

16 June 2020

Department of Foreign Affairs and Trade
By email: CyberAffairs@dfat.gov.au.

CCTIES

About us

The Allens Hub for Technology, Law and Innovation ('the Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law, the Allens Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society, and the broader community. More information about the Allens Hub can be found at <http://www.allenshub.unsw.edu.au/>. For this submission, we have partnered with Andrew Ray, Bridie Adams and Charlotte Michalowski, law students from the ANU College of Law and researchers at the National Judicial College of Australia, and Kate Renehan, a graduate from the ANU College of Law.

About this Submission

Our submission is not intended as a comprehensive response to all the issues in the inquiry, but rather focuses on topics on which our research can shed light. We thus limit our submission to the following issues:

- **Question 1:** Need for integrated approach
- **Questions 2 and 3:** Political misinformation, Internet of Things, telecommunications infrastructure
- **Question 4:** Engagement with inter-governmental organisations
- **Question 5:** Map of legal and regulatory framework for cyber security in Australia

Our submissions reflect our views as researchers and are not an institutional position.

Question 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?

We stress the importance of embedding any approach to cyber and critical technology within the broader international agenda, in particular the international development agenda. While critical infrastructure like the Coral Sea Cable (CSC) dramatically improves internet access in Papua New

A joint initiative of

Allens > < Linklaters



Guinea and the Solomon Islands, the full economic and social possibilities offered by the cable cannot be achieved without investment in the human capital and basic resources of both nations. For example, while improved internet access has the potential to transform the delivery of education and health services, this potential can only be realised with adequate numbers of trained medical staff and teachers and availability of medications and classroom resources.

Questions 2 and 3 – How will technology shape international strategic environment? / Risks and opportunities

Use of technology to spread political misinformation

The challenge in relation to political misinformation is the interaction among recent technological developments, the behaviour of particular states, and weak protections for data and cyber security. Differential ranking in search results/newsfeeds, for example by Google or Facebook,¹ the use of data and machine-learning analytics, the use of bots to amplify political opinions, and the creation of “deep fakes” are allowing actors to sway voters and public opinion in non-transparent ways.² For example, Extinction Rebellion Belgium released a fake video of Prime Minister Sophie Wilmès linking the COVID-19 pandemic with environmental damage and calling for urgent action on climate change.³ This is occurring within a context of increasing foreign interference in elections, most notably in the United States.⁴ Foreign state and non-state actors may be able to spread election-altering misinformation from outside a target jurisdiction in ways that are hard to monitor, in order to achieve a strategic objective or goal. As such, the need for a co-ordinated regional (and global) response should not be understated, particularly given the unclear application of international law to this issue.⁵

Internet of Things, Big Data and Network Security Risks

One trend of growing importance within the Indo-Pacific and the Asia-Pacific is the increased growth in the Internet of Things (‘IoT’).⁶ IoT has the potential to alter city design, how services are delivered to citizens, and how people interact with each other.⁷ IoT uptake is linked to other developments, such as improved network connectivity through 5G (increasing the strategic importance of telecommunications infrastructure as discussed below). While proponents of this technology emphasise the potential benefits to urban planning and city design as well as to increasing

¹ These companies were chosen purely by way of example given their reach, there is no indication that Google or Facebook alter their results in order to influence elections – as their algorithms are confidential.

² See, eg, the development and increasing use of deepfake technology: Supasorn Suwajanakorn et al, ‘Synthesizing Obama: Learning Lip Sync from Audio’ (2017) 36(4) *ACM Transactions on Graphics* 951; Yuezun Li et al, ‘In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking’ (2018) (advance) <<https://arxiv.org/pdf/1806.02877.pdf>>. See also generally Allens Hub for Technology, Law and Innovation, Queensland University of Technology: Datafication and Automation of Human Life and the Society on Social Implications of Technology, Submission No 19 to Senate Select Committee on Foreign Interference through Social Media, Parliament of Australia, *Foreign Interference Through Social Media* (3 April 2020) (‘Foreign Interference Submission’).

