Supplementary Submission

Disclaimer

The statements in this document are the opinions of the authors as members of the Active Cyber Defence Alliance and do not necessarily reflect the views of their individual employers.

Purpose

In the last few minutes of the hearing session that ran from 10:57am AEST to 11:53am AEST on Thursday the 8th of July, Senator Fawcett asked a question directly to Mr Andrew Cox and Ms Helaine Leggat from the Active Cyber Defence Alliance (ACDA).

This supplementary submission provides further detail in responding to the request of Senator Fawcett to expand on the ACDA assertion that there is legal uncertainty or lack of clarity around active cyber defence measures.

Context

In asking the question, Senator Fawcett states: "You say you think it could verge on offensive, which is the domain of the government, and companies are reluctant to engage in active cyber defence.".

Mr Cox clarifies that active cyber defence is about lawful countermeasures and does not cross the boundary into offensive actions as they are the sole domain of specific Government agencies.

Ms Leggat then provided a brief summary of the continuum of active cyber defence, doing so in an order that indicates the increasing likelihood of crossing from lawful to unlawful as perceived by security practitioners. This perception of increasing likelihood highlights the uncertainty that exists.

Further Explanation

The process of making a decision in regard to the defence of an organisation during a cyber-attack is neither simple, nor clear. On one side, there is the risk averse notion of doing nothing. On the other, there is the brashness of retaliation to protect assets and send a warning against similar attempts.

To do nothing is to fail at fulfilling the duties of due diligence and due care which leads to corporate and individual liability for directors and officers. Organisations that avoid risk by not acting against a cyber adversary will be placing their directors at greater risk.

To do too much could include criminal offences if the actions taken are of a criminal nature or civil law wrongs for disproportionate actions that cause damage or loss when stopping or disrupting the attack. Organisations that mitigate the risk of breach or data loss by engaging with the cyber adversary to thwart their attack will increase the likelihood of wading into unclear legal waters.

The middle path avoids breaches of law, but its boundaries are nebulous. Navigating this path can appear treacherous and consume resources of time and money.

Clarity in law regarding self-defence in the cyber environment will provide two specific outcomes:

a. corporate entities will save the time and money spent trying to find the lawful boundaries
b. directors and officers will have certainty about their rights and obligations in defending their digital ecosystem within cyberspace.

To illustrate the legal path between action and in-action, consider the targeting of online banking services by sophisticated malware.

Even in such an apparently simple phrase, there are a number of issues to be addressed:

a. Failure to act means failure to exercise due diligence (to identify the risk), failure to exercise due care (to act upon the risk identified) and negligence (failure to act as a reasonable person would in the circumstance). This translates to corporate and individual liability for directors, officers and employees with possible fines, imprisonment, claims for damage, shareholder actions for failure of directors' duties.
b. Paying a fee (ransom) for a decryption key may be deemed as contracting the services of a party held to be criminal organisation.
c. Persons wronged have a right of action, usually in the form of damages/compensation against the wrongdoer.
d. Innocent supply chain parties may be the victims of criminal offences and/or civil wrongs (tort). Apportionment of damages, fault, contributory negligence and downstream liability are relevant. Breach of contract may also apply.
e. The bank has a positive right/obligation to protect/defend itself, its assets, its customers and its third parties.
f. The bank's right/obligation to protect/defend extends to self-defence. Common law, criminal law and international law recognise the right of private and/or collective self-defence by individuals, corporate entities and nation states. Various conditions qualify the right which has been accepted to extend to pre-emptive attack. Self-help as a related doctrine is also relevant.
g. If the bank attacks the command-and-control infrastructure of the perpetrator that is distributing the malware then criminal damages will apply. Law does not distinguish or discriminate damage to property based on ownership. If damage to property is criminal, it will be criminal independent of ownership by perpetrators or innocent persons. Importantly, possession and control are seen as 'equivalent' to ownership.
h. When attacking the command-and-control infrastructure of the perpetrator, revenue generating operations of an innocent third party maybe taken down because the perpetrator has compromised the infrastructure of that operation. Innocent persons who have suffered wrongful damage/harm will likely have a claim for damages, which may extend to pecuniary loss (e.g., revenue). Apportionment of damages, fault, contributory negligence and downstream liability are relevant. The perpetrators of a crime will be prevented from asserting a claim of damages because of the legal doctrine in common law legal systems which prevents the assertion of matters before the court to prevent injustice (estoppel).

The law already exists to empower proportional self-defence in the cyber realm but needs clarity to empower action by risk averse industry entities.

Responses from other witnesses

Senator Fawcett asked if other witnesses had anything to add in regard to active cyber defence including the statement "…we need to understand how broad the call is for investing time into providing this clarity.".

The lack of responses from other witnesses to Senator Fawcett's question shows that the need for greater awareness around active cyber defence that drove the establishment the Active Cyber

Defence Alliance is self-evident. It should not be taken as lessening the need for this important legislative change but that the Active Cyber Defence Alliance is calling out an issue ahead of others.

Corporate entities will continue in their reluctance to plan for proportional self-defence during a cyber-attack until they have clarity on what they can and cannot do during a breach or in pre-empting a breach. With clarity, corporate entities will be able to confidently address breaches sooner and improve their cyber resilience.

Addressing the cyber resilience of corporate entities in Australia is addressing the cyber resilience of Australia.

Closing

In closing this supplementary submission, we would like to call out three action items that are necessary to provide legal clarity for cyber defence:

1. Research the national laws of Australia and other countries to establish what national laws apply to cyberspace and where possible re-interpret existing law
2. In Tallinn 1.0 & 2.0, the International Group of Experts held international law applies to cyberspace. Australia needs to contribute to Tallinn 3.0 and then extend this work to alignment of national law.
3. The Council of Europe Convention on Cybercrime (2004) is the only binding international treaty on cybercrime. Australia should work with other nations to negotiate a new treaty.