OCSC
Oceania Cyber Security Centre

Cyber and Critical Technology International Engagement Strategy (CCTIES) Submission

Prepared by Dr Carsten Rudolph and Dr James Boorman

June 2020

About the Oceania Cyber Security Centre

The Oceania Cyber Security Centre Ltd (OCSC) is a public company limited by guarantee and owned by 8 Victorian Universities with objectives to:

a) advancing education; and

b) advancing the security of Australia, through encouraging and facilitating the conduct of training, research and other activities focused on identifying and solving the key cyber security issues in Australia.

This submission is submitted on behalf of the Board of directors of the OCSC company and should not be interpreted as reflecting the views of its member universities, individually or collectively.

OCSC's submission provides responses to each of the 6 questions as proposed, and the company gives consent for the submission to be made public.

1. 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?

The key international cyber and critical technology objectives should be to:

1. build sustainable resilience;
2. ensure integrity of information and technology; and
3. strengthen relationships.

This should include consideration of at least:

4. capacity;
5. supply chain;
6. natural disasters and pandemics; and
7. purposive, persistent and incidental attacks.

Fundamentally this should include establishing a region-wide systemic view on cyber security and technology risks and support nations with their individual risk assessments and treatment plans. This is particularly important for digital transformation in developing countries in the Asia-Pacific region. Building a stronger region is important to reduce cyber harm to Australia and our partner countries.

This should include:

- Promote standards and interoperability at scale, beyond just the underlying communication infrastructure (i.e. Internet). Think data, applications, health data, security intelligence, etc.

- Establish an international view on the value of data, in particular around identity information, private and personal information and business data.

- Intellectual property protection, protect technology and technology-enabled innovations from theft, but also from misuse or manipulations. Think knowledge community in a regional and global scale.
- Improved exchange of technology transfers and joint development of new technologies across countries to remove dependencies on any one manufacturer / supplier.

Values should include:

- Security through secure technology and strong controls and not through obscurity and surveillance.
- Collaboration and contextualisation so that different cultures can achieve secure digital transformation that works.
- Promote the use of digital technology for peaceful activities for the benefit of all nations.
- Promote Global Internet Freedom and Global Cyber Safety
- Promote openness of cyberspace and international conventions (e.g. the Budapest Convention)

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

A combination of factors has brought cyberspace and critical technologies in to focus for geopolitical strategies, including: increased connectivity; a strong push for digital transformation to drive economic growth and thus increasing economic dependency; and a shift in defence focus toward cyber and the adoption of emerging technologies for unmanned vehicles.

The increasing complexity of traditional information infrastructure combined with emerging technologies such as Internet of things driven infrastructures, higher connectivity (5G) and the greater reliance on AI-driven services will provide organised, sophisticated and knowledgeable threat actors (e.g. lone wolfs, organised crime, nation-states) with greater leverage against targets (e.g. private enterprise as well as governments) to engage in theft (e.g. intellectual property and trade secrets, customer data) and disruption (IT services, but also cyber-physical systems).

Another important aspect is the growing dependency of democratic processes and politics on digital media. The dissemination of 'fake news' is having an increasing impact. Countries are using cyberspace and technology to enforce their political and economic interests.

Furthermore, cyber systems and critical technology will be the new target for international warfare due to our over dependency on technology to improve quality of life, decision making, facilitate traffic flows and the movement of goods. Hence, we need to build resilient self-healing systems and infrastructure that can deal with cyber-attacks and natural disasters.

Australia should take a strong role in leading the way to bridge digital divides between various countries and economies in the region in a way that does not exclude parts of the region, ignores national interests (even of very small nations) and targets stability of the region.

Start-ups / innovation paired with research and development will be key to move Australia from a commodity-based economy to a resilient technology hub in the pacific region. Australia can provide services, become a computation and data storage site as our relative political stability means Australia can safely house sensitive systems and data, as long as Australian laws enable to establish strong trust in technology providers.

3. 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?

Artificial intelligence, machine learning, big data paired with access to an increasing array of data sources brings many opportunities for Australia and the Indo-Pacific. Some examples include:

- efficient farming and opening of international markets for small farmers;
- better control of fishing;
- employment opportunities for people affected by climate change;
- international collaborations;
- enable disadvantaged people to participate in digital development; and
- efficient use (and production) of energy.

Innovation in wearable technologies and medical health devices are examples for opportunities particularly for Australian businesses to explore.

