THE AUSTRALIAN NATIONAL UNIVERSITY

Joseph Lee
Barrister (ACT); Advocate & Solicitor (Malaysia)
LLB (Hons) (Tas) LLM by Research (Tas)
PhD Candidate (ANU)

H Block
College of Law,
Fellows Road, Acton
Canberra ACT 2600
[redacted]

The Hon Peter Dutton MP
Minister for Home Affairs
Parliament House
Canberra ACT 2600

1 November 2019

Dear Mr Dutton,

Australia's 2020 Cyber Security Strategy — A Call for Views

Thank you for the opportunity to be part of the discussion on Australia's 2020 Cyber Security Strategy.

In this submission, I am addressing a few questions posed by the Department of Home Affairs.

1. **Is the regulatory environment for cyber security appropriate? Why or why not? What regulatory changes should Government consider?**
   My views on both questions focus primarily on the state of cyber security of Australia's critical infrastructure assets.

   The current state of cyber security of Australia's critical infrastructure assets is not appropriate because it contains a number of gaps and shortcomings. My discussion centres upon two pieces of legislation, as set out below:

   Security of Critical Infrastructure Act 2018 (Cth) (SCIA)

   The SCIA aims to strengthen the Australian Government's ability to manage the security risks of espionage, sabotage or coercion posed by foreign investors in Australian critical infrastructure assets such as water, ports, liquefied gas facilities, and electricity networks. The crux of the SCIA is the imposition of reporting obligations on owners and operators of Australian critical infrastructure assets, and the ministerial power to direct the owners and operators to do or refrain from doing certain acts. The SCIA contains two major shortcomings. One is the absence of any requirement that owners and operators of Australia's critical infrastructure assets take responsibility to implement and maintain good cyber security practices. Another is that ministerial intervention only occurs when the risks have come to light.

In a nutshell, the SCIA focuses on information-sharing between the Australian Government and owners as well as operators of Australia's critical infrastructure assets, with no obligations on the owners and operators to mitigate cyber security risks. In practice, owners and operators do implement safeguards against cyberattacks on Australian critical infrastructure assets — but the level of safeguards is currently left to self-regulation, potentially giving rise to varying standards of cyber security protection in the critical infrastructure sector in Australia.

Telecommunications Act 1997 (Cth) (TA)

The TA requires providers and carriers in telecommunications industry in Australia 'to do their best' to prevent Australian telecommunications networks and facilities from being used to commit cyber-related criminal activities. This is another example in which the Australian Government must show leadership. It ought to spell out what constitutes best cyber security practice. Does it mean world standard or accepted practice in Australia? The providers and carriers may have different interpretations of what is 'best' in light of their financial circumstances.

2. **What changes can Government make to create a hostile environment for malicious cyber actors?**

The Government can implement three measures:

A. Toughen the penalties for cyber-related crimes. The penalties in the *Criminal Code Act 1995* (Cth) (the Code) are too lax. Section 478.1 of the Code deals with hacking offences. It provides for a maximum penalty of 2 years' imprisonment. A similar length of sentence is set out under s. 478.2 of the Code as it applies to impairment of computer systems by using ransomware, spyware, worms, trojans and viruses. In a similar vein, s. 478.3 of the Code states that the possession or control of data with intent to commit cyber-related offences is punishable by a three-year imprisonment. It is timely for the Australian Government to increase the length of imprisonment penalties in the Code by the greatest possible number of years for cyber-related crime to demonstrate Australia's zero tolerance for such activity.

B. Engage with foreign countries from which cyber attackers originated. At present, some of the most serious cyberattacks in Australia have been committed by individuals in foreign countries. The Australian Government should sign extradition treaties with nations that are sources of cyberattacks in Australia. The main deterrence to this proposal relates to concerns about the lack of justice and human rights records in those countries. In 2017, the Australia jettisoned the proposed extradition treaty with China on these grounds. It is suggested the Australian Government revive this proposed extradition treaty, and treaties of a similar nature with other nations from which cyber security concerns in Australia arise. Further, the Australian Government could negotiate precautionary measures in an extradition treaty with its foreign counterparts to resolve any concerns about justice and human rights records.

Alternatively, the Australian Government ought to press Russia and China to join the Budapest Convention on Cybercrime (Budapest Convention). Currently comprising 67 signatory countries, the Budapest Convention facilitates intergovernmental cooperation in the investigation and regulation of cybercrime. If this option is not feasible, the Australian

Government could work with the Chinese and Russian Governments to deal with particular cyber security concerns in Australia. Both governments have denied any involvement in cyber-related criminal activities in Australia.

C. Build public awareness. The Australian Government could implement training courses at educational institutions of all levels in Australia to impart to students and teaching staff the importance of cyber security and how to achieve it. Further, the Government could support the provision of free workshops to create cyber security awareness among small businesses and the community. This public awareness will in turn elevate the standards of cyber security nationwide in the long run.

3. **Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?**

The Australian Government should invest more in understanding cyber criminals and their modus operandi, particularly those from overseas. There is a famous Chinese saying that to win a war, one must know thy enemies. A renowned Chinese strategist Sun Tzu is credited for arguing the importance of subduing one's enemies with stratagem. Implementing measures to protect Australians against cyber-related criminal activities is one part of the Cyber Security Strategy. The other part is to know who those cyber attackers are, where they are from, when they plan to attack Australia's computer systems, and how they attack those systems. These will be challenging tasks for the Australian Government but it is nonetheless a worthwhile effort.

4. **How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?**

Australia ought to attract the best and brightest cyber security professionals from around the world. We need these experts to lead Australia's cyber security industry, as well as resolve difficult and complicated problems for Australians. Once this pool of experts is established, high-quality cyber security professionals from overseas and Australia will be keen to work in the industry.

As an ideal country for immigrants, Australia has no problem in attracting the best and brightest to live in Australia. What is difficult, though, is to keep them in Australia on a permanent basis. This requires the Australian Government to relax immigration requirements for these individuals as well as provide various incentives to facilitate their cyber security-related business operations in states and territories in Australia. To further enhance Australia's competitiveness, the Australian federal and state governments should work with private entities in Australia, as well as institutions and information technology companies in the United States and Europe, to increase collaboration in research as well as exchange programs.

Yours sincerely,

[redacted]

Joseph Lee