16 June 2020

Office of the Ambassador for Cyber Affairs and Critical Technology
International Cyber Policy Division
Department of Foreign Affairs and Trade
Rg Casey Building, 10 John McEwen Cres
Barton ACT 2600

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

Palo Alto Networks appreciates the opportunity to provide input to the Australian Government's forthcoming *Cyber and Critical Technology International Engagement Strategy* (CCTIES).

Australia has demonstrated leadership and a commitment to international engagement on cybersecurity with the development and implementation of its inaugural *International Cyber Engagement Strategy* in 2017 (the 2017 Strategy). We are pleased to see the Australian Government's continued dedication to this important policy area through its call for views on the new and expanded CCTIES.

Palo Alto Networks is the largest cybersecurity company in the world. Palo Alto Networks secures the networks and information of more than 73,000 enterprise and government customers in 150+ countries to protect billions of people globally, including in Australia. Over 90 of the Fortune 100 and more than 71% of the Global 2000 rely on us to improve their cybersecurity posture. We work with some of the world's largest organisations across all industry verticals. We combine our knowledge from working with customers and governments across the world to directly inform our responses. Our submission includes overarching general comments immediately below, followed by responses to specific questions asked as part of the consultation.

General Comments

Critical Technology

Palo Alto Networks welcomes the expansion of Australia's *International Cyber Engagement Strategy* to include Critical Technology. We believe this reflects the importance of the Australian Government engaging in international advocacy with respect to how critical technologies may, or may not, impact international standards, laws, norms, policies and approaches. To assist in defining the objectives of the CCTIES, we would recommend including a definition of "critical technology", as many people will have different interpretations and views as to what this means for Australia's international engagement objectives.

Recommendation 1
Define "critical technology" to help inform CCTIES objectives, implementation and to provide clear direction to stakeholders.

Strengthen Private Sector Partnership on International Issues

Building on some of the themes identified by the 2017 Strategy, CCTIES should strengthen public-private sector collaboration on international issues, in recognition of the important role that the private sector can play in supporting and delivering international outcomes with respect to cyber and critical technology policies.

The private sector can provide subject matter and technical expertise in support of the Australian Government's international discussions. This is particularly desirable in the context of specialised technical conversations, such as those pertaining to international technology standards. These conversations can often require a level of expert knowledge that is found in companies at the forefront of technological innovation. Not leveraging the knowledge of companies that are developing innovative technologies has led to multiple instances in recent years where well-intentioned public policies had the unintentional consequence of stifling cybersecurity for individuals, governments and companies. In addition, companies, in particular those that are multinational, can help amplify government efforts internationally where it is appropriate. Multinational companies are well placed to do so because they are often involved in international forums in their own right, they maintain global visibility of trends and issues and can

support capacity-building initiatives as relevant (e.g., if they have an in-country presence). By working with trusted multinational companies, the Australian Government could amplify its messaging to the international community. The private sector, where appropriate and aligned, can also promote international topics, ideas and policies as part of regular operations, and be a valuable source on what topics, trends and issues might be of interest to certain countries and regions.

To achieve true public-private partnership, CCTIES must strengthen public-private communication and collaboration. Through CCTIES, the Government should identify the mechanisms for engagement with trusted partners to support Australia's international advocacy on critical technologies. Closer working relationships between the private sector and DFAT could be strengthened via working groups, advisory panels, and/or private-sector rotations or placements into DFAT. In the past, DFAT ran a series of Track 1.5 dialogues with various countries as a way of strengthening official and unofficial diplomatic interactions between Australia and key nation states. Palo Alto Networks has participated in a number of Track 1.5 dialogues, including the Australia-United States (U.S.) dialogue, and has found them extremely valuable. We suggest DFAT work with interested industry stakeholders to determine if Australia's Track 1.5 series should be reinvigorated/ expanded with key nation states and how to maximise their value for DFAT, the Australian Government as a whole, and industry stakeholders. Overall, ongoing collaboration with industry can help to ensure that the priorities and activities of Australia's international work remains calibrated with the commercial needs of its companies, whose focuses and needs will arguably change over time due to varying circumstances.

Recommendation 2
CCTIES should strengthen public-private partnerships, through consideration of mechanisms including, but not limited to:

- Maintaining an Industry Advisory Panel and/or Working Groups to assist with the implementation of initiatives in CCTIES and to support Australia's international advocacy on cyber and technology issues.
- Leverage and engage the private sector in capacity building efforts, as appropriate, by clearly communicating regional priorities (both country and themes/topics) and calling for private sector interest in supporting such activities (at their own cost).
- Coordinate and invite the private sector to support and amplify Australia's international positions and efforts, where appropriate, through leveraging public-private operational working groups.
- Consider a private sector placement or rotation through DFAT to support key topics/policy development.
- Work with interested industry stakeholders to determine if Australia's Track 1.5 dialogue series should be reinvigorated/ expanded with key nation states and how to maximise their value.

