REQUEST FOR COMMENT RESPONSE:

Call for Submissions: Cyber and Critical Technology International Engagement Strategy (CCTIES)

Department of Foreign Affairs and Trade, Australia

16 June 2020

I. STATEMENT OF INTEREST

In response to the Department of Foreign Affairs and Trade, State of Australia, Request for Consultation (RFC) on its Cyber and Critical Technology International Engagement Strategy (CCTIES), CrowdStrike offers the following views.

CrowdStrike approaches these questions from the standpoint of a leading cloud-native cybersecurity provider that defends globally-distributed enterprises from globally distributed threats. We offer insights informed by multiple practice areas: cyber threat intelligence, proactive, incident response and managed security services, and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

II.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?

Australia's concept of updating and expanding the 2017 International Cyber Engagement Strategy (ICES)[1] to a Cyber and Critical Technology International Engagement Strategy (CCTIES) is timely. Sustained malicious cyber threat activity, as well as enhanced focus internationally on technologies like the cloud, Internet of Things (IoT), quantum computing, Artificial Intelligence (AI), and 5G, provide an opportunity to develop a unified and strengthened approach to technologies with strategic implications. Critically, engagement in these areas should be viewed in the context of both mitigating risks and capitalizing on opportunities.

[1] Commonwealth of Australia, Department of Foreign Affairs and Trade, Australia's International Cyber Engagement Strategy, October 2017, https://www.dfat.gov.au/sites/default/files/minisite/static/ce81efe1-0c0d-42a8-9d7e-240ba210829d/aices/pdf/DFAT%20AICES_AccPDF.pdf.

ICES was a forward-looking document with an expansive scope—accounting for everything from human rights and trade, to cybercrime and international security. We recommend a high degree of continuity with the objectives outlined in that strategy. We highlight several opportunities throughout this comment to clarify or broaden the document to account for recent developments and the emerging importance of new technologies.

II.2. How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?

The rapid adoption of broadband around the globe, in some parts primarily through mobile devices, shows no signs of slowing. The UN Secretary-General's High-level Panel on Digital Cooperation has set 2030 as a target by which all adults should have access to digital networks.[2] Related to the transformative integration of cyberspace into every industry and aspect of life, technology privacy, trust, and supply chain issues have become a central theater of geopolitical competition. As more people, services, and critical infrastructure migrate online, the technologies that underpin the digital experience attract additional scrutiny from states.

In some instances, this heightens competition over access to or control of these resources, their underlying standards, and their reach. For example, some countries adopt protectionist measures, such as data localization rules, that serve to fragment Internet experiences and limit innovation. So far this competition has been most acute in the areas of market access and Internet governance, but disparate approaches increasingly manifest in debates over social media trust and safety, national privacy regulations, and standards like 5G. Over the next 10 years, the maturation or emergence of new technologies will reinforce these trends.

No single state will control the entire hardware and software supply chain, single-handedly dictate standards outcomes, and exert control over intellectual property, talent, and innovation across borders. This is an acceptable outcome given the rapid pace of change and now global nature of the technology providers. The key exercise Australia must undertake over this period will be to take risk-informed steps to:

1. Lower barriers to collaboration with strategic partners and trusted allies; and
2. Build stronger defenses against technological dependencies on, or compromises from, potential adversaries.

These objectives can be achieved through a combination of purposeful diplomatic, legal, and regulatory steps. While states must take both steps, Australia can distinguish itself and achieve stronger policy outcomes by focusing on (1) above, and aggressively pursuing proactive steps to enhance technical collaboration with allies and like-minded nations.

II.3. What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?

[2] Report of the UN Secretary-General's High-level Panel on Digital Cooperation. *The Age of Digital Interdependence*. P. 4. https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

Although sometimes overshadowed by the spectre of emerging threats, for today and for the foreseeable future the greatest technological risks relate to cyber espionage and attack. New technologies may over some time horizon alter Australia's threat environment; but today, skilled and well-resourced adversaries representing foreign military and intelligence services, along with criminally-motivated and 'hacktivist' actors, are attempting to breach critical systems to pursue a variety of ends. Some of these actors are motivated by geopolitical aspirations. Others by generating resources or causing adverse effects.

