CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:
Cyber and Critical Technology International Engagement Strategy (CCTIES)

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: Cyber and Critical Technology International Engagement Strategy (CCTIES)

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) submission to the Department of Foreign Affairs and Trade (DFAT) review of the Cyber and Critical Technology International Engagement Strategy (CCTIES). We commend the Federal Government for its ongoing commitment to ensuring Australia remains a world leader and evolving power in international cyber and critical technology and policy.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 24 Participants including seven Research Providers, seven State and Federal Government Agencies/Departments and 10 Industry/SMEs.

This submission is very broad based. We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding the CCTIES.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
(02) 6103 9922
ceo@cybersecuritycrc.org.au

Executive Summary

The Cyber Security Cooperative Research Centre (CSCRC) welcomes the opportunity to provide this submission to the Department of Foreign Affairs and Trade (DFAT) review of the Cyber and Critical Technology International Engagement Strategy (CCTIES). Such a review is essential to ensuring Australia's cyber and critical technology capabilities and objectives remain relevant in a globalised world.

COVID-19 has highlighted the interconnectedness of the world we live in and the vital importance critical infrastructure and supply chains play to national sovereignty. Therefore, while it is essential to embrace the connected world and the technologies that serve to enhance it, these needs must be balanced with the protection of digital sovereignty.

There is a clear opportunity for Australia to ensure domestic laws – laws with real-world consequences – are aligned with digital developments. This will enhance Australia's reputation as a safe and trusted place to do business.

And Australia must be forward thinking and agile, taking into consideration future sector requirements to ensure international relevance. This can be fostered by strong collaboration between industry and academia, delivered through organisations like the CSCRC.

The CSCRC submits:

- there should be no difference between the online or offline environment when it comes to rule of law and recognition of criminal activity;
- Australia has an opportunity be a world leader in cyber security law and policy by enshrining in law a National Data Policy and minimum cyber security standards;
- Australia's digital sovereignty and the integrity of our nation's critical infrastructure are priceless and the roll-out of 5G will have a profound impact on geopolitics;
- Australia should work with its Indo-Pacific neighbours to help them establish stringent and rigorous cyber security provisions and protocols to build regional security;
- There is an opportunity for Australia to build on and leverage existing FTAs to promote and export Australian-developed cyber innovations and technologies, and to include the sector in future FTA negotiations; and
- A holistic and multidisciplinary approach is needed in developing the cyber security professionals of the future.

What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?

In an increasingly connected world, ensuring that Australia remains a trusted and safe place to do business and engage online should be a key objective of government. To this end, the CSCRC contends there should be no difference between the online or offline environment when it comes to rule of law and recognition of criminal activity. Abiding to this principle will serve to enhance trust in Australia's cyber systems both internationally and domestically.

Australia has an opportunity to be a global leader in cyber security law and policy. This can be achieved through enshrining in law a National Data Policy and minimum cyber security standards. Sensitive data relating to Australian citizens – whether it is held by government, industry or academia – should be stored and protected in accordance with minimum cyber security standards alongside a National Data Policy. Such mechanisms would provide real consequences for organisations who fail to meet proscribed standards and recognise harm for victims in circumstances where their personal data is breached.

It is vital the Federal Government continues to pursue its stated aims regarding legal principles applying both online and offline[1]. What is illegal in the offline world must be illegal in the online world. Law enforcement and intelligence agencies must have the tools and appropriate processes to operate in a challenging threat environment and to prevent and prosecute such crimes. Australia has led the way globally with legislation such as the *Telecommunications and Other Legislative Amendments ('Assistance and Access') Act 2018* and the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, which are appropriate responses to an environment where organised crime, terrorism, and fraud is frequently amplified, inspired and facilitated online.

Ultimately, the Federal Government garners international trust when it confirms its guiding principles domestically through the establishment of defined legislative frameworks that mandate and enforce cyber conduct.

How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?

