THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Cyber and Critical Technology International Engagement Strategy (CCTIES)

Submission to the Department of Foreign Affairs and Trade

6 June 2020

Coordinating Authors

Dr Greta Nabbs-Keller
Research Fellow Southeast Asia & the Indo-Pacific
Centre for Policy Futures
g.nabbskeller@uq.edu.au

Professor Ryan Ko
Chair & Director - Cyber Security
School of Information Technology and Electrical Engineering
Faculty of Engineering, Architecture and Information Technology
ryan.ko@uq.edu.au

Table of Contents

Contributing authors

This submission has been written by the following authors.

- **Dr Micheal Axelsen**, School of Business, UQ
- **Dr Ivano Bongiovanni,** School of Business, UQ
- **Ms Dallas Dowsett,** Global Engagement and Entrepreneurship, UQ
- **Professor Ryan Ko,** School of Information Technology & Electrical Engineering, UQ
- **Associate Professor Rain Liivoja**, TC Beirne School of Law, UQ
- **Dr Ray Maher**, Centre for Policy Futures, UQ
- **Dr Eve Massingham**, TC Beirne School of Law, UQ
- **Mr Chris McEwan,** Centre for Policy Futures, UQ
- **Dr Simon McKenzie**, TC Beirne School of Law, UQ
- **Dr Greta Nabbs-Keller**, Centre for Policy Futures, UQ
- **Mr Richard O'Quinn,** School of Business, UQ
- **Dr Amelia Radke**, Centre for Policy Futures, UQ
- **Associate Professor John Williams,** School of Information Technology & Electrical Engineering, UQ

Introduction

This submission has been made by colleagues from The University of Queensland (UQ) Centre for Policy Futures, UQ Cyber Security, UQ International Development, TC Beirne School of Law and UQ School of Business.

We commend DFAT's focus on cyber and critical technologies as an essential part of Australia's international engagement and hope the information and recommendations in this Submission will prove valuable. We would welcome the opportunity to discuss these issues in more detail with DFAT or to otherwise assist in developing the Department's final international engagement strategy.

The University of Queensland

For more than a century, The University of Queensland (UQ) has maintained a global reputation for delivering knowledge leadership for a better world.

The most prestigious and widely recognised rankings of world universities consistently place UQ among the world's top universities.

UQ has also won more national teaching awards than any other Australian university. This commitment to quality teaching empowers our 53,600 current students, who study across UQ's three campuses, to create positive change for society.

Our research has global impact, delivered by an interdisciplinary research community of more than 1500 researchers at our six faculties, eight research institutes and more than 100 research centres.

The Centre for Policy Futures was established with the three-fold purpose of undertaking policy-relevant and rigorous research; capacity building within the University to enhance the ability of academics to engage with policy makers; and delivering a research engagement program for policy makers in Queensland, Australia and the Indo-Pacific.

UQ Business School is one of the world's leading business schools. It is recognised for the quality of its teaching and academic staff, the depth of its education programs, and for cutting-edge research and close links with industry.

UQ Cyber Security is a university-wide interdisciplinary research and education initiative located in the School of Information Technology and Electrical Engineering. Its mission is to address global cyber security challenges and educate top cyber security leaders. It works closely with the Australian Defence Force, Joint Cyber Security Centre, AustCyber and Austrade.

TC Beirne School of Law brings together leading national and international scholars, distinguished alumni and leaders of the legal profession to provide students with an outstanding legal education which will equip them for a wide variety of careers, both within Australia and internationally.

UQ International Development (UQID) is one of the leading university development groups in the Indo-Pacific region and in the past 25 years has successfully managed more than 500 development assistance activities in over 80 countries.

This submission represents the opinions of the contributing authors listed in this document. It does not necessarily represent an official position of The University of Queensland.

