QUESTIONS ON NOTICE

REPORT ON PROCEEDINGS BEFORE
PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

CYBERSECURITY

At Macquarie Room, Parliament House, Sydney, on Thursday 29 October, 2020

The Committee met at 10:00

PRESENT

The Hon. Tara Moriarty (Chair)

The Hon. Trevor Khan
The Hon. Taylor Martin
The Hon. Adam Searle
Mr David Shoebridge

PRESENT VIA VIDEOCONFERENCE

The Hon. Lou Amato

Helaine Leggat

Attorney at Law, Managing Partner ICTLC Australia

Fellow of Information Privacy

Certified Information Systems Security Professional

Certified Information Systems Manager

Certified Information Privacy Professional

Certified Information Privacy Technologist

Graduate of the Australian Institute of Directors

Melbourne

18 November 2020

INTRODUCTION

1. I am required to provide information to Portfolio Committee no. 1. Premier and Finance, Cybersecurity, taken on notice at the hearing on Thursday 29 October 2020.

2. In addition to this document, I have provided the following additional materials:

   2.1. Powerpoint presentation: *Hybrid Warfare and Cyber Attacks within the Asis-Pacific Area. The Legal Implications of Hybrid War and Private Sector Actice Cyber Defence*;

   2.2. Published article: Cyber Warfare: *An Enquiry into the Applicability of National Law to Cyberspace, in the International Journal of Cyber Warfare and Terrorism;* [1] *and*

   2.3. Report: *Into the Grey Zone – Centre for Homeland Security and the George Washington University.* [2]

3. **Active Cyber Defence**

   3.1. Active Cyber Defence is a proactive cyber defence posture that involves the responses listed at 6.1.1 to 6.1.12 below.

4. **Active Cyber Defence - The Issue**

   4.1. Active Cyber Defence responses involve access to information and information systems. Specifically, whether access is lawful.

[1] Volume 10. Issue 3. July-September-2020. ISSN: 1947-3435. eISSN: 1947-3443.

[2] This work is licensed under CC-BY version 4.0 https://creativecommons.org/licenses/by/4.0 © 2016 by Center for Cyber and Homeland Security. It includes examples of Active Cyber Defence responses by Microsoft orporation, Google Inc. and others.

5. Active Cyber Defence – Lawfulness

5.1. The lawfulness, of Active Cyber Defence rests upon whether the access to information and information systems is authorised or not.[3] Unauthorised access in not lawful.

5.1.1. Because Active Cyber Defence is about collecting intelligence and information on information systems, access to information and to information systems is a *sine qua non*.

5.2. Authorisation and lawfulness is primarily regulated under the following Australian Statutes,[4] and their State and Territory equivalents:

5.2.1. Telecommunications law (including interception and access);

5.2.2. The Criminal Code; and

5.2.3. Data Surveillance law.

6. Active Cyber Defence - Responses

6.1. A summary of Active Cyber Responses is set out below. The lower the number (6.1.1), the more likely the response is to be lawful. The higher the number (6.1.11), the higher the risk of the response being unlawful when carried out by a private sector entity or state government without the assistance of law enforcement or intelligence services.

[3] See *Criminal Code Act 1995* (Cth) Pt 10.7; *Telecommunications (Interception and Access) Act 1979* (Cth).

[4] Numerous other laws apply, specifically national intelligence and law enforcement, privacy and others, but for the purpose of this response, I am simplifying. The issue is to separate the executive powers of law enforcement from the legitimate actions by the private sector/state government.

6.2. The lower the number, the more compelling it is that these responses are adopted by private sector entities and state government. Not to do so could be a failure in due diligence and care, because these responses are now best practice. In my view 6.1.1 to 6.1.9 should be authorised/mandated.

6.3. The higher the number, the more compelling it is that these responses are conducted with law enforcement/national security assistance.

6.4. Lawfulness of an Active Cyber Defence response also depends upon timing and proportionality. Different rules apply to a response that is before, during or after the attack.

6.1.1 *Information Sharing* - The sharing of actionable cyber threat indicators, mitigation tools, and resilience strategies between defenders to improve widespread situational awareness and defensive capabilities.

6.1.2 *Tarpits, Sandboxes & Honeypots* - Technical tools that respectively slow malicious actors to a halt at a network's perimeter, test the legitimacy of untrusted code in isolated operating systems, and attract malicious actors to decoy, segmented servers where they can be monitored to gather intelligence on malicious actor behavior.

6.1.3 *Denial & Deception* - Preventing adversaries from being able to reliably access legitimate information by mixing it with false information to sow doubt and create confusion among malicious actors.

6.1.4 *Hunting* - Rapidly enacted procedures and technical measures that detect and surgically evict adversaries that are present in a defender's network after having already evaded passive defences.

6.1.5 *Beacons (Notification)* - Pieces of software or links that have been hidden in files and send an alert to defenders if an unauthorised user attempts to remove the file from its home network.

6.1.6 *Beacons (Information)* - Pieces of software or links that have been hidden in files and, when removed from a system without authorisation, can establish a connection with and send information to a defender with details on the the structure and location of the foreign computer systems it traverses.

6.1.7 *Intelligence Gathering in the Deep Web/Dark Net* - The use of human intelligence techniques such as covert observation, impersonation, and misrepresentation of assets in areas of the Internet that typically attract malicious cyber actors in order to gain intelligence on malicious actor motives, activities, and capabilities.

