Promoting Prosperity and Providing Protection: Australia's International Cyber Engagement Strategy

Damien Spry

INTRODUCTION

The launch of Australia's International Cyber Engagement Strategy (the Strategy)[1] in October 2017 followed the appointment of that nation's first Ambassador for Cyber Affairs, Dr Tobias Feakin, in early 2017 and updates and expands upon the 2016 Cyber Security Strategy – a flurry of activity reflecting the role that digital networks increasingly play in Australian international relations, trade and investment, and security and strategic concerns. This chapter discusses the Strategy, its priorities and progress to date, in the context of Australian foreign policy, with an emphasis on cyber security, governance and cooperation, and human rights and democracy online.

Australia's Strategy is partly a response to current developments and partly a consequence of persistent geo-strategic realities. Australian foreign policy is based on three pillars[2]: the security alliance with the United States, including the 1951 ANZUS Treaty; the pragmatic (if at times wavering) commitment to middle-power multilateralism through international and including regional institutions; and a deepening, broadening economic and cultural connectivity with the Asia-Pacific (or Indo-Pacific) region. These foreign policy pillars, and the 2017 Foreign Policy White Paper which is the most recent expression of how Australia pursues its security and prosperity in contemporary circumstances, are the essential background for understanding and evaluating the Strategy.

[1] Commonwealth of Australia, Department of Foreign Affairs and Trade (DFAT), *Australia's International Cyber Engagement Strategy* (October 2017), accessed 20 July 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html.

[2] Allan Gyngell, *Fear of Abandonment: Australia in the World since 1942* (Carlton: La Trobe University Press, 2017).

Australia is, and has been since colonial days, highly dependent on international networks of capital, trade, people and information. This outward-looking global connectivity remains a source of Australia’s prosperity and enriches the country culturally. However, these connections are also potential pathways for unwelcome or malevolent actors. Thus, the Strategy seeks to enhance Australia’s advantageous participation in global markets and governance, including through support for the technological and multi-stakeholder governance systems that underwrite the Internet, while protecting Australia from those same systems’ apparent risks and emerging threats.

Australia’s place in the Asia-Pacific means the Strategy must include and prioritise engagement in a region that is large and diverse – from micro-states in the Pacific to continental powerhouses – as well as being dynamic, turbulent, and potentially dangerous. The re-emergence of China as a global power is the dominant feature of this region’s trading and security landscape. For Australia, this is keenly felt: for the first time in its history, Australia’s major trading partner, China, is an authoritarian state while Australia’s major security partner, the United States, is China’s strategic rival. Cyber security, including cyber warfare, and the threat of malicious interference with national political systems, have prompted legislative responses in Australia and rank high among national security priorities. China’s use of digital means of surveillance and control is also at odds with Australia’s commitment to a free and open internet. Other nations, notably Cambodia and Myanmar, are similarly exploiting online methods of state control that place democracy and human rights at risk. Non-state actors, from terrorist networks to growing cybercriminal threats, pose increasingly alarming risks for Australia and her partners in the region.

In its Strategy, Australia has outlined how it perceives these risks, threats and opportunities, as well as how it will address them. This paper situates Australia’s Strategy in these contexts, outlining the rationale for its approach. It also charts some of its progress to date by considering programs and achievements from the first year of its implementation.

THE STRATEGY AND ITS CONTEXTS

The Strategy is structured around eight related themes: digital trade; cyber security; cybercrime; international security and cyberspace; internet governance and cooperation; human rights and democracy online; technology for development; and comprehensive and coordinated cyber affairs. Each of these themes contains a key goal and a number of related aims (see Table 1).

Table 1: Australia's Cyber Engagement Strategy: Themes, goals, aims.