³ XR Belgium, ‘The truth about COVID-19 and the ecological crises – a speech for Sophie Wilmès’ (online, April 2020) <<https://tube.rebellion.global/videos/watch/2ad12b6b-bb53-473c-ad74-14eef02874b5?title=0&warningTitle=0>>.

⁴ Office of the Director of National Intelligence, ‘Assessing Russian Activities and Intentions in Recent US Elections’ (Declassified Report, 6 January 2017) <<https://apps.washingtonpost.com/g/documents/national/read-the-declassified-report-on-russian-interference-in-the-us-election/2433/>>.

⁵ Foreign Interference Submission (n 4).

⁶ James Henderson, ‘Is Asia leading the way in IoT?’, *CIO Australia* (online, 19 July 2019) <<https://www.cio.com/article/3410043/is-asia-leading-the-way-in-iot.html>>.

⁷ See, eg, Andrew Zanella et al, ‘Internet of Things for Smart Cities’ (2014) 1(1) *Internet of Things Journal* 22.

productivity,⁸ there remains a need for governments to protect individuals from privacy and security risks. Privacy and consumer laws in some countries within the Indo-Pacific region will likely need to be updated to better protect individuals' data (especially where they cannot opt-out – as in the case of smart cities). Additionally, the gathering of large datasets about entire populations (as facilitated by IoT) poses significant security risks, as these datasets would be valuable to adverse state and non-state actors, including for manipulating elections.⁹ It is also important to note that the public and private interests in IoT differ, with significant human rights implications in the case of governments using data gleaned from smart cities to surveil citizens or to manage/control their behaviour.

Preserving Security in Cyberspace by Ensuring Appropriate Telecommunications Infrastructure

In the context of infrastructure, DFAT's current international engagement strategic framework is largely reactive in nature because it seeks to protect the integrity of *existing* telecommunications infrastructure. An alternative is to advocate for and implement new telecommunications infrastructure projects. To achieve an 'open, free and secure' cyberspace over the long-term, DFAT should develop a response to the substantial investments that are being placed in the construction and operation of a digital silk road spanning from the Indo-Pacific to Africa and Europe. Those investments are being realised by vendors which are currently classified as high-risk by Australia's national security agencies.¹⁰ Such vendors may be constructing network-capabilities with backdoors which may be used by particular state actors to conduct espionage, gather and control large quantities of data, and interfere with critical and sensitive infrastructure networks.¹¹

Some developing nations, particularly in the Pacific, which 'sign-on' to such projects, may not be in a position to evaluate associated cyber risks.¹² DFAT has already taken some action by facilitating consortiums to prevent both the funding of undersea cables and takeovers of telecommunications companies in developing nations by high-risk vendors.¹³ However, it has not developed a substantial aid or trade initiative which proactively ensures that telecommunications projects, such as the creation of 5G networks, are financed by telecommunications providers that have strict internal accountability measures and respect and adhere to the principle of an 'open, free and secure' cyberspace.

Financing under the recent Framework Agreement on Cyber and Cyber-Enabled Critical Technology Cooperation can be extended in the near future to support Australian and Indian businesses to manufacture and develop telecommunications infrastructure capabilities.¹⁴ India produces two

⁸ In an Australian context, some reports suggest that IoT uptake could lift productivity in the order of 2% per annum: PricewaterhouseCoopers, 'Australia's IoT Opportunity: Driving Future Growth' (Report, September 2018) <<https://www.pwc.com.au/consulting/assets/publications/acs-pwc-iot-report-web.pdf>>.

⁹ This increased risk occurs alongside a rise in the use of ransomware attacks to target both private and public computer systems, through simple phishing attacks aimed at low-security access points to a network (such as individual users' email accounts), the rise of IoT will increase the number of access points to a network increasing the potential vulnerabilities that must be secured.

¹⁰ Hanna Barczyk, 'Different Views of AI Fuel Distrust between China and America', *The Economist* (online), 16 January 2020 <<https://www.economist.com/china/2020/01/16/different-views-of-ai-fuel-distrust-between-china-and-america>>.