Recommendations

Recommendations (16) for DFAT as outlined in this document:

1. Australia should facilitate a human rights approach that recognises the importance of digital inclusion to balance the risks and opportunities for diverse populations in Australia and the Indo-Pacific. In particular, there needs to be a recognition that cyber safety has a direct relationship with digital inclusion.
2. Australia should continue to lead in clarifying disputed areas of international law relevant to cyber law. In cyber rules and principles, as with all areas of the law, Australia should be committed to openness and transparency of the law and the fair application of underlying principles. In the case of cyber warfare, Australia should continue to affirm the importance of the four fundamental principles of necessity, proportionality, distinction and humanity.
3. As cyberspace and the implementation of critical technologies have influence well beyond defence and geopolitics, citizens' perspectives must be systematically incorporated into decision-making.
4. Australia should address the risks posed by *inter alia* ransomware attacks on the IoT, compromised blockchain systems, cryptojacking, and privatised cyber warfare through the development of a world leading national program to include: information risk assessment, management and mitigation strategies; auditing security controls; continuous Information Security operations; continuity of operations plans and procedures for critical infrastructure and technologies; crisis management and incident response processes; cyber resilience programs; data pseudonymisation and encryption.
5. Australia must invest in national and international legal, regulatory, governance and diplomatic efforts to understand the impacts of emerging space-based platforms and shape global norms on their use.
6. Australia can contribute productively through research into data provenance, attribution and detection technologies, technologies and platforms for establishing chains of trust in media and digital content, and regulatory and diplomatic efforts in establishing and adhering to international norms.
7. Australia can contribute productively through research into the automated detection and identification of botnet and fake social media account networks, and continue engagement with social media platforms on regulatory responses.
8. Australia should continue to participate actively in discussions on new internet architecture to engage a global conversation.
9. Australia should develop Cyber Security and Critical Technology 'Centres of Excellence' within Australia that partner with key stakeholders throughout the region.
10. Australia should encourage the development of educational programs in decision-making around cyber and critical technology interests (at the strategic, management, and operational levels) in the Indo-Pacific region to encourage the development of cyber resilience in government and businesses throughout the region.

11. Australia should encourage societal resilience by developing and integrating programs that bolster political and societal resilience in the wake of coordinated electronic misinformation programs.
12. Australia should develop template public education programs that provide users across the region with tools, tips and techniques to identify 'Fake News' and the questions to consider in evaluating the news they receive by social media.
13. Australia should continue to encourage exchanges of views between states – and between experts within the private sector, civil society and academia – on how particular rules and principles of international law apply to state conduct in cyberspace.
14. Australia should continue funding of targeted training and professional development of key multi-agency personnel from government and industry in our region to underpin the building of regional capabilities and relationships, which Australia will be able to draw upon as and when required.
15. Australia should adopt an agile, multi-stakeholder approach to ensure efficient and effective collaboration among cybersecurity stakeholders through a six-step cycle, which could be easily scaled-up to other countries/regions (cycle detailed at Question v.).
16. Australia should adopt a collaborative systems mapping approach to identify how cybersecurity threats, issues, stakeholders, and technologies may impact on other issues throughout society. This process can help synthesise the perspectives of a more diverse range of stakeholders and incorporate the impacts of critical technologies in policy formulation, beyond defence and geopolitical considerations.
17. Australia should position itself as the location for the best minds and talent from the Indo-Pacific and Western nations. This can be achieved through campaigns and strategic messaging, showcasing past Australian technological successes and innovations.

Background

In October 2017 DFAT released Australia's inaugural International Cyber Engagement Strategy (ICES) to guide international engagement across the full range of Australia's interests in cyber affairs. Led by the Ambassador for Cyber Affairs, implementation of the ICES has established Australia as a leading international actor on cyber affairs. Recognising the dynamic of Australia's digital interests, DFAT will update the ICES in 2020, and broaden the scope to include critical technology, reflecting the increasing interdependencies and linkages between our cyber and technology policy interests.

DFAT invites industry, NGOs, civil society, academia and interested individuals in Australia and overseas, to provide input into the CCTIES through a public call for submissions. Public submissions will form part of a broader program of consultation DFAT will undertake as part of the development of the CCTIES. This will include consultation across the Australian Government; closed consultations with experts and key stakeholders; and the establishment of an Expert Advisory Panel.

Response to Questions

i. 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?

