Submission to DFAT's public consultation on Australia's cyber and critical technology international engagement strategy

16 June 2020

Contents

Introduction

ASPI's International Cyber Policy Centre (ICPC) commends the Australian Department of Foreign Affairs and Trade (DFAT) for conducting this public consultation to inform the next cyber and critical technology international engagement strategy.

One of ASPI's mandated objectives is to provide the Australian Government with fresh ideas and alternative sources of strategic policy ideas and advice. Our incentive to contribute to this request for submissions should be seen in this light and is informed by our other strands of work that include:

- conducting research and publishing relevant outputs;
- stimulating public discussion on key aspects of defence, security, cyber and technology policy;
- promoting international understanding, and;
- providing international training and support in cyber capacity-building.

ASPI's International Cyber Policy Centre is one of the implementing partners for DFAT's Cyber Cooperation Program and has also received funding from DFAT in support of research, activities and international fellowships.

The call for submissions requests respondents to address six big and open-ended strategic policy questions. Each one of these would deserve a proper study, analysis and assessment in their own right. Our submission presents five pillars for Australia's international cyber and critical technology engagement strategy.

ICPC encourages DFAT to continue to reach out to interested stakeholders throughout the drafting phase of this new strategy and we are looking forward to a draft strategy that is open for (written) submissions.

Five pillars for Australia's international cyber and critical technology engagement

1. Build upon Australia's Cyber Engagement Strategy

Australia's inaugural International Cyber Engagement Strategy strengthened Australia's international profile and demonstrated that the Australian Government can provide leadership on international cyber policy issues such as capacity building and responsible state behaviour in cyberspace. Australia should capitalise on this to lead in responses to critical technologies.

The Australian Government needs to maintain its regional leadership position on the issues raised in the 2017 International Cyber Engagement Strategy by continuing to be transparent, engaging and entrepreneurial.[1] These achievements in the area of international peace and security should be matched by similar approaches in the areas of international trade, human rights and international aid.[2]

Australia should continue to deepen its strategic cooperation with international partners in the Indo-Pacific, like Japan, India and ASEAN member states Singapore, Malaysia, Thailand, Vietnam, Philippines and Indonesia; with many of them DFAT signed memorandums of understanding on cyber cooperation. Australia should also consider partnering more closely with like-minded groups of nations, like those of the European Union and the Organization of American States.

Regional good practices from the Americas and Europe in cybersecurity, diplomacy, e-safety, digital trade and research and development could inform Australian efforts more substantially.

Australia's Cyber Cooperation Program has provided the foundation for regional cyber capacity building efforts in the Indo-Pacific. The program could increase its impact by being more strategic and direct in its calls for proposals (or: open tenders); an example to seek to replicate

[1] DFAT, *International Cyber Engagement Strategy* (2017), online.

[2] DFAT, *Cyber affairs: international security and cyberspace*, online.

is the EU Cyber Direct program; a project combining research, dialogues and capacity building in direct support of the EU's cyberdiplomacy agenda.

The program could also benefit from partnering with regional institutions involved in capacity building, such as the ASEAN-Singapore Cybersecurity Centre of Excellence, the Japan-ASEAN Cybersecurity Capacity Building Centre and the Pacific Regional Infrastructure Facility, to further enhance sustainability and coordination of, and consistency in, cyber capacity building efforts.

2. Maintain Australia's sovereign capabilities in critical technologies

The global debate around 5G, 'high risk vendors' and the Covid-19 crisis has underscored Australia's need for a degree of strategic autonomy - by this we mean an ability to protect the critical needs and values for our economy and our citizens; and to take advantage of global trends and market opportunities.

Autonomy in the cyber and technology domain remains best served in a rules-based order based on multi-stakeholder cooperation, while making sure our nation is not just a passive acquirer of products, services and emerging technologies.