Theme	Goal	Aims
Digital trade	Maximise the opportunity for economic growth and prosperity through international trade	Shape an enabling environment for digital trade, including through trade agreements, harmonisation of standards, and implementation of trade facilitation measures Promote trade and investment opportunities for Australian digital goods and services
Cyber security	A strong and resilient cyber security posture for Australia, the Indo-Pacific and the global community	Maintain strong cyber security relationships with international partners Encourage innovative cyber security solutions and deliver world leading cyber security advice Develop regional cyber security capability Promote Australia's cyber security industry
Cybercrime	Stronger cybercrime prevention, prosecution and cooperation, with a particular focus on the Indo-Pacific	Raise cybercrime awareness in the Indo-Pacific Assist Indo-Pacific countries to strengthen their cybercrime legislation Deliver cybercrime law enforcement and prosecution capacity building in the Indo-Pacific Enhance diplomatic dialogue and international information sharing on cybercrime
International security and cyberspace	A stable and peaceful online environment	Set clear expectations for state behaviour in cyberspace Implement practical confidence building measures to prevent conflict Deter and respond to unacceptable behaviour in cyberspace
Internet governance and cooperation	An open, free and secure Internet, achieved through a multi-stakeholder approach to Internet governance and cooperation	Advocate for a multi-stakeholder approach to Internet governance that is inclusive, consensus-based, transparent and accountable Oppose efforts to bring the management of the Internet under government control Raise awareness across the Indo-Pacific of Internet governance issues and encourage engagement of regional partners in Internet governance and cooperation discussions
Human rights and democracy online	Human rights apply online as they do offline	Advocate for the protection of human rights and democratic principles online Support international efforts to promote and protect human rights online Ensure respect for and protection of human rights and democratic principles online are considered in all Australian aid projects with digital technology components

Technology for development	Digital technologies are used to achieve sustainable development and inclusive economic growth in the Indo-Pacific	Improve connectivity and access to the Internet across the Indo-Pacific, in collaboration with international organisations, regional governments and the private sector Encourage the use of resilient development-enabling technologies for e-governance and the digital delivery of services Support entrepreneurship, digital skills and integration into the global marketplace
Comprehensive and coordinated cyber affairs	Australia pursues a comprehensive and coordinated cyber affairs agenda	Enhance understanding of Australia's comprehensive cyber affairs agenda Increase funding for Australia's international cyber engagement activities Coordinate and prioritise Australia's international cyber engagement activities

The strategy is in part an expression of how Australia's traditional interests have been transformed by the inexorable rise of digital communications technologies. This is certainly evident in the sections that discuss the importance of international trade and the support for digital industries, including cyber security but extended to encompass the digitalisation of all aspects of commerce, trade and investment. This aligns with Australian moves to diversify its economy, itself a response to the decline of manufacturing and growth in service industries like international education and tourism, and takes advantage of new tech-related opportunities. These sections of the Strategy that promote trade and global governance are therefore logical extensions of pre-existing, largely bi-partisan and long-standing Australian policies that favour and promote the systems of global governance and market conditions that underpin international engagement in trade and investment and bring these up-to-date bearing in mind new opportunities and risks arising out of digitalisation.

The strategy is more noteworthy as an expression of new confluences of national and international, especially regional, interests that arise out of new kinds of security threats associated with digital communications networks. National security interests are traditionally predicated on Australia's close relationship with powerful friends and allies as well as good relations with neighbours. In this Strategy, they are placed in a new context, one that is characterised by the rise of new types of risk and from a wider variety of international actors, using electronic networks that make borders, and thus security, less easily secured.

The security risks the Strategy seeks to confront are three-fold: criminals, operating for profit; non-state actors, motivated by ideological or political interests, including terrorist organisations and similarly motivated individuals; and foreign states seeking to infiltrate, interfere or threaten national institutions and democratic processes. According to reports from security agencies, affected companies and the Australian Government, concerns about such threats are rising. For example, in May 2018 Australian Security Intelligence Organisation (ASIO) Chief Duncan Lewis described the threat of foreign interference as being at "An unprecedented scale"[3]. In November 2018 the Australian Cyber Security Centre (ACSC) and Austal, an Australian shipbuilder and defence contractor supplying the Australian, American and Omani navies, announced a hacker had stolen personnel information and (non-sensitive) ship drawings in an extortion attempt[4].