Digital inclusion will be integral for balancing the risks and opportunities that can arise through technological developments and applications in Australia and the Indo-Pacific. Digital inclusion is defined as the capacity for a person to 'access, afford and have the digital ability to connect and use online technologies effectively'.[i] In Australia and the Indo-Pacific, digital inclusion needs to be prioritised to encourage opportunities and mitigate risks between and within diverse populations. For example, in remote Indigenous communities in Australia:

> *Poor understanding of cyber safety, and a lack of mechanisms to address the issues have led some remote communities to reject internet services. However, Aboriginal people, especially within remote areas, experience inequalities and hardships that may be exacerbated if they are not able to access information and services online.*[ii]

A Cyber and Critical Technology International Engagement Strategy needs to facilitate a human rights approach that recognises the importance of digital inclusion to balance the risks and opportunities for diverse populations in Australia and the Indo-Pacific. In particular, there needs to be a recognition that 'cyber safety has a direct relationship with digital inclusion'.[iii]

Clarifying disputed areas of international law. Australia has demonstrated sound leadership in recognising the centrality of international law in regulating the use of cyberspace. Australia is a member of the two fora established by the United Nations General Assembly to discuss responsible state behaviour in cyberspace: an Open Ended Working Group and a sixth Group of Government Experts.

It has been noted elsewhere that while the United Nations group took "a monumental step in recognising the applicability of existing international law in cyberspace, devising how exactly international law is applied to cyberspace, an entirely new domain, is the current conundrum."[iv] Australia should continue to lead in clarifying disputed areas of international law. In cyber engagement, as with all areas of the law, Australia should be committed to openness and transparency of the law and the fair application of underlying principles. In applying, in the case of warfare, Australia should continue to affirm the importance of the four fundamental principles of necessity, proportionality, distinction and humanity.

Recommendation:

- A Cyber and Critical Technology International Engagement Strategy needs to facilitate a human rights approach that recognises the importance of digital inclusion to balance the risks and opportunities for diverse populations in Australia and the Indo-Pacific. In particular, there needs to be a recognition that cyber safety has a direct relationship with digital inclusion.
- Australia should continue to lead in clarifying disputed areas of international law relevant to cyber law. In cyber rules and principles, as with all areas of the law, Australia should be committed to openness and transparency of the law and the fair application of underlying principles. In the case of cyber warfare, Australia should continue to affirm the importance of the four fundamental principles of necessity, proportionality, distinction, and humanity.

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

Application of international law. Cyberspace and critical technologies are changing interactions between states in a range of areas, including in the context of national, regional and global security. Unchecked, these changes will shape the strategic and geopolitical environment in the way that suits those who develop the technologies first or who are prepared to use them aggressively. Discussions to date have sought to clarify or develop rules of international law as they apply to cyber activities. Such discussions have occurred in non-governmental expert processes, such as those leading up to the Tallinn Manuals on the application of international law to cyber operations, as well as inter-state fora, particularly the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, and the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security.

Citizen's Perspectives. The ability of governments to position themselves strategically and respond to cyber security threats will be significantly enhanced or impeded by how citizens perceive these issues. Citizens' perspectives are in turn based on their understanding of these issues, their cultural values, the types of technologies being implemented, and the transparency through which they are communicated. Decision-makers can build trust and incorporate these critical perspectives into policy and strategy through collaborative approaches and engagement with diverse stakeholders.

Cyberspace. Overall, cyberspace will continue to develop as an increasingly important site of inter-state competition. It will not alone increase that competition, however, existing and future strategic challenges are increasingly likely to possess a digital component.

- **More flash points** - Interaction in cyberspace between states increases the number of contact points in the international system and thus potential flash-points.
- **Pervasiveness -** Competition in cyberspace is a consequence of the increasing scope and importance of, and ease of access to, computers and networks. This is the result of the wider trend of digitalisation, which has led to the integration of computers and computer networks into an increasing range of human actives. In consequence, cyberspace cannot be constituted as a separate domain of the strategic environment but instead overlays the entire existing strategic environment as a consequence of its digitalisation.
- **Continuity -** Competition in cyberspace will not alter strategic or geopolitical dynamics themselves, however events within cyberspace may have wider effects on these dynamics.
- **Compression -** The rapid transfer of data and information enabled by cyberspace has altered the relationship of action to time and space. In consequence, the strategic environment will become less geographically constrained and new nodes of interaction may develop not based on physical proximity.
- **Digital Actors -** Cyberspace may empower some non-state actors by reducing constraints on interaction, however major actors such as states are likely to retain considerable advantages in cyberspace too due to more effective coordination, stronger innovation, and greater resource investment.
- **Instability -** Rapid digitalisation may have destabilising effects on developing societies in Australia's near region due to poorer social cohesion and low governance capacity.