Subject Matter Experts (SMEs) at Key Diplomatic Posts

We congratulate DFAT's International Cyber Policy team on the work they have done delivering short training courses to upskill diplomatic officers on cyber issues prior to the commencement of their diplomatic post in Australian Embassies around the world. We recognise that it is common for diplomats to be "generalists" who can regularly learn new topics and change their areas of focus throughout their careers. However, as international conversations around cyber issues become more technical and detailed in nature-- and more important to Australia's national interests-- DFAT may wish to consider placing dedicated subject matter experts (SMEs) with backgrounds in technology/cyber issues at key diplomatic posts, where possible.

Increasingly a number of international organisations are engaging in complex technical and policy issues that require subject matter knowledge and expertise. Given the increasing pace of technological change, this trend is set to continue. A number of these new, emerging and critical technologies will require discussion and advocacy on a technical level internationally. We would recommend the Australian Government review

where technical SME representation at certain posts may be helpful to Australia's international interests. We acknowledge that this would not be possible, or necessary, for all diplomatic posts but rather, for key posts in capitals where international laws, norms and standards are frequently discussed and decided, such as Geneva or New York City.

Having dedicated DFAT officers at key posts who possess technical and policy expertise, alongside the diplomatic skills, would ensure that Australia is well positioned and effective in conveying its position on key technology issues into the future. It is recommended that these dedicated SMEs work solely on cyber and critical technology issues to the extent possible so as to give these topics the prioritisation needed. It would also be ideal if these officers had experience both inside and outside of the public sector, so as to understand the role that the private sector can play in these discussions. These specialised backgrounds would equip the cyber diplomats in effective engagements with the host government and industry to support and further Australia's international cybersecurity diplomacy efforts.

In addition, DFAT should engage the private sector in their training sessions for cyber diplomats. The U.S. Department of State takes such an approach, bringing companies in on a regular basis to update U.S. cyber diplomats on the latest technology trends, policy issues and concerns as well as how U.S. diplomats might best promote the needs of U.S. industry globally.

Recommendation 3
The Australian Government should consider placing dedicated SME on cyber and critical technology at key diplomatic posts to ensure that Australia's international interests are well served into the future.

Promote Industry-Led, Globally Harmonised Information and Communication Technology (ICT) Standards

ICT standards should be industry-led, market-driven, and globally workable. Unfortunately, some governments and multilateral organisations are increasingly seeking to develop ICT standards or promote country-specific / unique standards that

companies must use or build to. Policies like these, while often well-intentioned, can sometimes harm innovation and security, largely because they run counter to how the ICT industry works. The ICT industry can create leading-edge, sophisticated, affordable products because companies can build one product version that is sold globally, saving costs and raising manufacturing efficiencies. The ICT industry also builds to voluntary, global, industry-led consensus-based standards that are accepted (or chosen) by the marketplace as the most effective or most appropriate. Diverting resources to meet country-specific requirements negates these benefits because companies must build tailored products in addition to global product lines. This raises costs (ultimately to customers) and drains resources from research and development. Such discriminatory policies also likely decrease security. Policies mandating the use of certain standards cannot keep up with constantly evolving threats. Mandated technical standards can also benefit adversaries who, knowing the defences employed, can circumvent them. DFAT can play an important role in promoting the use of international, globally harmonised ICT standards as well as promoting the process of how ICT standards should be developed (industry-led).

For example, Australia, the United Kingdom (UK), the U.S., and Japan all are working to promote Internet of Things (IoT) security standards/best practices. However, Australia and the UK seem to be relatively aligned on how they are approaching IoT security standards for consumer devices, while the U.S. and Japan appear to be advocating and adopting different approaches. It is important to global industry that governments take harmonised approaches (and ones that meet industry needs). Australia could play an important role working with industry stakeholders and government counterparts in the region, with its allies and across the world to foster regular dialogues with the goal to ensure consistent government approaches to IoT security standards/best practices.

