THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Submission on the Department of Home Affairs' Consultation Paper on Protecting Critical Infrastructure and Systems of National Significance

16 September 2020

Department of Home Affairs

ci.reforms@homeaffairs.gov.au

Contact: **David Edney**
President, NSW Young Lawyers

Ashleigh Fehrenbach
Chair, NSW Young Lawyers Communications, Entertainment and Technology Committee

Contributor: Ravi Nayyar

Managing Editor: Olivia Irvine

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers Communications, Entertainment and Technology Committee (Committee) makes the following submission in response to the Department of Home Affairs' Consultation Paper on Protecting Critical Infrastructure and Systems of National Significance (Consultation Paper).

NSW Young Lawyers

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 16 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The NSW Young Lawyers Communications, Entertainment and Technology Law (CET) Committee of NSW Young Lawyers aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, confidential information and privacy, entertainment, and the media. As innovation inevitably challenges custom, the CET Committee promotes forward thinking, particularly about the shape of the law and the legal profession.

Summary of Recommendations

1. Question 23: The Committee submits in relation to Question 23 of the Consultation Paper that as much relevant threat information as practicable should be shared by Government with owners and operators of key systems of national security to ensure robust security responses, however, that such information should be tailored by relevance to reduce risks.
2. Question 31 and 34: In response to Questions 31 and 34 of the Consultation Paper the Committee submits that an independent oversight body must be created to ensure accountability.
3. Question 32: The Committee submits that a Government response to a cyber attack should not differentiate approach based on the geographical origins of the attack, due to the practical difficulty of ensuring that location, and the possible negative outcomes of a mistaken response.
4. Question 33: The Committee submits that, where dealing with presumed international cyber incidents, legal protections for industry and Government officers must conform to Australia's international legal obligations and international law norms surrounding state and non-state responses to cyber attacks.

Question 23

1. The Committee submits that as much relevant threat information as practicable should be shared by Government with industry, and particularly owners and operators of systems of national significance. As referred to by the United States' National Institute for Standards and Technology ('NIST'), key types of threat information include:
    - indicators;
    - tactics, techniques and procedures ('TTPs') of malicious actors;
    - security alerts;
    - threat intelligence reports; and,
    - tool configurations.[1]

2. In addition, the Committee submits that Government should provide open source intelligence ('OSINT') briefs to industry to augment their situational awareness, as well as preparatory and incident response capabilities.

3. The Committee considers that Government should share as much relevant threat information with industry as possible, subject to the need to prevent harm to ongoing operations by Australia's intelligence and law enforcement agencies. Government should explore whether agencies such as the Australian Signals Directorate ('ASD') can regularly provide classified briefings to chief information security officers ('CISOs') for systems of national significance to share threat intelligence.

4. Such information will help CISOs better coordinate the security of systems of national significance because, particularly when potentially defending against state actors, their strategies would be based on vetted signals intelligence, rather than relying upon the little and unqualified information available in private sector communities.

5. The Committee notes that a key benefit of greater threat information sharing is the development of more robust systems of defence around key sectors of national significance. The Committee seconds the comments of the NIST, that 'shared situational awareness', improved security posture', 'knowledge maturation,' and 'greater defensive agility' are likely to accrue as a result of greater information sharing.[2] Owners and operators of systems armed with the latest threat intelligence,

---

[1] Chris Johnson et al, National Institute for Standards and Technology, *Guide to Cyber Threat Information Sharing* (NIST Special Publication No 800-150, October 2016) 2.
[2] Ibid 3-4.

best practice guidance, and vulnerability information from reliable sources in Government agencies like the ASD, can be more proactive in instituting better security controls and practices which may identify and mitigate threats. Personnel may become better educated in how to respond to a variety of current and emerging threat actors on an ongoing basis through more targeted training programs. Key sectors, if better informed as to the TTPs of attackers, will develop informed incident response procedures more able to adapt to how those TTPs unfold in close-to-real time. As individual systems of national significance become more resilient by leveraging greater and richer threat information provided by Government, the overall critical infrastructure sector can become more resilient to attacks and slow the spread of malicious cyber activity.[3]