Further, cybersecurity should be viewed as a foundational component of new technologies. For example, while AI and 5G will reshape applications and communications and enable new use cases for existing technologies, their development, implementation, and use must be secure in order for them to achieve their promise. Failing to adopt these technologies due to security risks—or adopting them without due attention to security—represent future risks to Australia's economic and geopolitical competitiveness.

No formula will provide a definitive answer for how to balance these sorts of considerations. However, a few practices (described in section III.6, below) can inform a sound plan.

III.4. How should Australia pursue our cyber and critical technology interests internationally?

International engagement on cyber security can take many forms. Multilateral engagement, such as Australia's leadership and engagement in the UN Group of Governmental Experts, makes important contributions.[3] So too does bilateral engagement, including with important and like-minded allies like the United States. Importantly, commercial engagement represents a central avenue for pursuing interests internationally. Thoughtful commercial ties can be more durable and sustainable than other forms of interaction.

A reasonable premise from which to begin is that Australia may not have a full-scale industrial and innovation base for every critical technology. But efforts should be made to avoid dependencies on potentially adversarial nations; those with a well-established track record of being a bad actor in cyberspace; and those with predatory technology policies domestically or abroad. Everyday, CrowdStrike observes adversarial nation states leveraging cyber attacks in an attempt to steal intellectual property, disrupt key economic sectors, and conduct surveillance. Consequently, like in other aspects of international engagement, Australia must distinguish reliable partner nations from adversaries. That said, Australia can offset any dependencies—even on like-minded nations—by pursuing two key objectives.

First, Australia should identify at least one critical technology area in which to maintain a globally-leading position, and support national initiatives to that end (recommendations in section III.5). Second, it should cultivate a robust talent and research base in all other technology areas identified as critical. This will require thoughtful policy planning, robust international commercial engagement, and strong academic and civil society links.

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

[3] "Group of Governmental Experts." United Nations. (undated.) https://www.un.org/disarmament/group-of-governmental-experts/.

Cross-sector cooperation and partnerships can be extremely impactful, but should not be regarded as an end in their own right. Too often, states seek to create public private partnerships or cooperative agreements without first articulating a clear purpose. At best, such partnerships fail to provide practical utility; at worst, they consume resources and distract participants. The most useful partnerships probably already exist informally, because they serve a practical purpose to participants. When such partnerships are identified as strategically important, they can be provided clearer sanction, or additional resources. In the cybersecurity context, examples may include counter-botnet working groups, apprenticeship programs, and research commercialization initiatives.

For both cybersecurity and other critical technologies, government agencies should clearly opt for commercial off the shelf (COTS) solutions where possible, including from international providers that are able to establish trust. For immature emerging technologies where COTS solutions are inappropriate or none exist, focus should be placed on supporting basic research and research and development efforts. There are many different approaches to this end, but governments can start by articulating pressing problems and clear needs, and making available resources to support promising projects.

Where funding is provided to academic institutions or commercial partners, a venture or portfolio approach is preferable to supporting a single entity. Additional funds should only be made available based on demonstrated achievement of benchmarks.

> *III.6. What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?*

With respect to national-level cybersecurity policy issues, only a few widely agreed upon best practices have emerged. These include participation in relevant international fora (e.g., the UN Group of Governmental Experts) and treaties (e.g., the Budapest Convention on Cybercrime), and establishing leadership with the ministry of foreign affairs to lead international engagement. On these counts, Australia is already exceptionally well-positioned.

