16 June 2020

cyberaffairs@dfat.gov.au
Department of Foreign Affairs and Trade
R.G. Casey Building
John McEwen Crescent
Barton ACT 0221 Australia

Australia's Cyber and Critical Technology International Engagement Strategy Submission to the Department of Foreign Affairs and Trade

About us

As Australian university students and graduates working at the intersection of law, technology, and international affairs, we welcome the opportunity to provide input into the Cyber and Critical Technology International Engagement Strategy ('CCTIES').

Joshua Gacutan is a Bachelor of Arts and Bachelor of Laws (Hons I) graduate from Macquarie University. In 2018, Joshua was awarded a New Colombo Plan Scholarship (Hong Kong) from the Department of Foreign Affairs and Trade ('DFAT') to learn about cyber security and technology law and policy in the Indo-Pacific. Joshua is currently a Research Assistant at the Optus Macquarie Cyber Security Hub.

Erin Jory is a final year Bachelor of Arts (Asian History and Political Science) student from the University of Queensland. In 2019, Erin was awarded a Westpac Exchange Scholarship to study international relations and East Asian foreign policy at The University of Hong Kong. Erin is currently the East Asia Fellow at Young Australians in International Affairs.

About our submission

Our submission responds to one of the questions raised in the DFAT's call for views regarding Australia's CCTIES, namely:

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

Our combined experience studying and working in Australia, Thailand, Philippines, Japan, Mainland China, and Hong Kong has informed us that there is a need for greater cooperation and creative partnerships with Australian youth and tertiary students (collectively, 'students') to achieve Australia's international cyber and critical technology interests.

As many Australian students use social media and the Internet to access news and engage in politics, we recommend that students must be educated about international cyber issues, including how social media platforms may be subject to cyber-enabled information operations. Until the International Cyber Engagement Strategy ('ICES') includes partnerships and programs to educate students, Australia will remain susceptible to cyber-enabled information operations aimed to promote false narratives and undermine liberal democracies.

As the federal government's New Colombo Plan ('NCP') has been recognised as a core public diplomacy initiative,[1] we recommend that the ICES must include creative partnerships with NCP Mobility and Scholarship program students and alumni to advance Australia's cyber affairs interests in the Indo-Pacific.[2] If the ICES includes partnerships and programs to educate NCP students about Australia's cyber affairs interests, then this will help promote the ICES's overarching objective of maintaining an open, free, and secure cyberspace.

Our opinions expressed in this submission represent our personal views and experiences and do not reflect the positions of any institutions or organisations we are affiliated with, including their employees or representatives in any way.

Our recommendations

1. Include Australian students as a stakeholder in the ICES separate to 'civil society'.

2. Develop partnerships and programs with government, private sector, and academia to educate Australian students about cyber-enabled information operations, including how and why malicious actors use social media platforms to promote false narratives and undermine liberal democracies.

3. Develop partnerships and programs with DFAT's NCP Secretariat to engage and involve NCP Mobility and Scholarship students and alumni in promoting Australia's cyber affairs interests in the Indo-Pacific.

4. Develop partnerships and programs with DFAT's Australia Awards Scholarships program to educate scholars from Asia about Australia's cyber affairs interests.

The society-wide implications of cyber-enabled information operations

Our submission is grounded on the understanding that cyber-enabled information operations have direct implications for all members of society. While malicious foreign actors do target physical critical infrastructure, today's online information environment has also exacerbated the production of more threats that aim to 'manipulate or disrupt the information foundations of the effective functioning of economic and social systems.[3]

Researchers from Flinders University describe information warfare as 'cognitive' and 'society-centric' as they weaponise information, especially social media to disrupt liberal democratic institutions and values.[4] In the Indo-Pacific, the goal of foreign malicious actors in the society-centric cognitive battlespace is:

> First, to arouse doubt and confusion, to reinforce an adversary's own domestic propaganda campaigns against the utility of the 'western model'; and second, to diminish the moral attractiveness and viability of the western rules-based liberal international order in the Indo-Pacific during a time of Great Power transition.[5]

[1] Australian Government, Foreign Policy White Paper (Department of Foreign Affairs and Trade, 2017).
[2] The Australian Government's New Colombo Plan is comprised of two programs which aim to lift knowledge of the Indo Pacific amongst Australian students: (1) A scholarship program for study of up to one year, in addition to, internships, language training, and mentorships; (2) A mobility grants program for both short and longer-term study, internships, mentorships, practicums and research.
[3] Michael J. Mazarr et al., 'The Emerging Risk of Virtual Societal Warfare' (RAND Corporation, 2019) xii.
[4] Maryanne Kelton, Michael Sullivan, Emily Bienvenue and Zac Rogers, 'Australia, the Utility of Force and the Society-Centric Battlespace' (2019) 95(4) International Affairs 859, 868.
[5] Ibid 870.