Australian Government efforts to address such threats include the reorganisation of the intelligence community, including placing the Australian Signals Directorate (ASD) with its offensive cyber capabilities into the Defence portfolio[5], and the introduction of new laws that specifically address foreign interference. In his speech introducing the legislation to parliament, the then Prime Minister Malcolm Turnbull underscored the cyber threat – "The very technology that was designed to bring us together, the internet, is being used as an instrument of division"[6] – and named China and Russia as countries of concern. China in particular has also been identified as involved in cyber espionage, often targeting the intellectual property of companies supplying Australia's defence forces. China was reportedly behind cyberattacks on the Australian National University in 2018 and Australia's Bureau of Meteorology as far back as 2015[7]. And Chinese telecommunications giant Huawei has twice had bids rejected by Australian governments because of concerns about security, the most recent being the effective banning of Huawei from Australia's 5G

[3] Bevan Shields, "ASIO chief Duncan Lewis sounds fresh alarm over foreign interference threat," *The Sydney Morning Herald,* 24 May 2018, accessed 2 November 2018, https://www.smh.com.au/politics/federal/asio-chief-duncan-lewis-sounds-fresh-alarm-over-foreign-interference-threat-20180524-p4zhdk.html.

[4] Brett Worthington, "Explainer: Here's what you need to know about Austal cyber attack and extortion attempt," Australian Broadcasting Corporation News, 1 November 2018, accessed 2 November 2018, https://www.abc.net.au/news/2018-11-02/austal-ship-cyber-attack-and-extortion-attempt-national-security/10458982.

[5] Patrick Walters, "Spies, China and Megabytes: Inside the overhaul of Australia's intelligence agencies," *Australian Foreign Affairs 4* (2018).

[6] Malcolm Turnbull, "Second Reading: National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017," accessed 1 November 2018, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22chamber/hansardr/716f5e71-dee3-40a3-9385-653e048de81b/0193%22.

[7] Patrick Walters, "Spies, China and Megabytes: Inside the overhaul of Australia's intelligence agencies," *Australian Foreign Affairs 4* (2018).

network due to the likelihood that it could be required, under Article 7 of China's 2017 National Intelligence Law, to secretly collaborate with Chinese intelligence services[8].

For its own part, Australia's hands are not entirely clean when it comes to the use of cyber espionage capabilities. Past allegations include spying on then Indonesian President Susilo Bambang Yudhoyono, his wife and other senior officials in 2009[9], bugging the Timorese Cabinet offices during negotiations over a maritime boundary in 2004[10], and monitoring mining giant Rio Tinto's negotiations with a Chinese bank during the 2008 financial crisis[11]. Despite these indiscretions, Australia has positioned itself as a trusted partner.

The rising threat to security, whether from criminals, terrorists or countries, is the context for the Strategy and helps explain its sense of urgency and thoroughness. However, the Strategy's emphasis is less on naming cyber attackers – China is included as a potential partner, its statements in support of agreements against cyber theft highlighted – and more on the role that Australia can play in promoting and assisting with cyber security in Asia and especially the Pacific. The logic is clear: under-resourced Pacific Island Nations may prove a weak link in the chain of security required to keep the internet safe. Australia can and in its own interest should address this as a matter of national security, as well as a matter of international diplomacy and development.

CYBER SECURITY, CYBER CRIME, AND INTERNATIONAL SECURITY IN CYBERSPACE

These three closely interconnected themes are the areas where the Strategy is at its most innovative and internationally connected – a measure of how the issues

[8] Danielle Cave, "Huawei highlights China's expansion dilemma: espionage or profit," *The Strategist*, 15 June 2018, accessed 25 October 2018, https://www.aspistrategist.org.au/huawei-highlights-chinas-expansion-dilemma-espionage-or-profit/.

[9] Michelle Grattan, "Phone spying rocks Australian-Indonesian relationship," *The Conversation,* 18 November 2013, accessed 25 October 2018, https://theconversation.com/phone-spying-rocks-australian-indonesian-relationship-20445.