These societies may also be at risk from the online exploitation of existing social fractures.

Critical Technologies. A wide range of emerging technologies have the potential to alter international strategic dynamics including: machine learning, automation, hypersonics, improved space access. Many of these technologies will behave synergistically with cyberspace and one another, to produce potentially unforeseen applications and outcomes.

- **Supply Chains -** Technologies such as automation and additive manufacturing may alter global supply chains and potentially reduce the importance of manufacturing in low-wage countries. These global supply chains are a major driver of the geo-economic environment.
- **Regulation -** As with cyberspace there may be considerable first-mover advantage in many critical technologies. Furthermore, the potential benefits from emerging technologies may encourage some states to undermine international regulation in order to seek commercial and strategic advantage (e.g. the behaviour of China in stem cell research)

Fourth Industrial Revolution & Weaponisation of Information. For the past decade, data breaches have been among the most dangerous cyberspace risks in the international geopolitical environment. However, the Fourth Industrial Revolution (4IR), where technology more closely integrates the cyber and physical world, the risks are only starting to be realised. Furthermore, 'weaponisation' of information enabled by technology and wielded almost instantaneously in cyberspace is quickly becoming a formidable threat.[v] Cybercrime, cyberterrorism, and cyberwarfare – while each may stem from different intents, they can have the same devastating effects for both intended and unintended victims. Growing complexity of digital value chains makes data, infrastructure, applications, and people all exposed to risks.

Key risks include:

- **Ransomware attacks on the Internet of Things (IoT).** Where hackers encrypt victim data and demand payment for the encryption key. As more industries incorporate IoT technologies, vulnerabilities increase exponentially and could go far beyond financial loss to even human fatalities due to compromised transportation and medical equipment.
- **Compromised blockchain systems & cryptojacking.** Blockchain has surpassed its original purpose within the cryptocurrency markets. Vulnerabilities such as weak encryption, hashing, and poor key management could lead to data breaches, fraud, and loss of funds. Cryptojacking in hijacking computers by infecting them with malware that gives the attacker use of the victim's hardware, thus reducing digital system performance while the attackers mine cryptocurrency.
- **Privatised cyber warfare affecting trades and industries.** Not only nation states, but also privatised cyber warfare using mercenary hacking organizations. Effects include communication disruption or denial where loss of connectivity significantly affects organizations at multiple levels, from national to local.

The cyber security realm should be considered an 'irregular warfare' domain where asymmetric threats can produce strategic outcomes.[vi] Australia has significant recent lessons learned from the current COVID-19 pandemic and should incorporate these in creating strategies and plans for addressing the above risks.

Recommendation:

- As cyberspace and the implementation of critical technologies have influence well beyond defence and geopolitics, citizens' perspectives must be systematically incorporated into decision-making.
- Australia should address the risks posed by *inter alia* ransomware attacks on the IoT, compromised blockchain systems, cryptojacking, and privatised cyber warfare through the development of a world leading national program to include:
    - Information risk assessment, management and mitigation strategies
    - Auditing security controls
    - Continuous Information Security operations
    - Continuity of operations plans and procedures for critical infrastructure and technologies
    - Crisis management and incident response processes
    - Cyber resilience programs
    - Data pseudonymisation and encryption

iii. 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?

Space. The shrinking cost of commercial and private access to space, and accompanying development of cubesats and nano-satellites has the potential to impact the strategic landscape in several important ways. Examples include the recently launched SpaceX Starlink broadband service which realise a transnational direct-to-user internet service, raising questions about sovereign capability to regulate internet traffic; increased accessibility of space technologies lowering barriers for nations to develop and deploy earth observing and signals intelligence platforms; and the potential for space-based cryptocurrency platforms to create alternative payment platforms outside any national jurisdiction. Australia must invest in national and international legal, regulatory, governance and diplomatic efforts to understand the impacts of these emerging platforms and shape global norms on their use.

Deepfakes. The rapid and evolving developments in the use of AI and machine learning technologies for creating so-called 'deepfakes' – photorealistic but faked images and videos, raises fundamental questions about integrity and trust in the media, and particularly social media. There is genuine potential for plausible fakes to undermine trust in democratic institutions, particularly in less stable nations in the Indo-Pacific. Australia can respond with research into data provenance, attribution and detection technologies, technologies and platforms for establishing chains of trust in media and digital content, and regulatory and diplomatic efforts in establishing and adhering to international norms.