6. This is in accordance with the principles of the *Security of Critical Infrastructure Act 2018* (Cth), which aims to 'facilitat[e] cooperation and collaboration' between the private and public sectors to mitigate national security risk for critical infrastructure.[4] The imperative of collaboration is critical to the fulfilment of Australia's cybersecurity strategy, as the statement on Government's 'Approach' to delivering the 'Vision' of the strategy highlights: 'This vision will be delivered through complementary actions by governments, *businesses* and the community'.[5] The strategy goes on to state that 'everyone … has a role to play'.[6] Similarly, the Cyber Enhanced Situational Awareness and Response (CESAR) package, announced in June 2020, provided funding for measures to improve collaboration and information sharing by the ASD with industry, particularly vulnerable sectors.[7]

7. The Committee qualifies the above, noting that all information sharing should be tailored to the relevant industry sector and actor receiving the relevant information. For instance, information pertaining to an exploit which is specific to a version of software that helps operators control circuit breakers in a power station should not necessarily be provided, for example, to the operators of a water treatment plant which runs on a different version of that software. Strategic limitation of information is necessary to ensure that sectors and actors do not suffer from information overload resulting in *relevant* threat information being overlooked. Additionally, this kind of information may necessarily expose possible exploits which may be leveraged against critical information security

---

[3] Johnson et al, (n 1) iii, 3-4; Critical Infrastructure Centre, Department of Home Affairs, *Protecting Critical infrastructure and Systems of National Significance* (Consultation Paper, August 2020) 25.
[4] *Security of Critical Infrastructure Act 2018* (Cth) s 3(b).
[5] Australian Government, *Australia's Cyber Security Strategy 2020* (Report, 6 August 2020) 6 (emphasis added).
[6] Ibid 7.
[7] Scott Morrison, Peter Dutton and Linda Reynolds, 'Nation's Largest Ever Investment in Cyber Security' (Joint Media Release, Department of Defence, 30 June 2020).

and operations. As such, the relevance of information should remain a key consideration to the extent and structure of Government/industry cooperation.

Recommendation

Question 23: The Committee submits in relation to Question 23 of the Consultation Paper that as much relevant threat information as practicable should be shared by Government with owners and operators of key systems of national security to ensure robust security responses, however, that such information should be tailored by relevance to reduce risks.

Question 31 and Question 34

8. The Committee would like to preface its comments with acknowledgement of the Government position that there is a need for the power to declare an emergency ('declaration power') and that a direct action ('DA power') in a national emergency must be 'limited by robust checks and balances'.[8] These are significant powers in light of the nature of their exercise enabling and constituting, respectively, direct government interference in potentially privately owned and/or operated critical infrastructure systems and networks. The Committee is concerned by the broad wording of the factors to be considered by Government in determining whether an incident constitutes an emergency. References to 'the national interest' and 'any dependent essential services' may be similarly problematic,[9] as, the declaration power and the DA power may be triggered in a very wide variety of circumstances. The need for strong oversight of the DA power is critical since Government envisions scenarios where a relevant critical infrastructure entity would have to be coerced into allowing Government agencies to intervene against malicious cyber activity. If legislated, the possibility of coercive power may in turn impact the likelihood of voluntary acceptance of Government assistance by private sector entities.

9. The Committee therefore submits that oversight of the Government's use of these powers should be provided by the creation of an independent statutory office of the Cyber Emergency Powers Commissioner ('CEPC'). This office would be closely analogous with the Investigatory Powers Commissioner ('IPC') as recommended by the Independent National Security Legislation Monitor's ('INSLM') review of the *Telecommunications and Other Legislation Amendment (Assistance and*

[8] Critical Infrastructure Centre (n 3) 29.
[9] Ibid 29.