¹¹ Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (PublicAffairs, 1st ed, 2016).

¹² Standards Australia, 'Pacific Islands Cyber Security Standards Cooperation Agenda' (Research Discussion Paper, Standards Australia, January 2020) 7.

¹³ Department of Foreign Affairs and Trade, *The Coral Sea Cable System: Supporting the Future Digital Economies of Papua New Guinea and the Solomon Islands* (September 2018) Department of Foreign Affairs and Trade <<https://www.dfat.gov.au/sites/default/files/supporting-the-future-digital-economies-of-papua-new-guinea-and-solomon-islands.pdf>>.

¹⁴ Rohit Yadav, India and Australia Collaborated for Cyber and Critical Technology (5 June 2020) *Analytics India Magazine* <<https://analyticsindiamag.com/india-and-australia-collaborated-for-cyber-and-critical-technology/>>.

million tonnes of e-waste every year which can be reengineered to provide for the development of comparatively cheap 5G equipment particularly because 5G projects only need small receivers.¹⁵ This can provide a long-term industrial base for investment in integrated telecommunications hardware and equipment. These can be integrated with smart city, disaster management and structured project financing development initiatives and in turn provide alternative options for countries which would otherwise feel compelled to be locked into arrangements with service providers that may be high-risk. Given that Finnish researchers at the University of Oulu acknowledge that the emergence of 6G by around 2030 will need to build upon already-constructed 5G infrastructure, the projects that are implemented over the medium term will have significant ramifications for the security and prosperity of the Indo-Pacific and Australia's place within it.¹⁶

Digicel and critical infrastructure in PNG

Given the private nature of much technological infrastructure and investment, consideration must be given to whole of economy factors and ownership structures. We draw the Department's attention to the recent bankruptcy of Digicel, the virtual monopoly player in the PNG (and Pacific) mobile market. Digicel's privately funded infrastructure includes over 100 cell phone towers across PNG, the maintenance of which was challenging and costly. Digicel's collapse raises two potential negative outcomes, from security and developmental perspective. In the first, any investor that purchases Digicel's PNG assets immediately secures access to large amounts of important, and potentially security-related, data from our immediate neighbour. In the second, commercial decisions may result in the Digicel infrastructure no longer being maintained as a result of any transfer of ownership, limiting access to Australia's significant strategic investment in the CSC. Given the considerable cost of tower maintenance in PNG and the Solomon Islands, investors may decide to concentrate their attentions in less remote or volatile areas, with negative consequences for many of those most in need.

Critical infrastructure must be understood to include infrastructure privately built, owned, and maintained. Given the extraordinary wealth of information that can be extracted from call detail records, access to or control of mobile services in strategically important countries should similarly be treated as a national security consideration. We suggest that the collapse of Digicel represents an opportunity for the Australian government to support innovative ownership arrangements for critical private infrastructure in the Pacific, including but not limited to community owned and maintained towers. At a minimum, the Australian government should be promoting a robust mobile market in the Pacific, to ensure that our Pacific neighbours have access to competitive pricing. This would also limit the capacity for any single service provider to hold exclusive or monopoly access to CDR in any given mobile market.

The Digicel collapse also reinforces Australian interest in well-functioning data security laws within the Pacific. This body of law is presently undeveloped and, should a foreign interest secure ownership of the near-monopoly mobile provider in the Pacific, represents an immediate national security risk. Australia should be actively involved in the proper development of such laws across the region.

¹⁵ Jinoy Jose, 5G May Worsen India's Electronic Waste Mess (11 October 2019) *The Hindu Business Line* <<https://www.thehindubusinessline.com/opinion/5g-may-worsen-indias-electronic-waste-mess/article29594474.ece>>.

¹⁶ Matti Latva-aho and Kari Leppänen, 'Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence' (Research White Paper, University of Oulu Faculty of Information Technology and Electrical Engineering, Communications Engineering, 9 September 2019).