Leading Israeli strategy experts, Levite and Shimshoni, note that the social dimension of information warfare has become extreme in the twenty-first century:

> Virtually all the actors now challenging the West – large and small, state and non-state, from al-Qaeda and Hamas to China and Russia – have adopted multifaceted strategies with society at their core.[6]

As foreign cyber-enabled information operations target all members of society, it is important to develop and support public and private partnerships that educate the Australian public about international cyber issues and their societal implications.

We note the Australian Electoral Commission ran a 'stop and consider' campaign to coincide with the federal election in May 2019 to educate the public on how to check the source of electoral communications and information on social media. While this campaign is a good starting point in a public awareness campaign about misinformation, we believe programs in the future must be segmented to different user groups of the Internet.

As we will discuss, Australian students are more likely to use social media platforms to access news and engage in politics than any other age group.[7] This warrants educational outreach programs that are specific to students' online behaviours, especially if Australia wants their voters to make more informed and independent political decisions.

We argue that there is a need for greater cooperation and creative partnerships with Australian students to achieve Australia's international cyber and critical technology interests. As outlined in the Comprehensive and Coordinated Cyber Affairs chapter, the ICES states the importance of collaboration and cooperation with other states, the private sector, civil society, and the research community to advance Australia's cyber affairs agenda. However, the ICES does not envisage how Australia can cooperate and partner with Australian students to achieve the cyber affairs agenda.[8] While repeated references to partner with 'civil society' may extend to include Australian students, we recommend that the ICES must go further to explicitly include actions to increase cooperation and creative partnerships amongst Australian students in Australia's cyber affairs agenda.

The susceptibility of young Australians to manipulated media on social media

In 2019, the Oxford Internet Institute stated that 'the manipulation of public opinion over social media platforms has emerged as a critical threat to public life.'[9] However, there is a widespread lack of awareness of this manipulation.[10] As young Australians increasingly use social media to access news and engage in politics, we recommend that these users must be educated about cyber-enabled information operations, including how malicious actors use social media platforms to promote false narratives and undermine liberal democracies.

---

[6] Ariel E. Levite and Jonothan (Yoni) Shimshoni, 'The Strategic Challenge of Society-Centric Warfare' (2018) 60(6) Global Politics and Strategy 91, 92.
[7] Caroline Fisher, Sora Park, Jee Young Lee, Glen Fuller, Yoonmo Sang, 'Digital News Report: Australia 2019' (News and Media Research Centre, 2019) 95.
[8] There are no references to 'Australian students', 'university students' or 'youth' in any of the ICES's coordinated action points.
[9] Samantha Bradshaw and Phillip Howard, Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, (Oxford Internet Institute and University of Oxford, 2017) 3.
[10] Doteveryone, People, Power and Technology: the 2018 Digital Understanding Report (London, 2018) 6.

Social media platforms have become a primary source of collected and curated news for most Australians, especially those from Generation Y[11] and Generation Z.[12] According to the 2019 University of Canberra Digital News Report, almost half of Generation Z (47%) use Facebook for news, one third (36%) use YouTube and nearly one quarter (23%) use Snapchat.[13] While 43% of Generation Y use Facebook for news, 23% use YouTube, and 6% use Snapchat.[14] In a similar way, many Australian students use social media to engage in local and global activist movements. From #Metoo to #BlackLivesMatter, activists leverage the global and viral reach of social media to organise events with high levels of engagement and amplify voices that might otherwise not be heard.