Access) Act 2018.[10] The Committee uses the recommendations of the INSLM (contained in paragraph [11.21] and [11.30] of the INSLM's review) in relation to the proposed IPC as inspiration for the proposed CEPC. Like the IPC, the Committee considers that the CEPC should be a retired judge of the Federal Court, or State or Territory Supreme Court, 'appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition'.[11] The CEPC must approve every exercise of the proposed *coercive* power to intervene in critical infrastructure systems and networks, given the principle that 'the ability to use coercive powers without external and independent review and authorisation is exceptional and requires justification'.[12]

10. The Committee calls for the appointment of 'a suitable number of eminent, independent technical experts,' representative of 'Government, industry and academia and covering the range of scientific and technical disciplines required'[13] to advise the CEPC on the proposed exercise of coercive power. The experts, apart from advising the CEPC in relation to each proposed exercise of coercive power, would help the CEPC audit, and recommend necessary reform of the regime, and annually report to the Attorney-General and Parliamentary Joint Committee on Intelligence and Security on the operation of the regime. Much like the proposed IPC, some of these experts alongside the proposed CEPC would comprise a Cyber Emergency Powers Division headed by the CEPC, a dedicated division of the Administrative Appeals Tribunal providing an in-built venue to consider and examine contested matters whilst preserving confidentiality.[14] The advisers will play a crucial role in overseeing of the use of the powers due to the complexity of the policy and technical issues engaged by the powers, as well as the need for a swift and proportionate response to imminent/ongoing threats to the security of systems of national significance as 'the subset of critical infrastructure entities of highest criticality'.[15]

Recommendation

Question 31 and 34: In response to Questions 31 and 34 of the Consultation Paper the Committee submits that an independent oversight body must be created to ensure accountability.

---

[10] James Renwick, Independent National Security Legislation Monitor, *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters* (30 June 2020) 220.
[11] Renwick (n 10) 220, 223-224.
[12] Ibid 191.
[13] Renwick (n 10) 222.
[14] Ibid 223-224.
[15] Critical Infrastructure Centre (n 3) 13.

Question 32

11. The Committee submits that this question must be answered in the negative. As a matter of principle, the Committee submits that the following considerations that should *primarily* guide Government *whenever* it deploys any offensive cyber capabilities in a manner attributable to Australia in international law terms are:
    a. compliance with international law and norms, particularly those applicable to the conduct of states in cyberspace;
    b. compliance with the *Tallinn Manual on the International Law Applicable to Cyber Warfare*;[16] and,
    c. the need to preserve the operational security of Government capabilities to conduct computer network attack, defence and exploitation.

12. The Committee stresses the importance of the need to preserve operational security, given that cyber or signals intelligence capabilities, unlike most conventional military capabilities, lose their utility once their use is discovered. As national security scholar, Ben Buchanan, writes, 'Exposing particular hacking capabilities tends to render those capabilities much less useful, especially against well-secured targets. Shrouding cyber capabilities in secrecy is such a crucial principle'.[17] If Government conducts an offensive cyber operation against a target, there is a risk that the nature of the operation itself, the TTPs deployed, and the infrastructure used by the Government officers in the process, will betray the secrecy of Australian capabilities in cyberspace.[18] For instance, the targeting of specific vulnerabilities without proper operational secrecy controls in place can help Australia's adversaries better understand how to: defend against, or interfere with, Australian computer network operations (including the collection of signals intelligence) and/or attack Australian networks.

13. The Committee also points to the great difficulty with reliably identifying the location of malicious actors in cyberspace. The commentary on Rule 2 of the *Tallinn Manual* reinforces that difficulty in the context of determining whether any, and which, state has jurisdiction in international law terms in the cyber domain:

---

[16] Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) ('*Tallinn Manual*'). This document was developed by an International Group of Experts invited by the NATO Cooperative Cyber Defence Centre of Excellence and counts members of the Australian Defence Force as consulted 'Legal Experts' and 'Peer Reviewers': xi-xii, 1.
[17] Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Harvard University Press, 2020) 308-9.
[18] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks '(2015) 38(1-2) *Journal of Strategic Studies* 4, 18.

> It must be cautioned that it is possible under certain circumstances for someone who does not wish to be tracked to spoof[19] the geo-coordinates advertised by his or her computing device. It is also possible that user-location will not be made available by the infrastructure or service provider, or by the application or device itself. Actual physical presence is required, and sufficient, for jurisdiction based on territoriality; spoofed presence does not suffice.