The Use of Export Controls to Regulate Cyber Surveillance Technologies

Since the early 2010s, many international observers and scholars have suggested that ‘high-risk vendors’, as designated by Australian security agencies,¹⁷ may be intercepting encrypted communications and utilising cell data, including financial and security information, to assist particular regimes in regions such as Africa with the surveillance of political opposition forces.¹⁸ Law enforcement and national security agencies across the Indo-Pacific region may increasingly utilise data, through cutting-edge ICT means such as facial recognition technology, and employ advanced surveillance techniques to monitor and suppress political dissent.¹⁹ The troubling impact of state-led cyber surveillance is not always territorially contained, but can easily spill over internationally. Such a ‘spill-over’ may engender the furtherance of emerging norms which counterpose Australia’s commitment to an ‘open, free and secure cyberspace’, including new technical standards that align product development with state-directed priorities and necessitate compliance with government surveillance policies. These developments are also likely to constrain fundamental human rights such as the right to privacy, freedom of expression and political association as outlined in the International Covenant on Civil and Political Rights.²⁰

It is well accepted that imposing export restrictions is one of the few options available to regulate the availability and spread of cyber surveillance tools.²¹ DFAT should collaborate with Australia’s key international partners to facilitate the proper control of cyber surveillance technology, especially given recent developments with respect to the Wassenaar Arrangement regarding certain types of surveillance goods and technologies.²² Australia can also utilise international and regional forums to encourage other like-minded states to embrace its current approach to the domestic implementation of the Wassenaar Arrangement. One of the potential regulatory takes on this issue is to restrain the end-use of surveillance items for specific purposes such as the facilitation of internal repression or terrorist activity. A key limitation for DFAT in obtaining sufficient international and regional support from Wassenaar Participating States in this regard is the growing preference for some actors such as the United States to pursue isolationist policies and protectionist mechanisms rather than multilateral arrangements as means to address sensitive international policy problems.²³ Even if DFAT were to secure such support, there is a material likelihood that particular states with an increasingly neo-mercantilist approach may impose unilateral counter-regulatory actions or economically punitive responses to any export restrictions if they interpret those controls as a political manoeuvre against their interests.²⁴ This in turn may contribute to a

¹⁷ Australian Signals Directorate, *Cyber Supply Chain Risk Management Practitioner Guide* (June 2019) Australian Signals Directorate <<https://www.cyber.gov.au/publications/cyber-supply-chain-risk-management-practitioner-guide>>.

¹⁸ Steven Feldstein, *The Global Expansion of AI Surveillance* (September 2019) Carnegie Endowment for International Peace <<https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>>.

¹⁹ Justin Sherman, *The Troubling Rise of Facial Recognition Technology in Democracies* (April 2020) World Politics Review <<https://www.worldpoliticsreview.com/articles/28707/the-troubling-rise-of-ai-facial-recognition-technology-in-democracies>>.

²⁰ *International Covenant on Civil and Political Rights*, opened for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17, art 19 and art 22.

²¹ Heejin Kim, ‘Global Export Controls of Cyber Surveillance Technology – The Wassenaar Arrangement and the Disrupted Triangular Dialogue’ (2020) unpublished work (file with authors); Peri Meyers, ‘Wassenaar Nations Set New Export Controls’ (2020) 50 *Arms Controls Today* 34.

²² Australia has participated in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, the multilateral export control mechanism comprising 42 states.

²³ Patrick Homan, *The Battle for U.S. Foreign Policy: Congress, Parties and Factions in the 21st Century* (Palgrave Macmillan, 1st ed, 2020) Chapter 7.

²⁴ Paolo Guerrieri and Pier Carlo Padoan, ‘Neomercantilism and International Economic Stability’ (1986) 40 *International Organisation* 29, 42.

recent trend of retaliatory approaches by particular states, in response to the utilisation of soft law mechanisms by Australia during the COVID-19 pandemic, which have harmed Australia's economy.²⁵

Recent International Data Sharing Agreement Proposals

We refer DFAT to our recent submission on the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020*.²⁶ It outlines our concerns regarding how data should be managed and secured under future international data sharing agreements.