[10] Jonathon Pearlman, "Spy row a threat to Australia's ties with Timor-Leste," *The Straits Times*, 15 August 2018, accessed 25 October 2018, https://www.straitstimes.com/asia/se-asia/spy-row-a-threat-to-australias-ties-with-timor-leste.

[11] Angus Grigg and Lisa Murray, "Revealed: How Australian spooks 'spied' on Rio during 2008 debt crisis," *Australian Financial Review,* 25 July 2018, accessed 25 October 2018, https://www.afr.com/news/policy/foreign-affairs/revealed-six-governments-on-rio-tintos-it-network-during-2008-debt-crisis-20180725-h134my.

around crime and security are prompting significant transformations in approaches, resourcing and relationships.

Australia defines cyber security as “measures relating to the confidentiality, availability and integrity of information that is processed, stored and communication by electronic or similar means”, and nominates it as “the foundation for the achievement of Australia’s entire cyber affairs agenda”[12]. The fundamental elements of this theme and its goal and aims speak to the core of the entire strategy, firstly in outlining the seriousness of the threat and the consequent need for robust and resilient responses, and secondly in the intrinsic interconnections between national, regional and global actions required.

Australia’s strategic response to cyber threats, therefore, is a combination of robust domestic defensive – and offensive – capabilities and a forward-defence through international engagement. Australia’s cyber security efforts are in concordance with their overall security and strategic positions in that, more than the other themes, they are related to the alliance with the US and the close relationships with their fellow members of the “Five Eyes” intelligence sharing network. The ANZUS Treaty is affirmed in the Strategy[13] as applying to cyberattacks. Since April 2016, Australia has acknowledged that it has an offensive cyber capability and in November 2016, Australia’s then Prime Minister Malcolm Turnbull confirmed that these offensive capabilities were used to target the Islamic State. In 2017, Australia became the first nation to disclose that its offensive cyber capabilities would be directed at “organised offshore cyber criminals”[14].

Australia’s international engagement prioritises the Asia-Pacific because that is where it has identified threats and vulnerabilities but also because that is where it can have the greatest impact. As with Australia’s aid programs, the closer to home, the more engaged Australia is. Papua New Guinea (PNG), a growing, resource-rich nation with considerable social and political challenges separated from Australia at its closest point by a mere five kilometre stretch of water, is a clear priority. Australia has already committed AU$14.4 million (US$10.4 million) for an advanced cyber

[12] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia’s International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html, p. 23.

[13] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia’s International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html, p. 47.

[14] Fergus Hanson and Tom Uren, *Policy Brief: Australia’s Offensive Cyber Capability* (Australia Strategic Policy Institute, 2018), accessed 30 October 2018, https://www.aspi.org.au/report/australias-offensive-cyber-capability.

security package for PNG (encompassing technical, policy and training elements, and the establishment of a cyber security operations centre) as part of its focus on cyber-resilience in the Pacific through its Cyber Cooperation Program (CCP)[15].

Elsewhere in the Pacific, Australia is also supporting the Solomon Islands to establish a cyber security operations centre, and Vanuatu and Tonga to establish national Computer Emergency Response Teams, and has assisted Tonga to develop stronger cybercrime laws, a model approach to more robust legislation for other countries in the region.

More widely, throughout the Asia-Pacific, the CCP includes support for the Asia-Pacific Network Information Centre (APNIC), the Forum of Incident Response and Security Teams (FIRST) to provide cyber security training, including incident response training across the Pacific, and the Pacific Cyber Security Operational Network (PaCSON), launched in April 2018[16], comprised of government-designated cyber security incident response officials, which shares information, tools, techniques and ideas. The Australian Cyber Security Centre was re-elected as Chair of the Asia-Pacific Computer Emergency Response Team (APCERT) Steering Committee in Shanghai in October 2018[17], indicating Australia's commitment to, and the region's acceptance of, its leadership in Asian cyber security.