Bots and campaigns. Related to this is the rise of botnets and fake social media accounts used to sow political and social uncertainty and unrest is rising. For example, recent statistics show that as many as 7.3% of COVID-19 news in Italy are online fake news[vii], and the presence of troll/bot accounts controlled by unknown actors is stoking misinformation and fear around Australian COVID-19 policies. Australia can respond with research into the automated detection and identification of such networks, and continued engagement with social media platforms on regulatory responses.

"New IP" proposal for "Network 2030" to the ITU-T. A proposal for a new Internet architecture was recently made by China and Huawei to ITU-T to address the need to support heterogeneous networks (called "ManyNets"), the need to support "more types of devices into the future network."; the need to support Deterministic Forwarding; the need to enhance security and trust and support "Intrinsic Security"; and the ability to support ultra-high throughput and allow user-defined customised request for network services and get fine-grained information on the status of the network. The internet is critical to the lives and livelihoods of Australia society and enterprise, and it is critical that Australia participates and plays an active role in these discussions to engage a global conversation.

Across these emerging issues, Australia can and must maintain strong engagement, share resources and training, and influence regional democracies to understand these risks and how to adopt proactive responses.

Recommendation:

- Australia must invest in national and international legal, regulatory, governance and diplomatic efforts to understand the impacts of emerging space-based platforms and shape global norms on their use.
- Australia can contribute productively through research into data provenance, attribution and detection technologies, technologies and platforms for establishing chains of trust in media and digital content, and regulatory and diplomatic efforts in establishing and adhering to international norms.
- Australia can contribute productively through research into the automated detection and identification of botnet and fake social media account networks, and continue engagement with social media platforms on regulatory responses.
- Australia should continue to participate actively in discussions on new internet architecture to engage a global conversation.
- Australia must invest in national and international legal, regulatory, governance and diplomatic efforts to understand the impacts of these emerging space-based platforms and shape global norms on their use.

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

Centres of Excellence. There are three avenues that we highlight for Australia to consider in pursuing its cyber and technology interests internationally. Our suggestions relate to the local region of influence for Australia being the broader Indo-Pacific region. These suggestions consider how to attract cyber security talent to the region, how to improve cyber resilience and governance in government and business, and how to improve societal resilience in the face of online opinion influencing and misrepresentation campaigns.

The first avenue we highlight is for Australia to bolster both Australia's and the region's technical and business capabilities in addressing and ensuring cyber resilience. We envisage that this can be achieved by attracting cyber security talent to Australia. This suggestion focusses on developing Cyber Security and Critical Technology 'Centres of Excellence' in Australia that partner with key stakeholders throughout the region.

It is likely that this activity could be undertaken in collaboration with existing agencies and institutions in the context of attracting cyber talent and expertise to the region. The 'Centres of Excellence' would ensure cyber capabilities in Australia and the region by providing a pool of talent upon which Australia can draw in addressing incidents as they become critical. Furthermore, this talent could provide educational programs and specific professional advice to build cyber resilience in the region.

By partnering with stakeholders, Australia could support the training and development of cyber experts and policy makers in the region. If, after some period of time in Australia, those experts return to their home countries then the region benefits with strong skills, capabilities, and an appreciation of the broader regional context. This avenue is considered to operate in connection with the suggestion of improving cyber resilience and governance in government and business discussed below.

Educational programs in decision-making. The second avenue that we highlight is for Australia to encourage the development of educational programs in decision-making around cyber and critical technology interests (at the strategic, management, and operational levels) in the Indo-Pacific region to encourage the development of cyber resilience in government and businesses throughout the region. This suggestion focusses on programs that develop cyber governance capabilities in government and business to deliver long-term cyber resilience across the region.

It is apparent that some decisions – particularly relating to critical technology infrastructure – are made from a management (i.e. cost-focussed) rather than a strategic (i.e. long-term relationships) perspective. The development of cyber resilience requires programs focussed on achieving a high level of maturity in the decision-making frameworks and accountabilities in decisions relating to cyber and critical technologies (i.e. cyber governance).

