Cyber and Critical Technology International Engagement Strategy (CCTIES)

SSIT submission to DFAT Cyber Engagement Strategy

The following submission has been prepared by members of the IEEE Society on Social Implications of Technology (SSIT) in Australia. IEEE is the world's largest technology professional association, with 420,000 members in 161 countries. Founded in 1972, SSIT is the unit within IEEE which addresses the relationship between technology and society. SSIT Australia was formed in 2005 and has members in all states.

SSIT appreciates the opportunity to contribute to this review. We note

Overarching values and principles

> 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?

SSIT Australia is dedicated towards safe, trusted and secure cyber and online environments as important areas of human endeavour. These should be the bedrock for Australia's cyber and online engagement.

The importance of cyberspace has been startlingly illustrated in recent months with the transfer of a significant part of global human activity online, in a matter of weeks, due to Covid-19. Trust, safety, and security are essential for human flourishing in the physical world and it is clear that these are also essential values to be advanced in cyber and online environments. In working towards this we see many areas of overlay with cybersecurity. SSIT both in Australia and internationally has been working for several years on means to place a high value on safe, trusted and secure cyber and online environments. We are actively engaged in the IEEE Standards Association's Digital Inclusion, Identity, Trust and Agency program (https://standards.ieee.org/industry-connections/diita/index.html). SSIT Australia members actively promote discussion on security issues, including Professor Katina Michael's Social Implications of National Security, which held its 13th session in Arizona this year: http://www.katinamichael.com/sins20/.

Risks and Opportunities for Australia and the Indo-Pacific

> 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?

One of the substantial concerns that SSIT Australia identifies in Australia's current cyber and online environments engagement is the World Bank ID4D identity program. This program, supported by the UK Government, the French Government, the Australian Government and the Omidyar Network alongside Bill & Melinda Gates Foundation has as its core aim the facilitation of social inclusion; especially for women through the development of a secure and trusted digital identity systems. This is a tremendous opportunity for cyber and online

environments to provide positives for some of the most disadvantaged peoples and communities in the Indo-Pacific.

However, such programs also bring inherent risks. Strategies of discrimination, harassment and genocide have been greatly assisted by large-scale identity programs, supported by what today is very simple technology. For example the German census of 1933 and the colonial-Belgian population registration of Rwanda were used inform genocide. It is imperative that such programs must begin from a perspective of human safety, not convenience. This includes a design ensuring that effective risk assessment is undertaken, and that appropriate governance exists. For example, an identity program introduced into a country without the possibility of judicial oversight has a significant likelihood of providing an oppressive, rather than inclusive, outcome. Similarly there may be cause for concern as this program introduced into the Philippines (https://id4d.worldbank.org/peer-to-peer) a country with a record of extrajudicial killings (https://www.hrw.org/world-report/2019/country-chapters/philippines).

Cooperative approaches

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

In the executive summary of the current *Australia's International Cyber Engagement Strategy,* there is a commitment to 'advocate for multi-stakeholder Internet governance.' SSIT Australian strongly supports this commitment to a multi-stakeholder governance arrangement for the Internet as the most public and populated digital environment. While there has been many controversies over the governance structure for the Internet, at the present it seems to be the best way to ensure civil society engagement. An example of this is the recent decision by the Internet Committee for Assigning Names and Numbers (ICANN) to keep the management of the highly important '.org' in civil society hands. Commentators have welcomed this as a contribution to maintaining trust in the Internet.

Best Practice Approaches to Cyber and Online Environment Policy

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

SSIT is part of IEEE, which has 420,000 members in 160 countries. A cross-IEEE review found no support for weakening the protection of information flows. In particular IEEE is concerned with well-intentioned attempts to reduce security protocols:

> IEEE supports the use of unfettered strong encryption to protect confidentiality and integrity of data and communications. We oppose efforts by governments to restrict the use of strong encryption and/or to mandate exceptional access mechanisms such as 'backdoors' or 'key escrow schemes' in order to facilitate government access to encrypted data. Governments have legitimate law enforcement and national security interests. IEEE believes that mandating the intentional creation of backdoors or escrow schemes — no matter how well intentioned — does not serve those interests well and will lead to the creation of vulnerabilities that would result

in unforeseen effects as well as some predictable negative consequences. https://globalpolicy.ieee.org/new-ieee-position-statement-supports-strong-encryption-for-confidentiality-and-data-integrity/

Authors

Greg Adamson, Kieran Tranter, Kayleen Manwaring