14. Rule 8 backs this up: 'The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State'.[20]

15. Malicious cyber activity against the 2018 Winter Olympic Games Opening Ceremonies represents a suitable case study of the difficulty with reliably attributing such cyber attacks to a particular state. The allegedly Russian state hackers behind the 'Olympic Destroyer' malware were deploying TTPs resembling those of Chinese and North Korean hackers — apparently the 'first time someone used false flags of that kind of sophistication in a significant, national-security-relevant attack' — to confuse attribution efforts.[21] As Rid and Buchanan argue, 'Military organisations can be identified without identifying individuals and smaller units first — this may be starkly different in cyber operations'.[22]

16. The difficulty with identifying the location of a cyber actor is due to the *nature* of the actor, that is, whether they are state- or non-state-actors. Rule 7 of the *Tallinn Manual* is instructive*:* 'The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State…'.[23] The Commentary on Rule 7 reinforces this:

> Prior to the advent of cyber operations, the use of governmental assets, in particular military equipment, would typically have been attributed to the State without question because of the unlikelihood of their use by persons other than State organs or individuals or groups authorized to exercise governmental

---

[19] In this context, 'spoof' meaning to falsify: Australian Signals Directorate, 'Spoof', *Australian Cyber Security Centre Glossary* (Web Page) <https://www.cyber.gov.au/acsc/view-all-content/glossary/spoof>
[20] Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) 36.
[21] Andy Greenberg, 'The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History', *WIRED* (News Article, 17 October 2019) <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>; Ellen Nakashima, 'Russian Spies Hacked the Olympics and Tried to Make It Look Like North Korea Did It, U.S. Officials Say', *The Washington Post* (online, 25 February 2018) <https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html>.
[22] Rid and Buchanan (n 17) 13.
[23] Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) 34.

> functions. *This traditional approach cannot be followed in the cyber context.* It may well be that government cyber infrastructure has come under the control of non-State actors who then use it to conduct cyber operations.[24]

17. Thus, attempting to tailor a response to particular attackers based on their supposed location (such as in a government building) could be futile if that supposed location is a ruse devised by the attackers. Worse still, it could result in a diplomatic incident if Government officers conduct computer network attack, based on intelligence undermined by the original attackers' false flags, against infrastructure and systems located in a jurisdiction with nothing to do with the original attack.

Recommendation

Question 32: The Committee submits that a Government response to a cyber attack should not differentiate approach based on the geographical origins of the attack, due to the practical difficulty of ensuring that location, and the possible negative outcomes of a mistaken response.

Question 33

18. The Committee submits that the answer to this question pivots on whether the emergency actions, if comprised of computer network operations against offshore targets, raise international law issues, particularly in relation to norms defining states' activities in cyberspace, and issues under the *Tallinn Manual*. For instance, as a matter of principle, the Committee believes that states and their representatives must be held to account for committing war crimes, such as by launching armed attacks against civilians. The Committee agrees with Rules 31 and 32 of the *Tallinn Manual* that apply the principle of distinction to cyber attacks such that civilians must not be targeted.[25]

19. The Committee calls for extended consultation with experts in international law, in particular the law of armed conflict, to ensure that any legal protections for officers undertaking emergency actions are compliant with Australia's obligations under international law, the aforementioned norms, and with the terms of the *Tallinn Manual.*

20. The Committee also submits that the proposed CEPC be advised by experts in international law, in particular the law of armed conflict. This is to help prevent potential breach of legal obligations or norms that apply to, or otherwise govern, states' activities in cyberspace. These experts will play a

[24] Ibid 35.
[25] Schmitt (n 22) 110-14.

critical role in ensuring that Australia does not (un)wittingly contribute to the development of international norms — particularly in the absence of a bespoke treaty framework — that may run counter to Australian values and embolden hostile states to do harm to Australian interests via cyberspace.

Recommendation

Question 33: The Committee submits that, where dealing with presumed international cyber incidents, legal protections for industry and Government officers must conform to Australia's international legal obligations and international law norms surrounding state and non-state responses to cyber attacks

Concluding Comments

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions please contact the undersigned at your convenience.

Contact:

David Edney

President

NSW Young Lawyers

Email: president@younglawyers.com.au

Alternate Contact:

Ashleigh Fehrenbach

Chair

NSW Young Lawyers Communications, Entertainment and Technology Committee

Email: ashleigh.fehrenbach@younglawyers.com.au