Australia should play an active role in ensuring that international organisations, such as the International Telecommunications Union Telecommunications Standards Sector (ITU-T), operate within their mandate and do not duplicate other international efforts, which may cause confusion. Palo Alto Networks recognises and appreciates the ITU-T's history of international standards development work in the field of telecommunications. However, many stakeholders are concerned with ITU-T engaging in work outside its purview, particularly in cybersecurity, which is often redundant to standards work in

other fora. There are many established Standards Development Organisations (SDOs) that are better positioned than ITU-T to develop standards in areas outside of telecommunications, especially for cybersecurity and emerging technologies such as Artificial Intelligence (AI), IoT, and quantum computing. The Australian Government should encourage the ITU-T to avoid initiating work that duplicates or substantially overlaps with work underway or planned in other SDOs that already have a track record of success in developing timely, high quality and market-relevant standards. Instead, ITU-T should expand engagement with other SDOs to avoid redundancies and increase cooperation where appropriate. The ITU-T should refer its members to relevant work underway or planned in other SDOs, and it should reference that work where appropriate. While not standards-specific, we also note that the ITU-T has been undertaking various activities related to cybersecurity policy, which is outside its core competency. Overall, we recommend that the Australian Government press for a more focused role for ITU-T that is clearly within its mandate, as additional work is not only redundant but also may create confusing or poor recommendation documents for other global participants and stakeholders.

It will be also important that Australia maintains visibility of, and is appropriately represented at, relevant international organisations that are developing policies related to ICT standards these include, for example, International Organisation for Standards (ISO) and International Electrotechnical Commission (IEC). Australia must be consistently represented at these discussions to ensure that its interests are protected and that ICT standards remain industry-led and driven by market demands. Having a SME at key diplomatic posts and being able to rely on industry experts to support these standards-related activities (which are often quite technical) will be crucial to Australia's success in this regard.

Recommendation 4

The Australian Government should:

- Continue to promote the use of international, globally harmonised ICT standards as well as promoting the process of how ICT standards should be developed (industry-led).

- Take an active role in encouraging the ITU-T to work within its recognised areas of competence and within its mandate.
- Maintain communication with partner countries and stakeholders to increase awareness of proposals that exceed the scope of the ITU-T.
- Play a more robust role in more established SDOs, involving not just DFAT's policy experts but the Government's technical SMEs since the discussions are technical in nature; in particular, ISO and IEC.

CCTIES Resourcing and Governance

It will be important to the success of CCTIES that it is well resourced and supported at the most senior levels of government, that CCTIES leverages relevant expertise and initiatives across government stakeholders, that there are clear lines of accountability for identified initiatives and that progress updates are made publicly available.

CCTIES and its initiatives must be sufficiently resourced and have the buy-in from the most senior levels of Government. To achieve this, DFAT may wish to consider briefing Heads of Mission (HoM) and Deputy HoMs on CCTIES as well as other cybersecurity and critical technology trends and issues at annual HoM forums. With the expansion of its remit to include critical technologies, DFAT may also need to consider whether additional funding is required for staff, capacity building initiatives and so on as part of CCTIES; although we appreciate that additional funding for cyber and critical technology may be difficult given the financial strain of COVID-19, however we believe it is an important area of investment.

Leveraging the expertise from across the wide range of government stakeholders will be critical, as will be ensuring that DFAT has early visibility into cyber and critical technology issues being addressed in other Departments. DFAT's engagement across all relevant Government agencies will be important in this regard as will creating strong links between the Government domestic and international cyber activities. As the Government looks to finalise the *2020 Cyber Security Strategy*, consideration should be given to how it and the CCTIES cross reference and compliment each other. For example, national cyber exercises should contain an international component; as most cyber incidents have an international component, it is important that Australia's

coordination across domestic and international agencies is regularly exercised and strengthened.

CCTIES should articulate all relevant Government stakeholders, their respective roles and responsibilities and how DFAT will collaborate with these stakeholders. Clear lines of responsibility for the CCTIES should be established stemming from the Ambassador for Cyber Affairs and Critical Technology. Finally, as DFAT did with its 2017 Strategy, CCTIES should also articulate how the Government will update stakeholders on its progress, and make it publicly available. We appreciated how DFAT's 2019 Progress Report on its 2017 Strategy set out Australia's achievements under each of the 61 planned actions.

Recommendation 5
In order to ensures its success, CCTIES should:

- Be well-resourced and supported at the most senior levels of government.
- Leverage relevant expertise and initiatives across a wide range of government stakeholders.
- Establish clear lines of accountability for identified initiatives.
- Ensure there are publicly available progress updates available.

Specific Questions

In addition to the general comments above, we have addressed some of CCTIES consultation's specific questions below.

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?

Australia should continue to leverage its role as a regional and global economic leader to showcase best practices with respect to cyber and critical technology. A number of the goals identified in the 2017 Strategy remain relevant, such as the focus on cybercrime, human rights and democracy and digital trade, to name a few. However, we would also recommend that Australia should pursue the following five objectives

internationally: industry-led, globally harmonised ICT standards, mutual recognition of five-eyes government certification frameworks, supply chain security, free flows of data across borders, and securing and protecting electoral processes. As articulated above, the Australian Government should leverage and create strong cooperation with the private sector to promote these objectives.