Increasingly fine-grained datasets are being generated from: sensors; social media; banking and financial services; health-based services; and transport & logistics services. These datasets can be analysed using computational methods to 'connect the dots' across multiple contexts. The results can be used to drive positive digital transformation or used to predict and manipulate the behaviours and actions of a targeted population.

Key risks include:

- additional dependencies for Australia's economy.
- creating new digital divides.
- increasing the attack surface for many critical areas to potentially be exploited by criminals, state-based actors and other threat actors.
- technology advancements in drones and autonomous weapons.
- cloud based services based offshore and consolidation of supply chains.
- AI decision-based systems with humans not in the loop.
- dissemination of misinformation and disinformation/ information to undermine trust and confidence in democratic institutions and processes.
- misuse of surveillance technologies, especially by authoritarian countries, but also undermining trust in governments in democratic countries.

Even if Australia manages to be well-protected against cybersecurity and technology risks, exploiting weaknesses in other nations critical infrastructures, businesses, banking, government networks or supply chains, will impact all economies in the region.

Balancing risks and opportunities require stronger regulation and development/enforcement of strict quality standards that mitigate the risk of critical vulnerabilities emerging from flaws in engineering.
Minimising risks requires Australia to build and sustain cyber security capacity and support weaker economies to do the same. Further, Australia should promote the use of secure technologies. Sometimes, it might be necessary to slow down digital development in order for security to keep up.

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

Australia should work with our allies to develop international treaties, legislation, regulation and law enforcement with cross-jurisdictional powers to safeguard our interests and prevent proliferation of disinformation.

Australia should continue to support countries in the region in building cybersecurity capacity with a focus on tangible results. Projects should be evidence-based and enable countries to build up their own strong capabilities in risk assessment, security monitoring, exchange of threat intelligence, incident response and resilience.

One long-term goal should be the establishment of a framework for international collaboration in cybersecurity. This can include the identification of functions that can be delivered on a collaborative international level without compromising national sovereignty.

Standards for open networks, data exchange, security controls, exchange of security intelligence and threat information and norms for processes such as for nation-level risk assessment should be actively pursued.

To strengthen Australia's place in the region, it should also support equal opportunities in cyberspace by leading and contributing to the forming and shaping of international norms and regulations regarding the openness of cyberspace, cyber inequality, cybersecurity and cyber ethics. International cyber normalisation of laws to remove jurisdictional boundaries to enable better investigations of modern slavery, human trafficking, paedophilia, cyber enabled scams and organised crime.

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

- Fund strategic programs, build on existing expertise in academia, industry and civil society, be transparent about funding programs and enable independent co-ordination of activities in the region.
- Develop a strategy and in parallel match it with different national interest and regional co-ordination bodies.
- For new technologies promoted in the region, enable systemic risk assessment covering dependencies and conflicting interests.
- Foster international cybersecurity research activities with active researchers in different regions, East-Asia, Pacific Islands, etc. These can develop new solutions (that work across different cultures and economical and political models) and strengthen relations between the countries on different levels (similar to elements of European collaborative research framework programs).
- Build mechanisms for open threat intelligence exchange.

- Fund Australian organisations to participate in international co-ordination activities, such as GFCE, UN-based activities, FIRST, etc. This can strengthen Australia's position in the international community and creates synergies with strong benefits for Australia's own international cybersecurity programs.
- International cybersecurity exercises, critical infrastructure exercises, etc. can be useful.
- Australia should partner with other countries to promote Cyber Security Awareness. Australia (and New Zealand) have a particular duty to assist the South Pacific, perhaps there are joint initiatives and programs they can jointly set up to assist those countries in the South Pacific.
- Better incorporate experts from various disciplines. For example, scientists and social scientists, to ensure that both technical and behavioural issues are addressed. Diverse teams are needed.
- Establish research funding at a state level with a central register overseen by ACSC / Defence with an industry council. Funding should be open to any university and Australian industry partner.

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

- EU's ENISA works across Europe and has developed an international strategy. ENISA also has developed guides for national strategies, runs exercises, develops recommendations and standards for different sectors etc.
- Non-government institutions (e.g. East West Institute) have played a strong role in regional initiatives.
- The Organisation of American States is quite active in South America and Middle America to drive cybersecurity capacity building.
- The Global Forum on Cyber Expertise provides an international forum to connect countries, funder, researcher and implementer. Further, they have established a forum to collect exiting material for national cyber security capacity building.
- UK is a good example and some areas of the USA regarding DOD cyber credentials under DoD Directives 8570 and 8140.