6.1.8 *Botnet Takedowns* - Technical actions that identify and disconnect a significant number of malware-infected computers from the command and control infrastructure of a network of compromised computers.

6.1.9 *Honeyrecords (Information)* - Synthetically generated data records/documents containing unique code (finger print) that can be detected in a scan of the deep, dark and surface web. Honeyrecords provide positive evidence of data theft and give information on what data was stolen and when it was stolen.

6.1.10 *Coordinated Sanctions, Indictments & Trade Remedies* - Coordinated action between the private sector and the government to impose costs on known malicious cyber actors by freezing their assets, bringing legal charges against them, and enforcing punitive trade policies that target actors or their state sponsors.

6.1.11 *White-hat Ransomware* - The legally authorised use of malware to encrypt files on a third party's computer system that contains stolen information in transit to a malicious actor's system. Public-private partners then inform affected third parties that they have been

compromised and are in possession of stolen property, which they must return in order to regain access to their files.

6.1.12 *Rescue Missions to Recover Assets* - The use of hacking tools to infiltrate the computer networks of an adversary who has stolen information in an attempt to isolate the degree to which that information is compromised and ultimately recover it. Rarely successful.

7. Other factors

7.1. Consent – makes access and in many cases the response itself lawful. There are many legitimate ways of getting consent, supported by law and legal precedent.

7.2. Self-defence has been recognised for thousands of years in most legal systems. Just as the concept of 'unauthorised access' was a re-interpretation of 'trespass' in property law,[5] it is logical that the principles of self defence might be re-interpreted from lawful defence on property and premises, to lawful defence on a network. See for example 7.2.1 below.

7.2.1. Self -Defence - *Criminal Code Act 1995* (Cth)

S 4 – Definitions: **'**property' includes:
(a) real property; (b) personal property; (c) money; (d) a thing in action or other intangible property; (e) electricity; and (f) a wild creature that is tamed / kept.

Division 10 - Circumstances involving external factors. 10.4

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

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

[5] Recognised a criminal offence in the Budapest Convention on Cybercrime and adopted in to the national legal systems of signatory countries – in Australia, the Criminal Code Act 1995 (Cth)

(a) to defend himself or herself or another person; … or
(c) to protect property from unlawful appropriation, destruction, damage or interference; ...
and the conduct is a reasonable response in the circumstances as he or she perceives them.

(3) This section does not apply if the person uses force that involves the intentional infliction of death or really serious injury.

CAN INJURE PEOPLE AND PROPERTY, BUT CANNOT CAUSE DEATH IN THE DEFENCE OF PROPERTY

8. Proposition

8.1. 20 years ago, the world recognised electronic transactions and communications through UNCITRAL[6] which recognised and facilitated a new legal basis for the world to co-operate. Now it is time that we agree to what constitutes reasonable behaviour in cyberspace.

8.2. My proposition is that there is sufficient commonality in the national laws of many countries (especially Australia's allies), and sufficient legal precedent in numerous national legal systems to identify what cyber responses can best be the foundation for new norms in Cyberspace.

9. The Ask – Some ideas to commence action

9.1. Clarify through legislative, executive and judicial action:

9.1.1. That Australian laws apply to cyberspace;

9.1.2. Which Active Cyber Defence responses are lawful;

[6] UNCITRAL has been responsible for one convention and two model laws which have shaped the modernisation and harmonisation of electronic commerce: https://uncitral.un.org/

9.1.3. Establish whether the principles of self-defence apply to a network as they do to a property and premises;

9.1.4. Do the principles and defences applicable in burglary and hot pursuit apply to the recovery of data in the process of exfiltratiion?

9.1.5. Empower the private sector and state governments through existing law – for example, telecommunications law, intelligence law (ASIO Act), and even new statutes such as the Security Legislation Amendment Bill 2020 – to enable certain qualified persons in qualified industry sectors to undertake Active Cyber Defence responses. In simple terms, this means 'delegating' authority to spread the load on Government. This will raise the cost of attacking Australia at scale.

MR ANDREW COX
PORTFOLIO COMMITTEE NO. 1 - PREMIER AND FINANCE
INQUIRY INTO CYBERSECURITY
HEARING – 29 OCTOBER 2020

RECEIVED 19 NOVEMBER 2020

QUESTIONS ON NOTICE

Here is the Active Cyber Defence Alliance response to the question on notice regarding discussions the Active Cyber Defence Alliance is having with other Australian Government agencies.

- Cyber NSW - The Active Cyber Defence Alliance has made unsolicited submissions to the Minister for Customer Services NSW and the Minister for Transport for NSW. This has resulted in ongoing discussion with Cyber NSW
    - Contact Person - Stuart Staunton, Principal IT Security Advisor
- Transport for Victoria - The ACDA is scheduled to present the Active Cyber Defence Alliance agenda to the Information Sharing Working Group in late November
    - Contact Person - Graham Welch, Chief Security Officer
- ACCC (accc.gov.au) - The ACDA has provided proposals for a proof of concept of active cyber defence tools and methodologies to the ACCC in relation to the Consumer Data Right Initiative
    - Contact Person - Rob Deakin, Director Cyber Security
- Bussleton Water - Busselton Water has engaged the Active Cyber Defence Alliance in a Proof of Concept project to assess the efficacy of active cyber defence tools and methodologies
    - Toby Howes - Information Communication Technology Manager