Social media now comprises more visual content such as images, memes, GIFs, and videos. The Oxford Internet Institute's report on computational propaganda found that in 52 out of the 70 countries studied, cyber troops (defined as 'government or political party actors tasked with manipulating public opinion online') actively created content such as memes, videos, fake news websites, or manipulated media.[15]

In Australia, during the 2019 federal election, actors from Kosovo, Albania, and the Republic of North Macedonia used nationalistic and xenophobic Facebook content to exacerbate social divisions. The four Balkan-administrated Facebook pages[16] amassed a following of 130,000 users and hosted patriotic and agitational memes and a collection of news reports sourced from a single website that specialised in repackaging stolen content from mainstream news outlets. Despite the niche focus of these Facebook pages, some of the posts were shared over 20,000 times.[17]

Commentators have suggested that foreign malicious actors are using more visual forms of disinformation for their unique emotive impact and as it is easier to get away with subversive messages.[18] Research has also suggested that humans are inept at identifying manipulated media.[19] Without any educational programs for Australian students to help them critically identify the more subtle and increasingly visual forms of foreign propaganda, students may be more susceptible to cyber-enabled foreign information operations.

Australia should learn from the responses of other countries that are at the forefront of tackling information operations. For example, since the 2014 Ukrainian revolution, Ukraine has been subject to Russian disinformation operations aimed to delegitimise Ukraine's government. In 2015, Ukraine implemented a 'Learn to Discern' program in its schools to help students better identify misinformation and propaganda. An IREX study of Ukrainian students in Year 8 and 9 who had participated in the program found that students were twice as likely to detect hate speech, and 18% better at identifying misinformation than students that did not participate in the program. The 'Learn to Discern' program has been adopted in other countries such as the United States, Jordan and Indonesia.

---

[11] Persons with a birth year of 1981 to 1996.
[12] Persons with a birth year of 1997 and after; Australian Competition and Consumer Commission, Digital Platforms Inquiry (Final Report, 2019) 51.
[13] Caroline Fisher, Sora Park, Jee Young Lee, Glen Fuller, Yoonmo Sang, 'Digital News Report: Australia 2019' (News and Media Research Centre, 2019) 95.
[14] Ibid.
[15] Samantha Bradshaw and Phillip Howard, Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, (Oxford Internet Institute and University of Oxford, 2017) 3.
[16] 'Australians against Sharia' 'Aussie infidels', 'Stop the Mosque in Melbourne' and 'Stop all Mosque in Narre Warren'.
[17] Michael Workman and Stephen Hutcheon, 'Facebook trolls and scammers from Kosovo are manipulating Australian users' (ABC News, 16 March 2019).
[18] Jennifer Yang Hui, 'The Danger Meme: Countering Visual Disinformation in Asia's Politics' (The Interpreter, 3 April 2020).
[19] Sophia Nightingale, Kimberly Wade and Derrick Watson, 'Can People Identify Original and Manipulated Photos of Real-World Scenes?' (2017) 2(30) Cognitive Research: Principles and Implications 1.

At present, Australia's cyber security initiatives tend to focus on technical solutions, such as data protection and network security. For example, there are concerted efforts between government, industry, and academia to improve STEM education and professions.[20] Such measures, however, only tackle the shortage of cyber security professionals in technical terms and fall short of addressing the societal implications of cyber-enabled information operations.

If Australian students are not educated about the provenance of information on social media and the expertise of the person or groups communicating it, then malicious foreign actors will continue to interfere with Australia's democratic processes. We recommend the development of partnerships and programs to help Australian students navigate an online environment where malicious actors manipulate the information and platforms they interact with.

The same digital literacy arguments have been argued in the Department of Home Affairs' Submission into the Senate Select Committee on Foreign Interference through Social Media:

> The ability to access and critically interact with media, including traditional, internet, and social media, is more important than ever for citizens to make informed decisions. Over the long term, raising media literacy is the most reliable and cost-effective counter to the effects of propaganda and disinformation campaigns.[21]

Australian NCP students in the Indo-Pacific are at the front line of cyber affairs

To advance Australia's interests in the cyberspace, it is must engage and involve NCP Mobility and Scholarship program students and alumni in Australia's cyber affairs agenda. By 2020, the number of Australian students to benefit from the NCP to study and undertake internships in the Indo-Pacific will have reached over 40,000. Over time, the federal government envisions that the growing cohort of NCP alumni:

> Will play an increasingly important role in Australia's relationships with our neighbours to become an influential and diverse network of Australians with direct experience in the Indo-Pacific, strong professional and personal networks across our region, and a driving force in Australia's future prosperity and position in the region.[22]

The ICES states that Australia's 'international representatives' must 'be equipped with an in-depth understanding of international cyber issues and Australia's interests in cyberspace' to deliver Australia's cyber affairs agenda. However, 'international representatives' are limited to Australian diplomats in the ICES. The ICES states Australia's commitment to developing a Cyber Affairs Curriculum for DFAT's Diplomatic Academy. This leads to a restrictive approach to promoting Australia's international cyber interests and overlooks the potential for creative partnerships with existing public diplomacy initiatives in the Indo-Pacific such as the NCP.