Industry-Led, Globally Harmonised ICT Standards

As noted above under “General Comments”, ICT standards should be industry-led, market-driven, and globally workable. DFAT can play an important role in promoting the use of international, globally harmonised ICT standards as well as promoting the process of how ICT standards should be developed (industry-led).

Mutual Recognition of Five-Eyes Government Certification Frameworks

DFAT should work with its five-eyes partners to introduce compatible product certification frameworks for government procurements or, at the minimum, seek mutual recognition of certifications between Five-Eyes partners. Mutual recognition will be helpful to government agencies that need to access technology solutions as quickly as possible rather than waiting for something to be accredited locally. It will also greatly support both Australian and foreign companies in saving time, money, and avoid duplication of effort.

Supply Chain Security

Governments around the world want assurance regarding the integrity of the ICT products and services that they, as well as the critical infrastructure entities in their countries, procure and use. The Australian Government should encourage and educate other countries about supply chain risks, both with respect to the hardware and software they purchase, and how these risks can be mitigated. The Australian Government should do more to elevate the conversation internationally around how to promote best practices in supply chain security. This could include encouraging and incentivising ICT vendors to demonstrate adherence to best practice. There are measures Governments can encourage the private sector to adopt including with respect to internal processes

and oversight, hardware manufacturing processes, secure delivery of hardware products, third-party testing and vulnerability remediation and disclosure practices. The Australian Government could work within the region to raise awareness of supply chain risks and mitigations. Other representative best practices might include expecting ICT vendors to have:

- An organisational focus on end-to-end risk management. Supply chain risks should be identified across an entire product lifecycle – design, sourcing, manufacturing, fulfilment, and service – and proactive action should be taken to ensure the integrity of products. Risk assessments should be performed early in the product development lifecycle to help determine the feasibility of product design decisions.

- Strong supplier management focused on security requirements as well as a collaborative relationship to ensure a complete view of suppliers' security posture.

- Processes that account for geopolitical implications of product integrity, including identifying manufacturing locations that enable companies to more easily manage personnel, facility and product security, and identifying whether suppliers share product source code with other governments.

- Active engagement in public-private partnerships designed to increase collaboration between public and private sector organisations and make recommendations for enhancing supply chain security.

- Finally, executive management buy-in is vital, and strong coordination across business units is critical to successful supply chain risk management.

DFAT should encourage other governments to allow flexibility in how alignment to these best practices is demonstrated.

DFAT should also work with key partners to ensure Australia's own supply chain security with respect to the development and production of critical technologies. Australia needs to ensure that it can account for the security of the supply chain for these critical technologies, such as quantum computing and 5G, which will continue to

be important into the future. This could involve collaboration with key international partners, who may be responsible for the development and manufacturing of these critical technologies.

Free Flow of Data Across Borders

The Australian Government has a role to play in promoting the free flow of data across borders. Despite the benefits to consumers, companies and economies that arise from the ability of organisations to easily share data across borders, a wide variety of countries have instituted measures that restrict cross-border data flows, including data residency requirements.[1] The public policy rationales behind such policies vary; however, the end result is often one that inhibits value generation, reduces exports and foreign direct investment, and results in productivity losses for local companies that rely on a wide range of digital services, all without added benefits to privacy or data security. Data localisation requirements may also deter companies from investing in a given country as mandating local storage of data vastly increases the cost of doing business for all companies. DFAT can help educate other governments -- particularly its counterparts in the Indo-Pacific -- on two key benefits of cross-border data flows: economic growth and efficiency, and cybersecurity.

Economic growth and efficiency: The free flow of data is key to the health of the modern global economy, delivering countless benefits and enabling access to knowledge and tools for people around the world. For consumers and companies of all sizes, across all industries, data flows and reliance on digital technologies have fundamentally changed how domestic commerce and international trade are conducted. Firms rely on data to advertise and engage with clients and customers, discern market demand and adapt products and services accordingly, operate production systems, manage workforces and expenditures, monitor supply chains, and conduct a range of other day-to-day business activities.[2] Data propels businesses and governments forward, and supports everything from business operations to the way governments develop and implement

[1] Castro, Daniel and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," *Information Technology & Innovation Foundation*, February 2015, http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=2.100429661.252983325.1563809645-669743502.1548338492

[2] Cory, Nigel, "The False Appeal of Data Nationalism: Why the Value of Data Comes from How It's Used, Not Where It's Stored," *Information Technology & Innovation Foundation*, April 2019, https://itif.org/publications/2019/04/01/false-appeal-data-nationalism-why-value-data-comes-how-its-used-not-where

public policies.