At the ASEAN Regional Forum in August 2017, with Malaysia, Australia co-sponsored a proposal to establish a cyber Point of Contact database to facilitate communication in times of crisis – one of the Strategy's goals – and will pilot the concept in 2018-19. In August 2018, Australia and Indonesia signed a Memorandum of Understanding, with an associated Action Plan, regarding cooperation over the next two years. A Cyber Capability Engagement Program, which has provided training to 20 Indonesian government officials in partnership with the Australian National University's National Security College, is already underway[18]. The ASD's

[15] Information provided by email from DFAT.

[16] Sara Barker, "The Pacific Cyber Security Operational Network is now in action," 14 May 2018, accessed 1 November 2018, https://securitybrief.com.au/story/pacific-cyber-security-operational-network-now-action.

[17] Australian Government: Australian Signals Directorate, "Australia maintains a key role in international cyber security community," accessed 2 November 2018, https://cyber.gov.au/about-this-site/media-newsroom/aus-role-in-cyber/.

[18] Information provided by email from DFAT.

Essential Eight[19], a checklist of strategies to mitigate cyber risks, is scheduled for translation into the ten official ASEAN languages.

Beyond the Asia-Pacific, Australia has established key working-level partnerships to confront cybercrime. The Five Eyes Cyber Crime Working Group shares best practices and operational resources and an Australian Criminal Intelligence Commission (ACIC) Cybercrime Analyst is posted at the FBI International Cyber Crime Coordination Cell in the United States. Another is posted at the National Cybercrime Unit at the United Kingdom's National Crime Authority[20]. Diplomatically, Australia participated in coordinated action to protest unacceptable behaviour by North Korea WannaCry ransomware (December 2017) and Russia (*inter alia,* US Democratic National Committee email hack, 2016 NotPetya malware, February 2018; and cyber operations against the Organisation for the Prohibition of Chemical Weapons[21] and the investigations in the Malaysian Airlines plane shot down in the Ukraine, October 2018[22]). Australia also works closely with the International Telecommunications Union (ITU) and is at the time of writing standing for re-election to the ITU council.

Australia's approach to cyber security demonstrates a combination of international cooperation through leadership and modelling responsible practice, and a capacity and robust willingness to confront threats.

[19] Australian Government: Australian Signals Directorate, "Essential Eight explained" (March 2018), accessed 30 October 2018, https://acsc.gov.au/publications/protect/essential-eight-explained.htm.

[20] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html, pp. 42-3.

[21] https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog.

[22] Senator the Hon Marise Payne, Minister for Foreign Affairs, and The Hon Scott Morrison, Prime Minister, "Attribution of a pattern of malicious cyber activity to Russia," *Media Release*, 4 October 2018, accessed 4 November 2018, https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181004.aspx; additional information provided by email from DFAT.

Table 2: Main Australian and international agencies, networks and programs addressing cyber security/cybercrime.