Australia's digital sovereignty and the integrity of our nation's critical infrastructure are priceless, as is the case for all nation states. However, the advent of 5G – and potentially 6G by 2030 – is vastly altering the cyber environment and, in turn, the geopolitical environment. All nations, no matter how large or small, rely on the internet and, more and more, the Internet of Things (IoT) to function effectively and efficiently.

The CSCRC contends implementation of 5G networks will have a profound influence on geopolitics moving forward because a threat anywhere in the network will be a threat to the whole network. In 2018, the Federal Government banned high-risk vendors from providing 5G technology for wireless networks due to national security concerns. Central to this decision was the threat of disruption to a network as a result of third-party interference, which could cripple business, supply chains and other critical online infrastructure Australians rely on. Every reasonable step must be taken to ensure these systems are not compromised – and that includes evaluating risks associated with companies providing 5G technologies.

[1] https://www.theaustralian.com.au/commentary/encrypted-messages-favour-the-worst-of-the-worst/news-story/3fc80e3c44341f0a11f85824df0f7bcc

However, some of Australia's key allies have taken a different approach to 5G and have not limited vendors as strictly. While the move towards 5G is inevitable, Australia and other countries must remain vigilant to the potential risks it presents and work towards shoring up stringent and rigorous cyber security provisions and protocols to deal with hostile actors.

Therefore, Australia's relationships with other countries, based on collaboration, participation and openness, will play a vital role into the future.

What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?

Australia is committed to its enduring relationship with Pacific neighbours, as evidenced by the Federal Government's Pacific Step-Up. Part of this is helping ensure the resilience of Pacific Island countries to security challenges, including cyber security challenges.

As noted above, the expansion of 5G presents problems and opportunities. Across the Indo-Pacific, 5G offers the potential to bring nations closer together and help build the economic and social capacity of developing nations. Australia needs to work with these nations to help them establish stringent and rigorous cyber security provisions and protocols, which will build regional security and encourage the ongoing relationships of collaboration and cooperation Australia shares with its regional neighbours.

Automated vehicles deployed in intelligent transportation systems carry a high cyber security risk. Transportation infrastructure in Australia lends itself to provide autonomous services to rural areas (e.g. for bushfire detection and response) and manage ports and shipping infrastructure more efficiently. However, use of intelligent systems in support of these critical infrastructure bring additional risks and require a coordinated, agile approach to cyber security and incident response to manage the risk of cyber attack.

Smart grid technologies are essential to manage and ensure resilience in the electricity grid which, as a result of the increasing use of solar and other renewable energies, is increasingly complex. While smart grid technologies offer significant opportunities to the economy and ecology of Australia, the complexity and interdependence of these systems and the wide reliance of other sectors on this critical infrastructure means that they represent a significant risk. For this reason, cyber security and resilience must be addressed early as part of a secure-by-design approach.

In less developed countries in the Indo-Pacific region the rapid adoption of smart technologies in city infrastructure and critical services presents a risk to their economies, with potentially damaging consequences to Australia's supply chains and geopolitical position. Ensuring strong collaboration on cyber security policy and sharing of threat-intelligence across the region and other strategic alliances can reduce these risks and provide essential coordination and response to cyber security threats.

How should Australia pursue our cyber and critical technology interests internationally?

Australia is fortunate to have strong international strategic and trade ties.

The enduring Five Eyes relationship between Australia, Canada, New Zealand, the United Kingdom and the United States is pivotal for both national security and economic stability and has sharply increased its focus on cyber security in recent years. As noted in the Official Communique of the Five Country Ministerial Meeting of 2018: "The increasingly digitised and networked nature of all aspects of our economies and societies means that cyber security and resilience is of the highest priority".[2]

Likewise, a number of existing, new and emerging free trade agreements (FTA) continue to strengthen Australia's ties with other nations. Currently, cyber and critical technology transfers are limited within most of these FTAs (with the omission of Singapore[3] and New Zealand[4]). However, the CSCRC sees an opportunity to build on and leverage existing FTAs to promote and export Australian-developed cyber innovations and technologies, and to include the sector in future FTA negotiations.