Amongst other aspects, these programs provide education around the development of structures, processes, and relational mechanisms that ensure good decision making and operational responses. In targeted areas of specific expertise, in addition to educational services, these programs might also provide relevant specific professional advice on building cyber governance maturity and, optionally, critical technology infrastructure. It is considered important that this suggestion encompass both governmental and business organisations as frequently the private sector acts as a service provider or advisor in building critical technology infrastructure. This suggestion is considered to partner with the suggestion of attracting cyber security talent to the region as discussed above.

Societal resilience. The third avenue that we highlight is that Australia encourage societal resilience by developing and integrating programs that bolster political and societal resilience in the wake of coordinated electronic misinformation programs. The focus of this suggestion is upon developing partnering programs with key stakeholders to embed critical thinking and a general civil scepticism regarding information presented online.

Misinformation campaigns (aka 'Fake News') are online programs and coordinated cyber attacks intended to influence the social discourse and, often, to weaken trust in democratic institutions. Such programs are at best confusing for the populace, and at worst can result in hate crimes, unprovoked attacks, or misinformed civil unrest. This suggestion aims to create a general uplift of society in the region, and can be cost-effective against cyber attacks. An increasingly frequent feature of such attacks (for example, the recent #DCBLACKOUT social media event on Twitter or COVID-19 misinformation campaigns) is the use of social media 'bots' that amplify and distract the users of these social media platforms.

'Template' Public Education Programs. This suggestion envisages the development of template public education programs that provide users across the region with tools, tips and techniques to identify 'Fake News' and the questions to consider in evaluating the news they receive by social media. These templates can operate in combination with professional training services to train key service providers throughout the region. These providers can then provide training to local citizens to improve critical thinking and evaluation skills. As part of this program it is possible that Australia could support an independent fact-checking website resource, which provides verifiable curated resources that stakeholders can use. In this way, the effect of misinformation campaigns can be reduced somewhat and social discourse can be undertaken in a better-informed, more contextual, and robust manner.

International Legal Frameworks. Australia should continue to promote discussion, negotiation and clarification of the international legal frameworks regulating the use of cyber and critical technologies. Australia should continue to encourage exchanges of views between states – and between experts within the private sector, civil society and academia – on how particular rules and principles of international law apply to state conduct in cyberspace. Where appropriate, Australia should encourage the articulation of new norms on responsible state behaviour in cyberspace.

Australia is one of only a few states that has set out its position on important international legal questions relating to the use of cyberspace, and what behaviour by states is acceptable. Importantly, Australia has explained, *inter alia*, how it understands the prohibition of the use of force in the United Nations Charter to apply in the cyber domain, and that international humanitarian law applies to the conduct of cyber activities.

However, there is much about the legal framework that remains uncertain. For example, the extent to which cyber operations could constitute prohibited breaches of sovereignty, or the way in which medical facilities are protected against malicious cyber operations in time of peace, are unclear.

Australia's international cyber engagement and strategy action plan illustrates its commitment to an open and free internet supported and promoted by multilateral cooperation. Continuing to develop and clarify the law will require careful thought unpinned with rigorous interdisciplinary scholarship that develops a clearer understanding of the legal issues related to sovereignty, attribution and jurisdiction. It will help identify areas of cyberspace regulation that require further attention.

Recommendation:

- Australia should develop Cyber Security and Critical Technology 'Centres of Excellence' within Australia that partner with key stakeholders throughout the region.
- Australia should encourage the development of educational programs in decision-making around cyber and critical technology interests (at the strategic, management, and operational levels) in the Indo-Pacific region to encourage the development of cyber resilience in government and businesses throughout the region.
- Australia should encourage societal resilience by developing and integrating programs that bolster political and societal resilience in the wake of coordinated electronic misinformation programs.
- Australia should develop template public education programs that provide users across the region with tools, tips and techniques to identify 'Fake News' and the questions to consider in evaluating the news they receive by social media.
- Australia should continue to encourage exchanges of views between states – and between experts within the private sector, civil society and academia – on how particular rules and principles of international law apply to state conduct in cyberspace.

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

International education and soft power. Universities are key players in the provision of capability, capacity and innovation. For almost half a century, universities have been internationally engaged through the provision of scholarships, joint research projects, and, delivery of development outcomes through the provision of training, capacity development, technical expertise and advisory services beyond Australia's boundaries. They have been significant actors on the diplomatic stage through the use of "soft power" to build relationships and establish networks of current and future leaders who have been the beneficiary of an Australian education/training or research experience and who may have greater understanding and alignment with Australia's values.

