SUBMISSION TO THE AUSTRALIAN DEPARTMENT OF FOREIGN AFFAIRS AND TRADE: CYBER AND CRITICAL TECHNOLOGY INTERNATIONAL ENGAGEMENT STRATEGY (CCTIES) – JUNE 2020

International Cyber Engagement Strategy 2020

VMware Submission: A Cyber Smart Asia-Pacific

vmware®

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information visit https://www.vmware.com/company.html

As one of the world's top five software companies with over 30,000 employees, VMware has a wide footprint across the Asia-Pacific with staff working in Australia, China, Hong Kong, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, Pakistan, Philippines, Singapore, Taiwan, Thailand and Vietnam.

We are optimistic technology has the potential to solve the big problems of our day. As believers in technology as a force for good we are committed to putting back more than we take and generating exponential positive global impact.

VMware is intrigued by the hardest problems and engage the brightest minds to solve them. Our deep expertise in nearly all aspects of cyber mean we are well positioned to support Australia's cyber engagement and cyber security strategies. VMware welcomes the opportunity provided by the Department of Foreign Affairs and Trade (DFAT) to do so through this submission to the Cyber and Critical Technology International Engagement Strategy (CCTIES). We are also able to leverage additional contributions to DFAT's process via relevant VMware experts participating in closed consultations and expert advisory panels.

To discuss any aspect of this submission please contact VMware Global Government Relations:

Richard Dowling
Policy Lead - Australia & New Zealand
Global Government Relations
richardd@vmware.com

Kristen Foster
Director & Head Asia Pacific & Japan Policy
Global Government Relations
kristenf@vmware.com

Executive Summary

The 2020 update of the **Cyber and Critical Technology International Engagement Strategy (CCTIES)** is taking place in an entirely different landscape than could ever have been imagined when the 2017 strategy was conceived.

This submission considers the questions raised by DFAT in its consultation guidelines. The submission also provides recommendations and delivers additional context on best practice cyber hygiene principles through the attached **Cyber Smart Index commissioned by VMware and undertaken by Deloitte Access Economics**.

Considered and principled long-term engagement in the cyber sphere can deliver enormous potential benefits for Australia and its regional partners. One quantified example comes from the VMware Deloitte Cyber Smart Index, which has found **US$145 billion additional GDP** can be unlocked by achieving best practice cyber hygiene across twelve Asia Pacific economies.

VMware is generally supportive of the existing CCTIES framework and sees merit in maintaining targeted progress against these objectives including promoting confidence in the online environment, increasing economic opportunities, reducing losses attributable to cybercrime, minimising the risks of strategic miscalculation in cyberspace, promoting multi-stakeholder Internet governance, protecting human rights online and delivering sustainable development outcomes.

Australia should continue to work with regional partners on these objectives and advocate for open rules-based digital trade within multilateral institutions.

Effective cyber engagement will also require Australia to lead by example and demonstrate best practice in all aspects of cyber security and governance. The advent of 5G promises to deliver a much more connected world. This submission advocates for a stronger and more explicit consideration of 5G communications technology in the CCTIES.

VMware Recommendations (outlined in more detail in the recommendations section):

Greater cyber harmonisation ○ *VMware recommends the CCTIES take a more proactive role in internationally advocating for best practice cyber harmonisation*
Leading by example ○ *VMware recommends that the Australia Government set an objective with measurable criteria to be a leader in best practice cyber hygiene principles and adopt internationally recognised cyber standards.*
Transparent reporting and measurable targets ○ *VMware recommends that the CCTIES continues to track and report on progress against its broad objectives and specific targets.* ○ *VMware recommends consideration of regional targets that can be reported on in partnership through regional institutions such as APEC.*
Promote digital trade agreements in multilateral institutions ○ *VMware recommends that Australia should be a leading advocate for the adoption of digital trade agreements within multilateral institutions.*
Developing Skills ○ *VMware recommends that the CCTIES recognise the opportunity to develop cyber skills for the benefit of the domestic economy, to meet global skills shortages and to export cyber leadership and best practice education to the region.*
Recognition of 5G communications technology ○ *VMware recommends the CCTIES recognise 5G as a critical technology with consideration of the economic, security and geopolitical benefits and implications.*
Whole of Government Approach to Cyber Security ○ *VMware recommends that the Australian Government adopt a whole of government approach to international cyber engagement.*
Leverage the private sector ○ *VMware recommends that the CCTIES utilise the considerable skills and experience of the private sector to provide ongoing advisory support to effectively guide and implement Australia's cyber strategy. VMware would also welcome being appointed to the Expert Advisory Panel.*