The Australian government needs to join the debate around digital autonomy and follow developments in the European Union and in Southeast Asia. This should include strategic investments in the development and governance of technologies that are expected to become a critical part of the functioning of our society and economy. A first step should include a publicly released assessment which would map out which technologies are - or are likely to be - critical to Australia's economy, society and national security followed by a roadmap, like the recent roadmap 'Growing Australia's quantum technology industry'[3].

For example, technological advancements like artificial intelligence and 5G should become national priorities where we relinquish our position of passive acquirers to avert being exploited by nations that are leading research, development, and policies in these areas. The Australian Government must ensure that Australian interests - across government, industry, and civil society - are well represented in non-government bodies and networks where, for instance, technical standards and open protocols are determined.

Digital autonomy is also connected to Australia's responsibility for and accountability towards regional partners in the Indo-Pacific. The definition and adoption of cyber and critical technologies vary widely in our region and the strategy should accommodate this diversity. A digital Australia that is grounded in a regional setting also becomes a more interesting partner that has tangible products, services, and know-how to share.

[3] CSIRO, *Growing Australia's quantum technology industry* (May 2020), online.

3. Adopt a rights- and norms-based approach to Australia's cyber and critical technology engagements

Australia's Foreign Policy White Paper stated that Australia's values include 'political, economic and religious freedom, liberal democracy, the rule of law, racial and gender equality and mutual respect'.[4] These values should underpin every aspect of Australia's cyber and technology engagement strategy.

Australia has been leading the call for responsible state behaviour in cyberspace which is founded on a normative approach that is underpinned by the UN Charter and fundamental principles of human rights. Technologies and the use of technologies are often misperceived as being value-neutral; they are not.[5] Australia should strengthen its advocacy for a rights- and norms-based approach to cyber affairs and critical technology, for instance through the Freedom Online Coalition, without being perceived as imposing values on others.

The Covid-19 crisis forces societies to reappreciate social contracts around the balance between security, privacy and human rights. Normalising the use of such surveillance and public security technologies will usher in a new era that sees technology-enhanced social control help shift power from individuals to the state. A proliferation in the use of surveillance technologies across the Indo-Pacific, for example, risks entrenching global, ideological tensions and stand-offs. Such shifts, which will occur as we witness new and strengthened partnerships around critical and strategic technologies, for example between China and Russia, will exacerbate global trends toward a more illiberal world.[6]

Australia should pursue a cyber and critical technology engagement that is founded on human rights and international norms of good behaviour. Australia should make a greater effort of gathering good practices around the world for our domestic use. The government should work more closely with industry and civil society to develop, promote and share Australian examples of best practice in international forums, while also being able and willing to provide assistance in conceiving and developing rights-based solutions that other states can turn to and use.

[4] DFAT, Foreign Policy White Paper, Chapter One: foundations for success (2017), online.
[5] See for instance: Laura DeNardis, *The global war for internet governance* (2014); Laura DeNardis, *The internet in everything* (2020); and ASPI, *Mapping China's technology giants* (2019), online; ASPI, *Capabilities, competition and communication* (2019), online.
[6] ASPI, *A new Sino-Russian high-tech partnership* (October 2019), online.

4. Shape Australia's vision on the future of cyber and technology in international relations

Cyber affairs and new technologies will continue to shape the global order. The ability to exert influence over the cyber domain, and to lead in emerging technologies, has become vital to national resilience. Therefore, it is important that the Australian Government formulates a congruent vision on how it sees cyberspace and critical technology shaping the international strategic/geopolitical environment by 2030.

The Australian Government should facilitate national, and potentially regional, consultations concerning the future of cyber and emerging technologies and their impacts in the Indo-Pacific.[7] This should involve interdisciplinary and interagency participation and would help with the development of a 'national agenda'. Such a national agenda will also strengthen Australia's diplomatic and international reach in shaping a common perspective, particularly on future uses and impacts of emerging technologies.

The national agenda could be overseen by a multi-stakeholder cyber and critical technology advisory council - involving government, industry, academia and civil society. This council could support solidifying public momentum and ensure that national and foreign policies remain aligned and reinforce one another - at home and on the global stage.