An often overlooked policy area, even among nations with leading cybersecurity capabilities, is for the government to lead by example in terms of maintaining an exceptionally strong cybersecurity posture. To this end, CrowdStrike recommends governments implement the “1-10-60 Rule” or similar metrics.[4] This concept challenges enterprises to detect malicious cyber activity within one minute, have a human investigate that detection within ten minutes, and remediate or isolate any compromised assets within one hour. This rule serves as an organizing principle for security personnel training and staffing, technology acquisitions, and modernization projects. This recommendation represents an ambitious program that only organizations with mature security programs can achieve. But measuring these metrics, testing security programs against them, and tracking performance over time can be remarkably effective.

[4] This concept is also relevant to the private sector. Most recently, the U.S. Cyberspace Solarium Commission recommended that the U.S. Congress require public companies to track cyber incident time to detection, time to investigation, and time to remediation metrics in order to continuously improve defenses. U.S. Cyberspace Solarium Commission, *Final Report*. March 2020. p. 83. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

Comprehensive visibility across the enterprise is the first step to strengthening security posture. CrowdStrike's Falcon platform operates on this basis, and is enabled by a massive distributed graph database using cloud-scale AI and deep link analysis to identify threats. This means threats targeting disparate entities and organizations can be identified and prevented. As soon as a malicious indicator or behavior is identified anywhere, it can be stopped everywhere.

A few additional practices will help on this journey. Governments should use shared-services acquisition models where possible. These models drive procurement efficiencies by reducing the number of contracting actions required to support multiple departments and agencies. They also provide simpler training requirements, easier management and maintenance, and reduced administrative complexity. From an operational perspective, they enable standardized service levels across government—and even more importantly—a common operating picture across federated entities.

Countries and industries across the globe have made purposeful decisions over the last few years to adopt cloud technologies. These promote the shared services concepts described above. The best practices here (e.g., used by the United Kingdom[5]) makes clear not only that cloud computing technologies should be adopted, but there is no prohibition on storing data outside the country, when that fits within the risk profile of the use case. This ensures no inhibition on the use of critical technologies, where other countries have more established providers or other advantages. Finally, empowering end-users (e.g., department Chief Information Security Officers) to make risk management decisions—and accept risks where necessary—is key. Overly-centralized risk planning can cause rigidity that encumbers decisionmakers, who at times are best positioned to understand countervailing factors or mitigations.

More broadly, the adoption of principles-based cybersecurity requirements can incentivize both innovation and organizational implementation of state-of-the-art technologies to protect data. While the Notifiable Data Breaches scheme is already influencing organizations to treat security breaches seriously, there are additional steps that can encourage proactive adoption of cutting edge technologies, like SaaS solutions, from around the globe. The European Union General Data Protection Regulation (GDPR), for example, requires organizations to look to the "state of the art" and protect personal data with technological and organizational safeguards "appropriate to the risk." Creating non-prescriptive mandates that nonetheless encourage organizations to analyze the probability and severity of threats in line with technological realities is important for ensuring cybersecurity evolves with critical technologies.

III. CONCLUSION

Australia already has a strong posture on international cybersecurity and critical technologies—but improvements are possible. The ICES strategy outlines a thoughtful approach on cybersecurity issues, and continuity with the objectives outlined therein is appropriate. However, now is a good time to expand the scope with CCTIES, to increase focus on emerging areas. Other nations may soon follow Australia's lead

[5] Guidance: Cloud Guide for the Public Sector. Government of the United Kingdom. March 31, 2020. https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector#offshoring-and-data-residency.

in approaching technology engagement this comprehensively. Importantly, cybersecurity underpins and enables most other critical technologies—and thus must remain central to the new strategy.

IV. ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint security. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver real-time protection and actionable threat intelligence from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed threat hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and Indicator-of-Attack (IoA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 2 trillion security events a week from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches. Learn more: www.crowdstrike.com.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Privacy and public policy inquiries should be made to:

Mike Sentonas
Chief Technology Officer

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Contact: policy@crowdstrike.com

###