As Australia's cyber affairs agenda is 'global in perspective and regional in focus', increasing cooperation amongst Australian students on NCP Mobility and Scholarship programs in the Indo-Pacific may prove the best forum for advancing Australian's long-term international cyber affairs interests. Tran and Vu argue that the NCP construes Australian outbound student mobility explicitly as a vehicle of public diplomacy, with the aspiration of NCP students creating people-to-people links with the Indo-Pacific and therefore being regarded as actors or potential

[20] Jennifer Yang Hui, 'The Danger Meme: Countering Visual Disinformation in Asia's Politics' (The Interpreter, 3 April 2020).
[21] Department of Home Affairs' Submission into the Senate Select Committee on Foreign Interference through Social Media.
[22] Australia Global Alumni Webpage (https://globalalumni.gov.au/New-Colombo-Plan/Home).

actors of public diplomacy.[23] For example, the 125 NCP Scholars selected each year are fully-funded to spend up to 19 months in the Indo-Pacific and undertake semester exchanges, internships, mentorships, and language training. Although not comprising a formal component of an NCP Scholar's program, they also participate in ambassadorial activities and events.[24]

If Australia wants to advance its cyber affairs interests in the Indo-Pacific, it should explicitly recognise students sponsored by DFAT's NCP initiative as 'international representatives'. The ICES should also develop partnerships with DFAT's NCP Secretariat to increase cooperation and understanding of Australia's cyber affairs agenda amongst NCP students, scholars, and alumni. For example, this could be achieved by introducing a similar Cyber Affairs Curriculum (with sensitive diplomatic and political issues omitted) for NCP pre-departure sessions. This curriculum should include the topics raised in the ICES such as internet governance and cooperation, innovative uses of technology for financial inclusion, and awareness of existing and future cyber capacity building efforts in the Indo-Pacific.

Minister for Foreign Affairs Marise Payne announced the 125 New Colombo Plan Scholars for 2020 as 'Australia's best and brightest undergraduates from all universities across the country.'[25] The Australian government envisions that today's NCP scholars will be tomorrow's future leaders in business, politics, law, government, education, medicine, environment, and academia. If Australia can educate NCP students and scholars with an understanding of Australia's cyber affairs interests, then Australia can cultivate a future generation of leaders that will advocate for a free, open and secure cyberspace.

Australia Awards Scholarships program

Since the original Colombo Plan in 1951 (developed to bring the future leaders from Asia and Africa to study and form connections in Australia) to other inbound scholarship schemes,[26] Australia has supported more than 80,000 Asian students and scholars to undertake study and professional development in Australia.[27] These inbound mobility programs cast Asian scholarship recipients as emerging leaders and key actors in strengthening the relationships between Australia and the region.[28]

DFAT's Australia Awards Scholarships program offers emerging leaders from developing countries the opportunity to undertake study, research, and professional development opportunities in Australia. If Australia wants to further advance its cyber affairs interests, the ICES should explicitly target and involve students sponsored by DFAT's Australia Awards Scholarships program. Australia can leverage this inbound scholarship program to ensure recipients return to their home countries with an in-depth understanding of Australia's democratic vision of the Internet. This will further growth and stability in the Indo-Pacific and promote a more resilient cyber security posture.

[23] Ly Tran and Vu Thao, 'Beyond the "Normal" to the 'New Possibles": Australian Students' Experiences in Asia and their Roles in Making Connections with the Region via the New Colombo Plan (2018) 72(3) Higher Education Quarterly 194-207.
[24] The NCP program can be divided up into three components: an optional in-country language training component (up to 6-months), a mandatory study component (up to 12-months) and an optional internship component (up to 6 months).
[25] Marise Payne, New Colombo Plan 2020 Scholars (Media Release, 25 November 2019).
[26] Australian government inbound scholarship schemes include, but are not limited to: AusAid scholarship program, Endeavour program, Prime Minister's Australia Asia Awards.
[27] Australian Government, Foreign Policy White Paper (Department of Foreign Affairs and Trade, 2017).
[28] Mark Rahimi, 'New Colombo Plan: A Review of Research and Implications for Practice' (2018) International Education of Association of Australia Research Digest 2, 4.

Joshua Gacutan and Erin Jory

16 March 2020