In the modern global economy, data is already an essential means of widening consumer choice and the affordability of goods and services, helping SMEs reach global markets, and fostering international production through global value chains, and its uses are widening.[3] Any regulatory measures restricting data flows will therefore also have detrimental consequences for trade and economic development. These consequences are likely to be particularly acute for SMEs, as data-restrictive policies affect access to a range of cost-efficient digital technologies, including cloud and over-the-top communication services that small businesses rely on. As such, DFAT could call on countries to avoid policies that call for data localisation or otherwise restrict the flow of data, recognise the enormous societal and economic benefits from innovative new technology and data-based services, and pursue policies that promote the ability of firms and consumers to leverage these technologies.

Cybersecurity: As we noted above, some countries equate data localisation with improved security. In fact, data localisation has the opposite effect. Any data localisation policies that stifle the cross-border flow of information related to cyberthreats can deprive organisations of the benefits of real time, global deployment of preventative defences and security. Cross-border data flows can contribute to cybersecurity in two important ways.

- *Security telemetry:* In today's world, cyberattacks are increasingly sophisticated and automated, launched by adversaries anywhere in the world, hitting targets in all countries. Australia, like all countries, is seeing its businesses, citizens, and public sector systematically targeted by threats which may or may not originate from inside its borders.

  To counter this, leading organisations in the cybersecurity community regularly leverage "security telemetry," in which cyberthreat information is combined from around the world to develop a global picture of cyber adversaries—their techniques, tactics, infrastructure, motives, and the like. This analysis is in turn used to develop new protections such as automated preventive measures, which

[3] Casalini, F. and J. López González (2019-01-23), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, http://dx.doi.org/10.1787/b2023a47-en

are deployed to customers globally to help them to prevent successful cyberattacks. In other words, the global model enables rapid response time to detect and prevent new and unknown threats (or threats similar to previous attacks) from impacting multiple organisations around the world. Customers benefit from a globally aggregated view of cybersecurity threats and a real-time global deployment of responses. In short, effective cybersecurity requires connecting the dots between different threats, and taking immediate action to automatically deploy defences against these threats.

Because the threats can originate from, and target anywhere in the world, security telemetry needs to be freely transferred between countries to best understand and counter the full range of cyber adversaries and threats we all face. If countries begin to block security telemetry from leaving their borders, that valuable threat information will not be analysed as part of this larger effort, which means the cybersecurity community then may not be able to develop preventive measures as robust or effective as it otherwise could. This impacts the country in question as well as the global community. To be most successful, security telemetry must be made as accessible as possible globally, combining cyberthreat information from all countries.

- *Cyberthreat research:* Cross-border data flows also are important to cybersecurity researchers, who gather, research, analyse, and provide insights into the latest cyberthreats. Cybersecurity researchers often collaborate across borders on their work. Prohibitions on the transfer of data would hinder the effectiveness of this threat research.

Cross-border data transfers and meaningful privacy protection are not mutually exclusive goals. When transferring cybersecurity-related information across borders (whether security telemetry, or research), appropriate privacy protections must be in place.

Supporting Countries' Efforts to Secure Election Infrastructure

DFAT should assist countries both globally and regionally to secure their electoral infrastructure and democratic institutions. Interference and hacking activities against

elections in the U.S. and Europe in recent years should be a wake-up call. In Australia we have seen a number of attacks against Parliament House infrastructure. Ensuring election security encompasses security of electronic voting machines as well as voter registration databases and voting tabulation, and reporting applications (which often reside on insecure state or local government networks). Many countries, in recognition of the importance of securing their democractice institutions, have now deemed election infrastructure as critical infrastructure.[4] Australia should collaborate and support countries' efforts to secure their electoral and key democractic infrastructure.

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

There are a number of ways cyberspace and key critical technologies will shape the international strategic and geopolitical environment for the next decade. A very important one is the role that cyberthreats and cyber adversaries are playing and will continue to play into the future. Although the trend is worrisome, if cybersecurity is prioritised, we have the opportunity to address these challenges in Australia and the Indo-Pacific. We expand on this point in our answer to Question 3.

High profile incidents of cybercrime have exemplified the speed with which cyber threats can propagate globally, how rapidly adversaries can adapt to security responses, and how easily a compromise can impact an organisation's core functions or services. In 2020, there has been increased reporting of cyber incidents affecting big Australian companies; a large Melbourne-based global logistics company has been hit twice by ransomware attacks, cyber incidents have also affected a government agency, resource company and a financial services company.[5]

Globally, countless adversaries are willing to steal information, illegally make profits, and undermine their targets. Over the last decade the level of sophistication employed by adversaries (in particular, cybercriminals) has dramatically increased. While some criminals continue to compromise networks using publicly known vulnerabilities that

[4] In January 2017 the U.S. Department of Homeland Security (DHS) designated the election infrastructure used in federal elections as part of the nation's critical infrastructure as a subsector under the Government Facilities sector. The designation allows DHS to provide services on a prioritised basis at the request of state and local election officials.
[5] 'Recent cyber attacks just the tip of the iceberg for Australia', 18 May 2020, Available: https://www.afr.com/by/alastair-macgibbon-p4yvwb

have known mitigations, others are leveraging sophisticated attack tools to help find new exploits and automate and scale their attacks. Today, cybercriminals operate like a sophisticated business – they employ people, they have hierarchies and processes, and unfortunately they are making a sizeable profit from their clandestine activities.