A number of emerging critical technologies need to be considered already. These have the potential to change the global balance of power. The practise of concerted state-backed intellectual property theft, the US-China trade war and the controversy surrounding the deployment of 5G technologies have demonstrated this.

Some technologies that are commonly included on critical technologies lists include:

- Artificial intelligence
- Robotics, automation and autonomy
- Advanced manufacturing and semiconductors
- Aerospace
- Synthetic biology and gene engineering
- Quantum computing

These technologies share some attributes:

[7] For instance, a scenario-based survey inspired by ASPI, *Australia's cybersecurity future(s)*, online or Government of the Netherlands, Future Policy Survey: a new foundation for the Netherlands Armed Force (2010), online.

- For each of these technologies their impact on great power competition is not yet certain but ranges from 'no impact at all' to 'gamechanging'.
- These technologies could be used for either good or ill, depending on how they are applied. For example, facial recognition technology can be used to both prevent crime and can also be used to oppress minorities and to coercively surveil populations.
- Their application could be wide-ranging and therefore have a significant impact on individual people and their lives.
- Finally, Australia has some expertise in these technologies, but certainly not a monopoly position where we could shape their application on our own.

Given the attributes and properties of these critical technologies, and their potential effect, Australia should build coalitions that can shape international behaviour around the development, transfer and use of these critical technologies. Australia's diplomacy should be focused on creating awareness of the multi-use aspects of certain emerging technologies and mitigating the risks, while ensuring that it continues to benefit from such technologies.

5. Strengthen cyber and technology diplomacy in the years to come

How to approach international cyber and critical technology engagements?

Australia should acknowledge that neither the government nor DFAT alone can lead or implement an international agenda on cyber and critical technology. The inaugural International Cyber Engagement Strategy demonstrated that, at the very least, execution requires a solid whole-of-government endeavour. The alignment between domestic priorities and approaches and foreign policy needs to be stronger.

Australia's international interests should be primarily coordinated by DFAT. Playing this key coordination role will require DFAT to lead on high profile foreign policy issues, while also encouraging other government departments or agencies - who lead nationally on different cyber and technology issues - to play a greater international role. In other words, more investments need to go to enhancing skills and knowledge in international affairs for other government departments, at federal, state and territory levels, as well as with non-government entities like industry groups, civil society organisations and representatives of technical communities.

Finally, Australia's posts and missions need to get into a better position to support and maintain bilateral and regional policy dialogues on cyber affairs and emerging technologies. This includes 1.5 track dialogues with local industry, academia, and other civil society organisations. Such dialogues should encourage closer engagement with Australian technical communities to support their connections with counterparts overseas. This would help the government to better tap into influential civil society groups and think-tanks across the Indo-Pacific.

Australian posts and missions could also play a more active role in facilitating connections and encouraging joint collaboration and activities between Australian industry, academic and civil society groups and their counterparts overseas, particularly in key states that Australia wishes to engage with more closely.

About ASPI

ASPI is an independent, non-partisan think tank that produces expert and timely advice for Australia's strategic and defence leaders. ASPI generates new ideas for government, allowing them to make better-informed decisions for Australia's future. ASPI is one of the most authoritative and widely quoted contributors to public discussion of strategic policy issues in Australia and a recognised and authoritative Australian voice in international discussion of strategic issues, especially in the Asia-Pacific.

ASPI's International Cyber Policy Centre focuses on the growing importance of cyber, technology and information related issues for broader strategic policy. The centre focuses on the Indo-Pacific region and has a mixture of expertise and skills with teams of analysts who concentrate on domestic and international cybersecurity policy, technical issues, information operations, cyber capacity building, critical & emerging technologies, satellite, surveillance and China-related issues

Recent reports, op-eds and activities can be found on our webpage: www.aspi.org.au/icpc

Contact: icpc@aspi.org.au