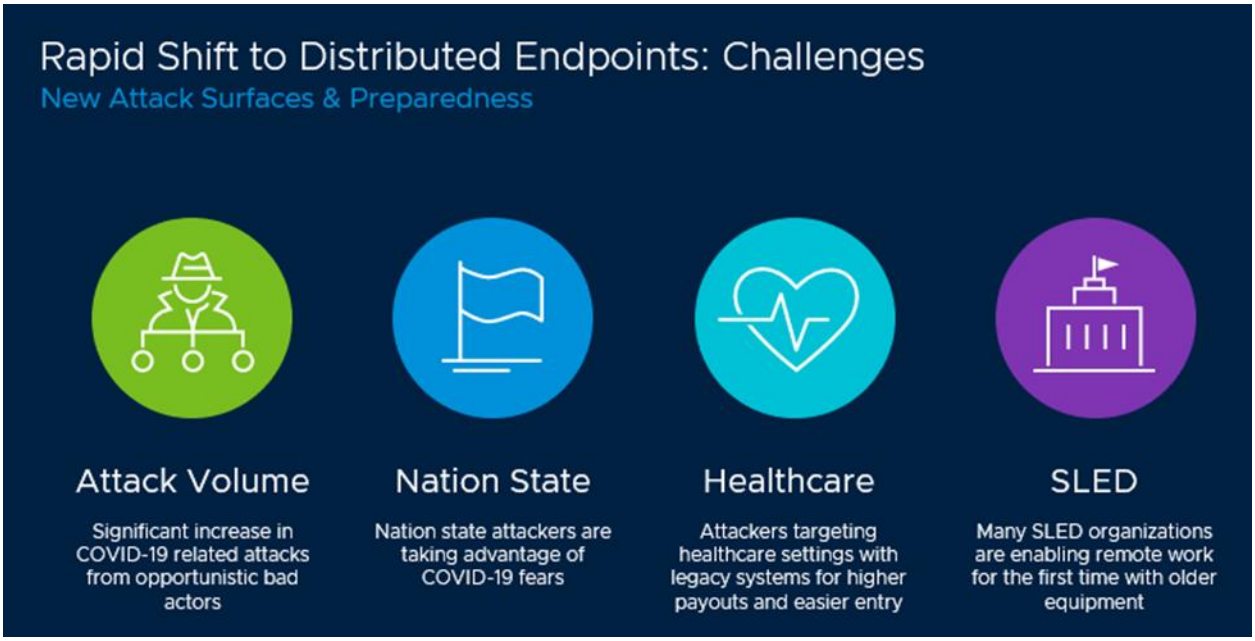
VMware Deloitte Cyber Smart Index 2020: Enabling APAC businesses

As many as three in five businesses in the Asia Pacific region have put off digitization plans out of fear of cyberattacks, according to the **Deloitte Access Economics Cyber Smart: Enabling APAC Businesses Report, commissioned by VMware**. The report analyses cyber exposure, preparedness and economic opportunity across 12 economies in the region. A key finding is that a cyber smart Asia Pacific can unlock as much as 0.7 per cent or **US$145 billion additional GDP** growth over the next ten years.

VMware views this contemporary and original research as a highly complementary input to the CCTIES and would welcome the opportunity to present the findings at appropriate forums.

The attached VMware Deloitte Cyber Smart Index forms a key component of this submission and is supplemented by VMware's responses to the consultation questions below. The VMware Deloitte Cyber Smart Index is publicly available on the VMware website - *https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/company/vmw-cyber-smart-enabling-apac-businesses.pdf*

In addition to the Cyber Smart Report, VMware continues to closely monitor changes to the international cyber security landscape. A noticeable trend has a been managing the challenge of a rapid shift to distributed endpoints accompanied by an increased attack volume, including from nation states. The infographic below depicts the context of this increased attack surface and related challenges.



SLED: State, Local and Education Government

Q1 - 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 first International Cyber Engagement Strategy in 2017 set a broad framework of goals and actions. VMware is generally supportive of this framework and sees merit in maintaining targeted progress against these objectives including promoting confidence in the online environment, increasing economic opportunities, reducing losses attributable to cybercrime, minimising the risks of strategic miscalculation in cyberspace, promoting multi-stakeholder Internet governance, protecting human rights online and delivering sustainable development outcomes.