To ensure a comprehensive and complete approach to the fast paced change in cyber and critical technology space there is a need to ensure graduates are equipped with multi-sectoral understanding. A cross-disciplinary approach to education, training and innovation is core. The university sector has already invested heavily in links with academic partners across the globe and expanded the partnering model to industry and government where research and innovation is applied to solving issues and challenges – both current and future. The expansion of engagement models facilitates a transnational approach to the development of and protection against ever-changing cyber and critical technology developments.

Those universities who have solid domestic and international engagement with government, industry, civil society and academic partners will be best placed to ensure the development of future-ready and capable personnel and graduates who are able to respond to the fast paced evolution in the cyber domain. The continued funding of targeting training and professional development of key multi agency personnel from government and industry in our region will underpin the building of regional capabilities and relationships which Australia will be able to draw upon as and when required.

Multi-stakeholder approach. A multi-stakeholder approach is essential for Australia to achieve its cyber objectives. At the same time, this approach has the flexibility to be replicated in other countries, enabling engagement at the regional and international levels. In this scenario, Australia can act as an engagement facilitator, by tapping into a wealth of powerful actors and creating the necessary synergies. Institutions such as the Australian Signals Directorate – Australian Cyber Security Centre, Australian Cyber Emergency Response Team (AusCERT) and the Australian Ambassador for Cyber Affairs represent global-scale best practices on what governments can do in the cybersecurity fight. Universities such as Monash University, the University of Queensland and the Australian National University excel on the international scenario thanks to their course offerings and the research they conduct in the field of cybersecurity. Global industry players such as NTT, Akamai, and Gridware have either a strong presence in, or where developed in, our country. Personalities like Troy Hunt and Dr Tobias Feakin or think-tanks such as the Australian Strategic Policy Institute (ASPI) have promoted the importance of cybersecurity and the need for supporting policies, with implications that stretch beyond our borders. The sheer number of Australia-based institutions, organisations, initiatives, and public figures, which are raising the bar in the cybersecurity environment, demonstrate the gigantic steps forward that our country has made in the last decades.

Such scale has its downsides, however, the most compelling one being the associated coordination costs. In this rich environment, duplication and wastage of resources are a recurring risk, one that Australia has to take particularly seriously, especially in the wake of

the COVID-19 crisis and the ensuing reduction in available resources. To tackle this issue, and ensure cooperation is effective and efficient, agility should be the cornerstone.

How can Australia orchestrate cybersecurity cooperation in an agile way? We propose a 6-step cycle:

1. One or more mapping exercises, organised among relevant stakeholders (e.g., representatives from the institutions and organisations listed above), in order to have a complete understanding of all the cyber-related initiatives and entities currently operating in the country (stakeholder mapping);
2. Through a series of facilitated, **design-led workshops** involving the same actors, co-created activities aimed at ideating innovative ways to ensure efficiency and effectiveness in the coordination of the complex Australian cybersecurity stakeholder scenario;
3. The creation of a **common platform** for 'live' monitoring of cybersecurity initiatives, in order to avoid duplication and to facilitate work and investments on uncovered areas; the platform would act as a one-stop-shop for all cybersecurity needs and resources in the country and could take the form of a digital dashboard, with embedded project and performance management systems, rewards, and a solid component of external/internal communication;
4. The organisation of a series of **road-shows** across the country to publicise the ideas generated in step 2) and the platform constituted in step 3), in order to ensure adequate levels of visibility. In this step, representatives from other countries in the Asia-Pacific region and beyond can be invited to contribute, with a view to scale the initiative to a regional level;
5. **Aggregation of small teams** of representatives from the different stakeholders groups to select the ideas emerged in step 2 that are the most promising and deserve implementation (e.g., investments and other resources); the platform as per step 3) can be utilised to 'vote' the most promising ideas too;
6. **Implementation of the selected ideas** and monitoring of the different projects on the platform as per step 3); review and re-design/re-adjustment then follow, and the cycle can start over, where necessary.

This 6-step cycle can be easily scaled-up to other countries/regions, with Australia playing the role of coordinator and facilitator of the engagement. DFAT's capability building and professional training initiatives can be the vehicle for scaling-up. We believe that this format would ensure the necessary agility for Australia to maximise the value produced by the collaboration among its outstanding stakeholders in the field of cybersecurity.