Palo Alto Networks threat intelligence team, Unit 42, confirms this trend. In an annual 2019 report on one Nigerian cybercriminal organisation, assigned the name "SilverTerrier", Unit 42 detailed their rapid expansion from just a few individuals experimenting with malware purchased online, to an organisation encompassing around 480 different actors and groups collectively producing more than 81,300 samples of malware that has been linked to 2.1 million attacks worldwide.[6] The report also detailed that the frequency of SilverTerrier's attacks had dramatically increased. In 2018, there were an average of 34,039 attacks per month against Palo Alto Networks customer base. In 2019, this number climbed to an average of 92,739 per month – peaking at 245,637 attacks in the month of June 2019. While our customer base was protected against these attacks, the statistics demonstrated the widespread proliferation of cybercriminal activities.

If governments are going to deliver on the social contract and protect their citizens and the businesses that reside in their jurisdiction, they must look at holistic ways to improve cybersecurity and address cybercrime at scale. Harnessing the technological developments we describe below as part of DFAT's international cyber and critical technology efforts will be essential to achieving this task.

Question 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?

We have identified four game-changing technological developments and applications as presenting risks and opportunities for Australia and the Indo-Pacific region. These include 5G, IoT and Industrial IoT (IIoT), AI and Machine Learning (ML), and cloud security. We think in all cases the opportunities can outweigh the risks if cybersecurity is prioritised and integrated from the beginning.

[6] 'SilverTerrier: 2019 Nigerian Business Email Compromise Update', publish 31 March, Available: https://unit42.paloaltonetworks.com/silverterrier-2019-update/

Risk and Opportunity: 5G

5G promises transformative mobility by offering an enhanced mobile broadband experience and enabling the mass digitisation of businesses and industries. The early stages of 5G evolution will revolve around delivering higher data speeds, latency improvements and the functional redesign of mobile networks to enable greater agility, efficiency and openness. Although these improvements will yield revenue opportunities for operators, the explosion of low-cost, low-power, unsecured IoT will also pose increased security risks for both operators and end users.

As all nations continue to adopt and roll out 5G infrastructure, they must develop 5G networks that are secure and trusted by design. This approach can help to avoid some of the challenges we have securing today's 3G and 4G networks, which arguably were not designed to be secure. As the world moves closer to a digitally connected 5G world, there are an increasing array of attack vectors – inside out, outside in, and roaming, to mention just a few. Infected "trusted" end devices become sources of inside out attacks, targeting external web sites, creating signaling storms, wasting bandwidth, and stealing data from users and providers. Furthermore, mobile and fixed line networks infrastructures' convergence can result in unsecure interconnectivity points, which need to be protected. Secure Wi-Fi and LTE access and handover challenges are additional problems. The threat and potential damage is relevant not just to the telecom/service provider sector, but to the many interconnected sectors including energy, finance, healthcare, transportation, IT, government, manufacturing, and retail. Given all of these challenges, 4/5G infrastructure security requires a holistic approach, where detection and prevention is the key ingredient to the infrastructure.

The answer to the growing number of advanced, automated threats to mobile networks is to leverage technology to automatically identify and block the threats. Mobile Network Operators (MNOs) and Internet Service Providers (ISPs) need to have constant real-time visibility across traffic passing through their networks and be able to detect and stop in real time cybersecurity threats within that traffic. Automated visibility and enforcement are possible using advanced security solutions such as mobile tunnel traffic inspection. Such technologies allow MNOs and ISPs to determine if traffic flowing in their tunnel is malicious or benign and take steps to prevent attacks in real time. In

fact, prevention is crucial: we would encourage a greater focus on detecting and preventing threats and incidents -- with investment in the right technology, a majority of attacks can be detected and successfully prevented. Automation is also key, reducing the need to keep responding to every attack, which is time-consuming and costly. In fact, manual prevention is impossible.

With this in mind, we recommend that DFAT work with the private sector and regional counterparts to highlight the importance of 5G networks being secure by design. In particular, DFAT should convey to government counterparts the importance of 5G operators maintaining constant real-time visibility of traffic passing through their 5G networks and being able to detect and stop in real time cybersecurity threats within that traffic; and design into their networks a high reliance on automation, ML and AI.