Regular updates and progress reports should continue to be provided to ensure the strategy remains a living document that meets the contemporary challenges of effective cyber engagement. Tangible and transparent progress also supports the case for further budget allocations to support specific measures within the strategy.

Most critically, the objectives must connect with and be meaningful to the cyber priorities of other Asia Pacific nations and globally strategic partners. The overarching mission for an engagement strategy is to work in partnership with our region rather than serving as a document for domestic policy. As a regular participant in regional and industry dialogue on cyber affairs, VMware is able to provide ongoing feedback to DFAT on key cyber priorities across the Asia Pacific.[1] Most recently, the company has been very active through the American Chamber of Commerce network in the region to present the findings of the abovementioned VMware Deloitte Cyber Smart Index.

The inclusion of critical technology into the engagement framework is a welcome addition. For many Asia Pacific partners, basic digital infrastructure and capabilities serves as a roadblock to full cooperation and engagement. While nearly nine in ten Australians are Internet users, this is not the case within the wider region with only six in ten Indonesians and four in ten Indians using the Internet.[2] However, this also means that with the right support this region stands to have enormous further upside from being provisioned with critical infrastructure and being cyber engaged.

There is strong merit in the CCTIES continuing to emphasise an open, free and secure Internet. On a governance spectrum, the Internet and ultimately society has derived net benefits from a model of permissionless innovation.[3] Permissionless innovation refers to the notion that experimentation with new technologies and business models should generally be permitted by default. Unless a compelling case can be made that a new in invention will bring serious harm to society, innovation should be allowed to continue unabated and problems, if any develop, can be addressed later.

The benefits of innovation from a free and open marketplace for ideas should of course be balanced with best practice security and rule of law. VMware has previously commented that certain 'bad apples' have worked to undermine confidence in technology as a societal force for good.[4] Ultimately the cybersphere and its supporting technology is morally neutral. It can be harnessed for both good and evil.

The COVID-19 climate has seen an increase in the latter, with the Australian Security Intelligence Organisation Director-General of Security warning that "…the coronavirus pandemic has made Australia less safe, with spies, hackers and terrorists looking to do more harm online."[5]

---

[1] See Appendix A for example of VMware's APAC digital monitoring activities
[2] https://www.internetworldstats.com/
[3] https://permissionlessinnovation.org/what-is-permissionless-innovation/
[4] https://www.afr.com/technology/us-s-best-ceo-wants-google-and-facebook-regulated-and-bitcoin-banned-20191119-p53c2i
[5] https://www.smh.com.au/politics/federal/covid-has-made-australia-less-safe-asio-boss-20200608-p550hv.html

The default setting should be to maintain an open and free digital environment and any intervention should be grounded in a principle of 'first do no harm'. Where policy interventions do occur they should seek to empower technology to do good -

> *I sincerely and equally believe that technology has the opportunity to expand the life of every human on the planet and eradicate diseases that have plagued mankind … to give modern education to every child on the planet … to lift the remaining 10% of the planet out of poverty, and reverse the implications of climate change."*[6]
>
> Pat Gelsinger, VMware Chief Executive

Utilising cyber strategy as a platform for achievement of Sustainable Development Goals should be retained as key element of the 2020 CCTIES. The challenges we face as a global community are complex and deeply entrenched. In order to make substantive progress in areas such as healthcare access, financial inclusion and environmental sustainability, there needs to be greater collaboration in the cyber sphere across both the private and public sectors.

The United Nations' Sustainable Development Goals are a blueprint to achieve a better and more sustainable future for everyone, laying out detailed strategies to address issues as diverse as extreme poverty, inequality, climate, environmental degradation, prosperity and peace and justice.

Q2 - How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?

This remains an open question with a high degree of uncertainty. What we do know is that efforts to create an open and peaceful cybersphere can unlock benefits similar to the enormous poverty reduction that has occurred as a result of a multilateral trading system that has evolved since the second world war. The increasing prevalence of digital economy components in new free trade agreements is a sign that we are on the right pathway.

Within our own region, Singapore has been a leader formalising digital economy agreements, both at a bilateral level with Australia and trilaterally with Chile and New Zealand.