Agencies	Role
Australian agencies	
Australian Criminal Intelligence Commission (ACIC)	Australia's national criminal intelligence agency.
Australian Cyber Security Centre (ACSC)	Coordinates cyber security capabilities across the Australian Government. Engages with international partner organisations to share threat information, to cooperate on operational responses to major incidents and to work collaboratively on best practice mitigations. Run by the ASD.
Australian Federal Police (AFP)	Australia's Federal police force, with major emphases on counter terrorism and national security, and interagency cooperation on transnational crime.
Australian Security and Intelligence Organisation (ASIO)	Australia's national security agency responsible for defence against espionage, illegal acts of foreign interference, and terrorism.
Australian Signals Directorate (ASD)	Monitors and intercepts foreign communications. Defends against cyber threats. Conducts offensive (counterterrorism and military) cyber operations.
Computer Emergency Response Team Australia (CERT Australia)	Australia's expert group that handles computer security incidents, now part of the ACSC.
Department of Foreign Affairs and Trade	Australia's government department managing foreign affairs, diplomacy, international trade (through Austrade) and development assistance programs (through AusAID)
International institutions, networks and programs	
Asia Pacific Computer Emergency Response Team (APCERT)	A grouping of leading and national CERTs and Computer Security Incident Response Teams dedicated to the protection of national infrastructure in the Asia Pacific.
Asia Pacific Network Information Centre (APNIC)	The Regional Internet address Registry for the Asia-Pacific region, providing registration services that support the Internet's operation.
Cyber Cooperation Program (CCP)	A program facilitating the development of policies, legislative frameworks and cyber governance institutions to empower Australia's regional partners to safely embrace the benefits of connectivity.
Cyber Security Pacifica (CSP)	Program partnering the AFP with law enforcement agencies in the region to enhance capacity to address cybercrime.
Forum of Incident Response and Security Teams (FIRST)	Network of internet emergency response teams from over 78 countries, promoting cooperation among CERTs through developing and sharing technical information and best practices
Pacific Cyber Security Operational Network (PaCSON)	A network of Pacific governments' technical experts, supported by not-for-profit organisations and academia, with operational cyber security points of contact. Launched April 2018.
"Five Eyes"' network	Intelligence sharing arrangement between Australia, Canada, New Zealand, the United Kingdom and the United States.

HUMAN RIGHTS, DEMOCRACY AND DEVELOPMENT

The human rights and democracy platforms of the Strategy are based on Australia's proclaimed commitment to international human rights standards. It aims to meet its human rights commitments and to promote human rights internationally through advocacy and capacity building. It does this in part through collaboration with the Australian Human Rights Commission, an independent statutory body, and its equivalent national human rights bodies in the region. Australia's engagement with and support for human rights includes participation in the Freedom Online Coalition[23], a network of 30 governments promoting internet freedoms, and the Digital Defenders Partnership[24], which provides emergency funding for human rights defenders who are under threat because of their online activities. A key achievement to date is supporting the Human Rights and Technology Conference in Sydney in July 2018, bringing together ten representatives from ASEAN and Pacific nations. The conference produced an issues paper, with an aim to invite participation and feedback and to publish a final report in 2020 – an indication that this area is one still requiring extensive consultation and leadership.

In this context, the Strategy's approach taken toward human rights online has some weaknesses. Foremost among these is the assertion that "human rights apply online as they do offline"[25] and that democratic debates occurs online "just as it does offline"[26], which occludes – perhaps inadvertently – the specific and new types of threats to human rights because of changes in the techno-social landscape. While making mention of the capacity for governments to use digital means to monitor, harass, intimidate, censor and even persecute citizens (often in the name of national security), the strategy does not adequately consider how information and communications technologies pose additional risks. These risks include, *inter alia*, the potential for Artificial Intelligence and Big Data systems to make discriminatory decisions; the rights of privacy relating to data access, ownership and use; the role of the internet in spreading hate speech and violent extremism; the debate between protection and participation online with respect to child's rights; and the

[23] https://freedomonlinecoalition.com.

[24] https://www.digitaldefenders.org.

[25] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html, p. 64.

[26] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html, p. 65.

labour rights of those involved in the extractive and manufacturing industries that are part of the supply chain for digital devices[27]. Access Now, a digital human rights Non-Governmental Organisation, has directly criticised the Strategy on the basis that the explicit right to privacy is not afforded an adequate level of consideration and connects this to Australian governmental efforts to access private citizens' data in the name of policing efforts and national security[28].

Notable also through omission are sufficient considerations given to the role that the major social network platforms play in undermining human rights and democracy, and what Australia's interventions should be, and should aspire to achieve, in this regard. There are good reasons to believe that engagement with digital media companies, especially Facebook, is desirable and feasible and would promote human rights and democracy in the region. A recent human rights impact assessment of Facebook use in Myanmar, commissioned by Facebook and undertaken by BSR[29], a business consultancy and research network, makes several recommendations as to how the social media platform could address underlying systemic problems which lead to abuses being facilitated by social media in Myanmar and elsewhere, especially in the ASEAN countries. Because of Australia's ongoing engagement with ASEAN on cyber security matters, this is an area in which Australia could provide assistance through advocacy, networking, and provision of expertise and program funding.