Question 4 – Opportunities for Australia

Engagement with inter-governmental organisations

There is capacity for Australia to engage more extensively with inter-governmental organisations in the field of cyber and critical technology (CCT). This is an under-developed area, and Australia can advocate for more regional collaboration regarding new and emerging threats. By way of example, there was a discussion during the First Committee (Disarmament and International Security) of the United Nations General Assembly about CCT and how best to tackle cybercrime. There are two working groups considering various measures and attempting to find consensus on these issues. Yet, in the 2019 session of the First Committee, only three resolutions were considered concerning technology, cyber and telecommunications. This is broadly indicative of the international community's reluctance to give new and emerging threats in the area of cyber the same attention as more traditional security threats.

Secondly, we note that DFAT has provided funding to Pulse Lab Jakarta since 2014. The Lab is a cooperative enterprise between the United Nations and BAPPENAS, the Indonesian National Planning Ministry. The recently commenced second phase of the Lab's development has seen the arrival of new staff, a deepening of the technical expertise hosted at the Lab and strengthened relations with BAPPENAS. Given the returns DFAT's relatively modest investment has generated, we encourage the Department to promote Australia's ongoing engagement with the UNGP project. We particularly commend investment co-sponsored by host-government agencies. We draw the Department's attention to a request made by the Government of Samoa for a Pacific-region lab, based in Apia. Support for a Pacific Pulse Lab would represent meaningful investment in a strategically important area. We further recommend supporting increased engagement between Australian research organisations and the Pulse Lab network, providing Australian organisations access to difficult-to-research areas.

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

There are already several ways in which such co-operation is occurring. We focus here on one, which we are developing with colleagues at the University of Melbourne, following seed funding from the Cyber Security Co-operative Research Centre. One challenge in the context of international cyber security policy is a lack of understanding, internationally, about Australian law in this area. An example of this lack of understanding is the map created by Bundesverband der Deutschen Industrie (BDI) and

²⁵ Daniel Hurst, 'Why has China slapped tariffs on Australian barley and what can Australia do about it?', *The Guardian* (online) 20 May 2020 <<https://www.theguardian.com/business/2020/may/20/why-has-china-slapped-tariffs-on-australian-barley-and-what-can-australia-do-about-it>>.

²⁶ Genna Churches, Michael Murdocca, Monika Zalnieriute and Lyria Bennett-Moses, 'Review of the Effectiveness of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020' (Submission to the Parliamentary Joint Committee on Intelligence and Security, Allens Hub for Technology, Law and Innovation, 30 April 2020) <<https://www.allenshub.unsw.edu.au/sites/default/files/inline-files/PJICIS%20Cloud%20Act%20Framework%20submission%20-%20Allens%20Hub.pdf>>.

Deloitte showing that Australia has ‘no dedicated cyber security law’.²⁷ The misunderstanding arises because, while Australia has no piece of legislation dedicated solely to cyber security, it has a range of laws with similar effect that operate in areas such as critical infrastructure protection, criminal law, telecommunications regulation, privacy, and consumer law. We hope to collaborate in the creation of a map of Australian laws that impact on cyber security and cyber resilience, to be made available via the web, in order to both a) enhance national and international understanding of Australian law in this area and b) build a community of experts and practitioners in this area familiar with developments in adjacent cyber law. This development will assist Australia’s ability to contribute at an international level as governance moves forward in this area.

This is an example of the benefits of collaboration with universities and research institutions. We would encourage DFAT to collaborate with, share information with, and support Australian universities and universities in the region within the Cyber Cooperation Program.

Yours sincerely,

Lyria Bennett Moses, Caroline Compton, Michael Murdocca, Heejin Kim

Andrew Ray, Bridie Adams, Kate Renehan, Charlotte Michalowski

Disclosure: Since 2018, Caroline Compton has been working on a research project which examines operations of Pulse Lab. The research has involved working closely with Lab members.

²⁷ The Federation of German Industries, ‘Cyber-Landscape I: Cyber Security Laws’ (Interactive Map) <<https://english.bdi.eu/topics/global-issues/cyber-landscapes/#/article/news/cyber-security-laws/>>.