Risk and Opportunity: IoT/IIoT

The number of IoT devices globally is set to proliferate over the next decade. Today, pretty much any object can, and is being transformed into an IoT device that can be controlled or communicate information via the internet; from lightbulb, to a baby monitor to the components in a car's engine, which now contain hundreds of sensors collecting and transmitting data. The uptake of IoT is only set to increase with IoT devices being deployed at an industrial scale to autonomous mines and smart cities. IoT represents great opportunities to improve our way of life but it also presents a security risk. It will be important that the Australian Government promotes globally both IoT device level security built in by design but also that IoT devices can be secure at the network level.

We acknowledge that the Australian Government has shown leadership on IoT device level with the release of the *Draft Code of Practice - Securing the Internet of Things for Consumers* earlier this year. This Code was an important 'first step to improve the security of IoT devices in Australia' recommending, among other things, that devices do not have duplicate, default or weak passwords and that they can receive software updates and patches. However, to address IoT security vulnerabilities at scale, countries must look to secure these devices at the network level.

We stress the network level as a priority security enforcement point because IoT device security, while important, is often a very operationally inefficient approach that is prone

to error, given the many issues encountered when trying to secure at this level (e.g. highly heterogeneous IoT device environments, poor or nonexistent product security/patch support from some vendors, and inability of some products to be secured directly). There is also the issue of legacy devices - billions of already-deployed IoT devices that cannot be retroactively designed and certified. Policymakers must look more holistically and promote security in both the network and the large ecosystem of companies that work together to deploy and run IoT systems. The network is a logical detection and enforcement point for IoT security, because all IoT devices leverage mobile/ISP networks to communicate.

DFAT should educate regional governments about the importance of IoT security, both at the device level and the network level, and how failing to do so may present a substantial risk to their national security and economic prosperity. The relevance of IIoT security will be even more important in the post-COVID-19 era, where we expect there will be a growing focus on factory and supply chain automation in many countries.

Risk and Opportunity: Automation of Cyberattacks and the Benefits of AI/ML

Both cyberattacks and cybersecurity defences are leveraging machine learning and automation.

An automated attack is one performed by a computer program rather than the attacker manually performing the steps in the attack sequence. While cyber adversaries have leveraged attack tools for quite some time, older tools could only initiate one attack sequence at a time, requiring human intervention to launch additional attack sequences. However, newer tools can perform the entire attack process on their own. This speeds up the process as well as makes it easier for hackers who lack technical skills to mount a successful attack. Some attack tools even have user-friendly graphical interfaces as well as detailed help files to instruct attackers in their use.

If organisations try to defend against these attacks manually, the fight becomes man versus machine, with highly unfavorable odds for the organisation. To successfully protect against automated attacks, it is essential to fight fire with fire – or in this case, machine with machine – by incorporating automation into cybersecurity efforts. Automation levels the playing field, reduces the volume of threats, and allows for faster

prevention of new and previously unknown threats.

Many security vendors look at automation as a way to become more efficient and as a means to save in manpower or headcount. While true, automation should also be viewed as a tool that can, and should, be used to better predict behaviors and execute protections faster. If implemented appropriately and with the right tools, automation can aid in the prevention of successful cyberattacks.

DFAT should play a role in educating countries about the increasing automation of attacks and how they can leverage ML and AI to combat these threats.

Risk and Opportunity: The Transition to Cloud

There are many benefits to organisations for both the public and private sector adopting cloud services. Cloud services can help organisations both public and private save costs and enable them to be agile and elastic – accessing and scaling resources up and down as required. With the outbreak of COVID-19, and the call for social distancing resulting in companies adopting work from home policies, more and more organisations are transitioning to the cloud. This trend is set to continue for some time to come and makes this a key opportunity to understand the importance of securing the cloud.

However as more and more organisations and governments around the world adopt cloud technologies, it will be important they understand some of the risks associated with cloud adoption and appreciate that cloud services are not secure by default. All organisations should be aware of the respective roles and responsibilities that they share with Cloud Service Providers (CSP) in managing the security of their cloud solutions and data stored in the cloud.

Organisations, including governments are also increasingly multi-cloud environments - meaning that they have a number of CSPs providing different services across their organisations. This can be problematic, as the organisation may have different security settings enabled with different CSP. It also can result in organisations having limited visibility as to the security across each environment.

Relatedly, organisations should consider automation in the context of cloud and what this might mean for improving cloud security. For example, automation can play a significant role in governance, recovery and management of these environments using telemetry, automation and cloud specific management strategies. Governments should be educated on robust operational practices, cybersecurity, and the fact that security controls are often easily circumvented in cloud environments lacking mature management practices.

DFAT should work with regional Governments to ensure that they understand the benefits of securely transitioning to the cloud.

Question 4: How should Australia pursue our cyber and critical technology interests internationally?