Strategic Foresight and Scenario Planning. Established methodologies which can support a multi-stakeholder approach include strategic foresight, scenarios and approaches for anticipating change relevant to cyber security. Systems mapping can help to synthesise seemingly divergent points of view and identify how different cyber policy options influence society, the environment, and the economy in many different ways. Such approaches can help to develop well integrated initiatives which provide multiple benefits synergistically and minimise conflict among diverse stakeholder groups. Facilitating a collaborative systems mapping process can help identify how cybersecurity threats, issues, stakeholders, and technologies may impact other issues throughout society. This process can help to synthesise the perspectives of different stakeholders (beyond cybersecurity), and systematically incorporate the impacts of critical technologies beyond defence and geopolitical considerations.

Recommendation:

- Australia should continue funding of targeted training and professional development of key multi-agency personnel from government and industry in our region to underpin the building of regional capabilities and relationships which Australia will be able to draw upon as and when required.
- Australia should adopt an agile, multi-stakeholder approach to ensure efficient and effective collaboration among cybersecurity stakeholders through a 6-step cycle, which could be easily scaled-up to other countries/regions (cycle detailed at Question v.).
- Australia should adopt a collaborative systems mapping approach to identify how cybersecurity threats, issues, stakeholders, and technologies may impact on other issues throughout society. This process can help synthesise the perspectives of a more diverse range of stakeholders and incorporate the impacts of critical technologies in policy formulation, beyond defence and geopolitical considerations.

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

The USA's policy of attracting the best ideas (through basic research funding via the grants of the Army, Air Force and Navy coordinated by their regional office in Japan) for their defence technologies, and Singapore's policy of attracting the best scientific minds to increase its global research impact contributes strongly to their pipeline of innovation. Australia could leverage and adapt such policies to be a centre of gravity for the latest ideas, and pull itself away from its inherent 'tall poppy syndrome' and retain its top talents. With a strong creative and scientific base, it will be able to position itself as an influencer in the emerging technologies space (e.g. space and cyber). Through campaigns and strategic messaging showcasing past Australian successes and innovation (e.g. the birthplace of Wifi, etc.), DFAT can play a key role in positioning Australia as the best place in the world for the best minds and talents from the Indo-Pacific and Western nations to relocate to Australia for great opportunities and lifestyle – leveraging its recent strong reputation in the management of COVID-19.

Recommendation:

- Australia should position itself as the location for the best minds and talent from the Indo-Pacific and Western nations. This can be achieved through campaigns and strategic messaging, showcasing past Australian technological successes and innovations.

Endnotes

[i] Thomas, J, Barraket, J, Wilson, CK, Rennie, E, Ewing, S, MacDonald, T, *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2019*, RMIT University and Swinburne University of Technology, Melbourne, for Telstra, 2019, p. 8.
[ii] Ellie Rennie, Eleanor Hogan & Indigo Holcombe-James, *'Cyber safety in remote Northern Territory Aboriginal communities and towns: summary interim report', Swinburne Institute for Social Research*, Melbourne, 2016, p. 4.
[iii] Ibid.
[iv] Klée Aiken and Jessica Woodall Tallinn, '2.0: Cyberspace and the Law', *The Strategist*, Australian Strategic Policy Institute, 14 May 2015, https://www.aspistrategist.org.au/tallinn-2-0-cyberspace-and-the-law/
[v] Myriam Dunn Cavelty, *Cyber-security and threat politics: US efforts to secure the information age.* (Abingdon: Routledge, 2017).
[vi] Patrick Michael Duggan, 'Strategic Development of Special Warfare in Cyberspace', *Joint Force Quarterly*, 79, 4 (2015); Thomas Rid & Mark Hecker, *War 2.0: Irregular Warfare in the Information Age: Irregular Warfare in the Information Age*, (Westport: Praeger Security, 2019); Frank C. Sanchez, Weilun Lin & Kent Korunka, 'Applying Irregular Warfare Principles to Cyber Warfare', *Joint Force Quarterly*, 92, 1 (2019).
[vii] Daniela Coppola, 'Share of online fake news related to coronavirus (COVID-19) in Italy 2020, *Statistica*, 18 May 2020, https://www.statista.com/statistics/1109490/share-of-coronavirus-fake-news-italy/,