Australia's efforts to promote technology for development include the provision of technical expertise and financial resources to improve digital infrastructure and access. Examples of this include fibre-optic submarine cables for Fiji, Samoa and the Republic of Palau and improved mobile phone coverage in the Solomon Islands and Kiribati[30]. Through the Department of Foreign Affairs and Trade's innovationXchange, Australia collaborates with private sector and university partners to identify and develop projects aimed at upskilling populations in the Asia-Pacific, with a focus on young people, women and girls, and people with disabilities.

[27] BSR, "10 Human Rights Priorities for the Information and Communications Technology Sector," 6 December 2017, accessed 1 November 2018, https://www.bsr.org/en/our-insights/primers/10-human-rights-priorities-for-the-ict-sector.

[28] Access Now, "Human rights in the digital era: An international perspective on Australia," accessed 25 October 2018, https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf.

[29] BSR, "Human Rights Impact Assessment: Facebook in Myanmar," October 2018, accessed 5 November 2018, https://newsroom.fb.com/news/2018/11/myanmar-hria/.

[30] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October 2017), accessed 20 July 2018, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html, p. 72.

CONCLUSIONS

The Strategy provides a clear articulation of Australia's priorities, intentions and capabilities. In part, it is an expression of how the country will continue to pursue its national interests in the new techno-social trading and strategic environment. The key pillars of Australian foreign policy, in one sense, have not changed much: the US alliance, its position as a middle-power engaged in and supporting global cooperation through multilateral institutions, and its key relationships in the Asia-Pacific region.

In another sense the Strategy clearly sets out a new purposefulness to Australia's engagement, especially with its near neighbours. Its clarity is also a conscious effort at putting into practice one of its core values: transparency. Together with the 2016 Cyber Security Strategy[31] and successive Foreign Policy White Papers[32], the Strategy explains Australia's intentions and outlines its capabilities in an effort to reduce the risk of miscommunication with, and to encourage greater candidness from, other international actors. This is one of the Strategy's most laudable objectives.

All nations, governments and policies are faced with the conflict between pragmatism versus principles. The strategy has elements of this in the scant attention to privacy rights. The omission of certain state actors as risks – either to their own people (Myanmar, Cambodia) or to other nations (China, Russia) – can be chalked up to diplomatic prudence. And the shortage of due attention given to digital platforms such as Facebook may be a product of timing – the abuses in Myanmar and the risks to democratic processes both being associated with social media only quite recently. These are, however, areas which Australia's Cyber Ambassador and his department may wish to give further attention to.

Despite these slight concerns, Australia's combination of good standing and comparatively hale resources make its leadership feasible, the interconnectedness of the issues at stake makes its engagement necessary. The purposefulness and thoroughness of the Strategy are in large part cause for confidence; its implementation thus far, likewise.

[31] Commonwealth of Australia, Department of the Prime Minister and Cabinet, "Australia's Cyber Security Strategy" (2016), accessed 20 October 2018, https://cybersecuritystrategy.homeaffairs.gov.au.

[32] Commonwealth of Australia, Department of Foreign Affairs and Trade, "2017 Foreign Policy White Paper" (2017), accessed 20 October 2018, https://www.fpwhitepaper.gov.au.

Dr. Damien Spry is a Lecturer in Media and Communications at the University of South Australia and a Visiting Fellow at the Digital Media Research Centre at the Queensland University of Technology. He has previously held academic positions in Hong Kong, Japan, South Korea and the United States of America. His scholarly research focuses on digital media impacts on international politics and diplomacy. He has developed the Facebooking diplomacy database for this purpose. He is a regular contributor to think tanks, including the Lowy Institute and the Australian Strategic Policy Institute, and has consulted for several multinational companies, including Google, Facebook and Amnesty International, as well as to several governments.