As previously noted, ensuring strong international collaboration on cyber security policy and sharing of threat-intelligence can reduce cyber risks and provide essential coordination and response to cyber security threats.

How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?

It is a legitimate role of government to address these global interests by providing leadership and fostering collaboration between industry and academia through organisations like the CSCRC. In this space, Australia must be forward thinking and agile, taking into consideration future sector requirements to ensure international relevance. For example, advances in machine learning and artificial intelligence (AI) are likely to automate many of the basic cyber security requirements currently met by trained personnel – this needs to be considered in long-term planning for both academic programs and the types of workforce Australia and other nations will need in the next 10-15 years. However, there are also growth opportunities that will arise because of AI and automation, such as an increase in cyber-physical systems.

The need for advanced cyber security products and services – a sector projected to be worth US$248 billion globally by 2026[5] – will not be met by training people only in basic network security. A holistic approach is needed. Skillsets need to be diverse and include skills such

[2] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018
[3] https://www.dfat.gov.au/trade/agreements/in-force/safta/Pages/singapore-australia-fta
[4] https://www.dfat.gov.au/trade/agreements/in-force/anzcerta/Pages/australia-new-zealand-closer-economic-relations-trade-agreement
[5] https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1

as critical thinking and ethics to enable digital products to be secure-by-design and to operate as intended. Similarly, cyber security professionals of the future will need to have legal, regulatory, marketing and other qualifications. Any long-term planning with respect to building skilled professionals must include a broad approach and not just be confined to STEM-based qualifications.

As noted above, the CSCRC also sees a real opportunity for Australia to continue to lead the way globally in regards to legislative frameworks that help regulate online behaviour, as has been the case with the *Telecommunications and Other Legislative Amendments ('Assistance and Access') Act 2018* and the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*. In this space, we contend that the Federal Government has the opportunity to consider corporate issues, including Directors' obligations and frameworks that would mandate companies to take responsibility for the security of products they supply and import.

What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

Firstly, the CSCRC notes that Australia, through its domestic laws and the Five Eyes relationship, is a global leader in international cyber and technology policy issues. The Federal Government has taken a strong – and necessary – stance in protecting the nation's critical infrastructure by its refusal to allow high-risk vendors take part in the development of the 5G network. Likewise, through the Five Eyes partnership, Australia has agreed to:

- Collaborate with industry and standards bodies to provide better protection to users by advocating that devices should be secure-by-design;
- Actively seek out opportunities to enhance trust and raise awareness of security safeguards associated with IoT devices;
- Identify and engage industry partners who share Five Eyes' goals to enhance the security of IoT;
- Identify and engage like-minded nations to encourage international alignment on IoT security, unlocking innovation that builds a strong economy that works for everyone; and
- Share information with Five Eyes partners in a timely manner through appropriate channels and arrangements, consistent with international and domestic law, to aid in the overall improvement of IoT security.[6]

It is also worth noting the European Union's Network and Information Security (NIS) Directive as a case study for regulation. The advantage of Directives such as NIS, is the establishment of a common reference framework to ease communication and collaboration between countries. The CSCRC believes this is a significant advantage for the protection of critical infrastructures that cross state boundaries. It also supports operations and

[6] https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

compliance assessments for organisations that operate across state and country boundaries, offering "a well-thought of and balanced response that takes into account the (cybersecurity) problem and plans for the future … and introduces a system of cross-EU cooperation"[7] as long as any compliance assessment results in actual security improvements for organisations that own and manage critical infrastructure. It is imperative that any system in place to help organisations better understand and manage their cyber security risk is more than a desktop review.

[7] D. Markopouloua, V. Papakonstantinoua, P. de Hertab. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, *Computer Law and Security Review*, 35:6, 2019.