The work that DFAT has done to date and continues to do with respect to regional and global advocacy remains important. DFAT must continue this advocacy and build likeminded alliances with other countries to cooperate on initiatives and advocacy on key issues. In addition to continuing its advocacy via key international forums pertaining to cyber and critical technology sectors, we would like to reiterate the following as important ways Australia should pursue its interests:

SMEs at Key Diplomatic Posts

DFAT should consider placing dedicated SMEs at key diplomatic posts. These dedicated SMEs would ensure that Australia is well positioned to advocate on cyber and critical technology issues on the world stage, as they would have both the capacity and the technical/policy expertise to focus on these issues. Please see our “General Comments” for more information.

Strengthening Public-Private Partnerships

As noted above, working closely with the private sector will be important as Australia pursues its cyber and critical technology interest. Formal mechanisms should be established to facilitate regular engagement and ensure DFAT has the ability to

leverage the collective expertise and capabilities of the private sector. Please see our "General Comments" for more information.

Strengthening Regional Capacity Building and Cooperation

With the proliferation of technology developments and accompanying policy challenges it will be crucial that capacity building and education efforts in the Indo-Pacific are continued and expanded. It is critical that nations are educated about how they can effectively and securely adopt and deploy new technologies. It will also be important that the Australian Government is able to support these nations not just on a policy and legislative basis but also provide technical support and advice on a range of issues including operational matters and supply chain best practice, which is needed by many countries in the region.

The Australian Government may also need to consider a more targeted, regional focus for its law enforcement cooperation and capacity building efforts. While it makes sense to support international cooperation on cybercrime, Australia could work with five-eyes partners to ensure global coverage of law enforcement cooperation and capacity building initiatives. This would allow Australia to maximise its investment and align its focus on hotspot countries in the region. Strong relationships between investigators could also be developed via Australian cybercrime liaisons at posts and/or exchange programs.[7]

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

Please see our comments throughout this document on the importance of public-private partnerships and suggested useful mechanisms to leverage such partnerships.

Question 6: What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

[7] Cybercrime in Southeast Asia: https://www.aspi.org.au/report/cybercrime-southeast-asia

A number of countries around the world have demonstrated useful best practices that are worthy of consideration. We describe just a few below.

The Netherlands: The Netherlands continues to undertake a very impressive, outsize role in terms of international cyber and technology policy issues. The Dutch Government has held its International NCSC One Conference (a cybersecurity conference focused on policy/governance as well as technology trends) annually since 2008 (the 2020 ONE Conference has been cancelled due to COVID-19). Thousands of people from government, industry, and academia attend this conference, including from across Europe, the U.S., and beyond. The Dutch also have institutionalised cyber capacity-building efforts through the Global Forum on Cyber Expertise (GFCE), launched in 2015. In the GFCE over 70 organisations and countries work together on practical initiatives to strengthen cybersecurity, fight cybercrime, protect online data, and support e-governance around the world.

The United States: The U.S. Department of State (DFAT's counterpart) as well as the U.S. Agency for International Development (USAID) and U.S. Trade and Development Agency (USTDA) all undertake global capacity-building in cybersecurity, particularly in developing countries. A best practice of this work is the strong outreach all three agencies undertake to private companies to involve them in these efforts, including by jointly prioritising countries/ regions of focus, jointly planning events, and having companies speak at events and/or otherwise actively participate.

International Partners: Australia should look to some of its key partners, including but not limited to five-eyes partners, Japan and Singapore, on international policy to ensure alignment and deconflict on key policy initiatives, particularly in the region. Working collaboratively with key nation states and leveraging their work with respect to capacity building and deterrence/collective engagement, will be key in ensuring that Australia maximises its international advocacy.

Conclusion and about Palo Alto Networks

As the Australian Government embarks on the development of the *Cyber and Critical*

Technologies International Engagement Strategy Palo Alto Networks is ready to contribute our expertise and experience. We would be happy to discuss our ideas further. For more information, please contact Sarah Sloan, head of government affairs and public policy, Australia and New Zealand, at sasloan@paloaltonetworks.com and Sean Duca, chief security officer, Asia Pacific & Japan, at sduca@paloaltonetworks.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the future with technology that is transforming the way people and organisations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seises the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of security, protecting tens of thousands of organisations across clouds, networks, and mobile devices.

Palo Alto Networks is committed to helping the Australian Government and private organisations across all industry sectors embrace the digital world safely and protect their business operations from cyberattacks. Many of our customers are Australia's largest enterprises and government organisations. We also have undertaken a range of activities that contribute to strengthening Australia's cybersecurity posture, including hosting roundtables with government and enterprise stakeholders to promote thought leadership; and partnering with the education sector to design cybersecurity courses. For more information see https://www.paloaltonetworks.com.au/