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

Dr Brett van Niekerk[1] and Dr Trishana Ramluckan[2]

[1.] vanniekerkb@ukzn.ac.za, School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal, Westville, South Africa

[2.] ramluckant@ukzn.ac.za, School of Law, University of KwaZulu-Natal, Durban, South Africa

Overview of the authors:

Dr Brett van Niekerk is a computer science academic at the University of KwaZulu-Natal. He serves as chair for the International Federation of Information Processing (IFIP) Working Group 9.10 on ICT Uses in Peace and War and the co-Editor-in-Chief of the *International Journal of Cyber Warfare and Terrorism*, associate editor for the *International Journal of Information Security and Privacy*, on the international advisory board for the *Journal of Information Warfare*, and for a term as the Academic Relations Director on the ISACA South Africa board (2016-2018). He participated in the international research advisory group for the Global Commission on the Stability of Cyberspace, and is a reviewer for policy proposals for the Carnegie Endowment's Partnership for Countering Influence Operations. He has over 50 peer-reviewed publications (book chapters, journal articles and conference papers) and has made over 20 presentations at industry or professional conferences and events. In 2012 he graduated with his PhD focusing on information operations, information security and critical infrastructure protection. He worked at Transnet as a senior information security analyst, and is a Certified Information Security Manager.

Trishana Ramluckan has been an academic and researcher in the IT and governance fields for the past 12 years. She is currently a Postdoctoral Researcher in the College of Law and Management Studies at the University of KwaZulu-Natal. She participated in the international research advisory group for the Global Commission on the Stability of Cyberspace, and is a member of the IFIP working group on ICT Uses in Peace and War, the Institute of Information Technology Professionals South Africa and serves as an Academic Advocate for ISACA and a reviewer for multiple journals and conferences. In 2017 she graduated with a Doctor of Administration specialising in IT and Public Governance. Her current research areas include Cyber Law and Information Technology Governance.

What are the values and principles Australia should promote regarding cyberspace and critical technology?

Values and principles should include:

- The protection of human rights;
- The promotion of societal advancement;
- The promotion of peace, international security and stability through the use of technology; and,
- The promotion of stability and security of the technology and infrastructure itself at national, regional, and global levels.

The latter two points can be facilitated by strengthening the cyber security ability in collaboration with allies and partners in deterring and the provision of legal recourse to address those who use cyber tools for malicious purposes.

The documents presented below will provide some detail on these values and principles.

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

The use of cyberspace in international crime and in geopolitical tensions has been increasing. Since the COVID-19 pandemic, there has been a significant increase in cyber-attacks and online disinformation / influence operations. There have been examples of kinetic attacks in retaliation to persistent cyber-attacks, cyber-attacks in response to kinetic attacks, and state cyber-attacks against critical infrastructure of other nations. There has also been tensions regarding the use of 5G technology from certain countries. It is therefore likely that cyberspace and related technologies will continue to have a growing impact on geopolitical and strategic contexts. This will result in increasing uncertainty given there is unpredictability regarding the application of international law and cyberspace. There are also limited models of how cyber-operations will influence international relations; indicating that cyber-operations may play a significant role in escalating tensions between states (for example see Ben Buchanan, *The Cybersecurity Dilemma*).

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

A risk management approach should be used for the implementation of critical technologies. For example, points to consider include:

- Are there any known or suspected vulnerabilities with the technology?
- Is the technology produced in another country?
- Should there be intentional vulnerabilities that could affect the confidentiality, integrity or availability of the technology or data related to it, would there be a major impact on critical infrastructure, or would there be a breach of sensitive or personal information?
- Would there be any adverse reaction by other nations in choosing a specific vendor or product?

Similarly, a risk management approach with a pre-defined set of questions can be used as a guide to implementing cyber-operations, or responding to incoming cyber-attacks. An important question in this case is: are Australian Laws aligned to International Laws on cyber security?

An important aspect to position Australia is to provide support other nations, in particular those that are developing or middle-income that are lagging behind in their technological maturity. This can be support in the form of skills to aid the implementation of cyber-security facilities and legislation, or collaboration and funding of tertiary education research to grow a skills base. This will strengthen the country in question, creating a mutually beneficial situation for collaboration in securing cyber-space and responding to incidents.

Australia should actively seek to have representation at the various international fora relating to cyberspace and critical technology. Whilst there is no doubt Australia does contribute to many of these, there are possible initiatives that may not always be apparent to national governments that could be of benefit to, or benefit from, Australia's participation.

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

A number of initiatives can be implemented to foster cooperation:

- A ministerial advisory council with representatives from government, industry, civil society and academia;
- The implementation of a national expertise register, where members of government, industry, civil society and academia can verify their skills and be listed as experts to be called for collaboration to support one another;
- An accreditation and funding scheme for tertiary education and research to recognise the best instructions for research and educational programmes; and,
- A national conference including government, industry, civil society and academia participation.

The ministerial advisory council can be sounding board the for policy development, and can aid in regulation and internal sustainability management, with the experts on the register being the first point of call for input on drafts before opening for public comment. The facilitation of national conferences can be an important feedback mechanism to the relevant communities of practice on policies, regulatory matters, and other significant events or projects. The accreditation and funding scheme will allow for the interaction of experts in the various sectors to engage with the next generation, providing for long-term sustainability of the initiatives.

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

NGO / regional / international organisation documents that can used to guide the strategy include:

- The Global Commission on the Stability of Cyberspace Final Report (https://cyberstability.org/report/)
- The *Paris Call for Trust and Security in Cyberspace* (https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433.pdf)
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant reports
- The *Tallinn Manual* and *Tallinn Manual 2.0*
- The Budapest Convention (The Convention on Cybercrime of the Council of Europe (CETS No.185))
- The AU Convention on Cyber Security and Personal Data Protection
- The SADC Model Law on Computer Crime and Cybercrime

National documents that can be used to inform the strategy include:

- Letter of 5 July 2019 from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace; Appendix: International law in cyberspace (https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf)

- The French perspective on International Law Applied to Operations in Cyberspace (2019) (https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf)
- Cyber Security Strategy for Germany
- National Cyber Strategy of the United States of America (2018)
- The South African Electronic Communications and Transactions Act (Act 25 of 2002)
- The South African Cybercrimes Bill (Bill)
- The South African Protection of Personal Information Act (Act)
- The South African National Cybersecurity Policy Framework
- The South African Terms of Reference for the National Cybersecurity Advisory Council (https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/NCAC-ToR-2017-Reappointment_V1.pdf)