These agreements recognise the importance of digitalisation of business models and free trade in the cyber landscape in addition to the physical landscape. As Prime Minister Morrison has noted, these agreements as well as cooperation on cybersecurity are about "sharing a resolve to promote an open, interoperable, resilient and secure cyberspace….which will enhance information exchanges on cyber and critical technology priorities, best practices and training, and advance bilateral operational sharing and cooperation to strengthen cyber resilience, as well as joint regional capacity building efforts."

Further progress toward such a secure and cyber resilient environment can be achieved by continuing to prioritise digital agreements with Australia's major trading partners and ultimately promoting widespread adoption through the multilateral trading system. It was therefore encouraging to see a cyber agreement as part of the Comprehensive Strategic Partnership between Australia and India announced when Prime Ministers Morrison and Modi met virtually in June 2020.

Now more than ever before, cyber security should form a core part of such agreements. The need to have well understood norms, practices and laws governing the cyber domain are critical as more people work remotely and study online. Establishing a clear baseline of standards and harmonised rules can generate significant benefits and ease the disruption and trust concerns associated with digital transformation.

---

[6] https://www.zdnet.com/article/technology-as-a-force-for-good-the-vmware-plea/

The unprecedented levels of prosperity over the past century owe a great debt to the rule of law and appropriate proper enforcement mechanisms. The modern equivalent to be aiming for is a secure cyber space. The cyber sphere needs to be seen as a trusted environment where bad behavior has consequences just as it does in the traditional economy and in the physical world. The risk-reward tradeoff for bad actors needs to be set very high so as efficiently to deter nefarious and malicious activity.

There are signs that the promise of digital prosperity could be impeded when three in five businesses across the Asia Pacific have put off digital transformation because of cyber fears.[7] The consequence of cyber aversion is a direct threat to achievement of nearly all sustainable development goals.

As such, VMware asked Deloitte Access Economics to calculate how much economic value was being left on the table if the Asia Pacific region does not embrace the cyber opportunity. Deloitte Access Economics modelled a scenario where organisations have confidence that cyber risks are well managed. In this scenario, there is a reduction in risk aversion when evaluating new technology and digital projects. This supports a higher adoption rate of new technologies, in turn leading to higher levels of capital investment and productivity growth. This could lift annual real GDP by 0.7 per cent over ten years. Across just 12 APAC countries[8], this would translate to a lift in GDP of US$145 billion in the long term.[9]

In response to the COVID-19 pandemic, people are using the Internet for critical information and services and to contribute their labour from the safety of their homes. Technology is allowing millions to maintain their economic contribution in a pandemic, supporting the national economy. More broadly, we are permanently shifting to a more digitally connected world that shapes every aspect of how we learn, play, work and live. The upshot is that the four billion people globally who are not yet online are now getting even more marginalised.[10] While many Australian schoolchildren quickly jumped online when their schools closed, half the world's population still lack connectivity to complete schoolwork at home.

> *As we Build Back Better, it's imperative that we double-down not only on building our 5G network but also reaching inner cities and rural areas. This is our opportunity to accelerate universal connectivity, including greater support for global initiatives like Internet for All* [11]
>
> Pat Gelsinger, VMware Chief Executive

The pandemic response also presents a catalyst to democratise skills training at scale. In particular, there must be a focus on digital-skills training as core to the recovery, with a focus on massively expanding access to jobs of the future.

There is significant potential upside into supporting cyber security skills development both domestically and across the region. Globally, the cyber security market is expected to reach US$170 billion in 2020.[12] The importance of this sector to the region is notable due to the Asia Pacific experiencing the highest cyber losses (as a proportion of gross regional product) globally.[13] As a result, cyber spending in APAC is expected to grow faster than the global average with an additional $31 billion to be spent by 2026.[14]

---

[7] https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/
[8] Australia, New Zealand, Singapore, Japan, Malaysia, Indonesia, South Korea, India, Philippines, Thailand, Sri Lanka and Vietnam.
[9] https://www2.deloitte.com/au/en/pages/economics/articles/cyber-smart-enabling-apac-businesses.html
[10] https://www.linkedin.com/pulse/build-back-better-turning-turmoil-lasting-pat-gelsinger/
[11] ibid
[12] Australian Trade and Investment Commission 2016, Cyber Security US clusters
[13] http://www.hfw.com/downloads/The-Rise-of-Cyber-Crime-in-Asia-Pacific-August-2019.pdf
[14] https://www.austcyber.com/resources/sector-competitivenessplan/chapter1

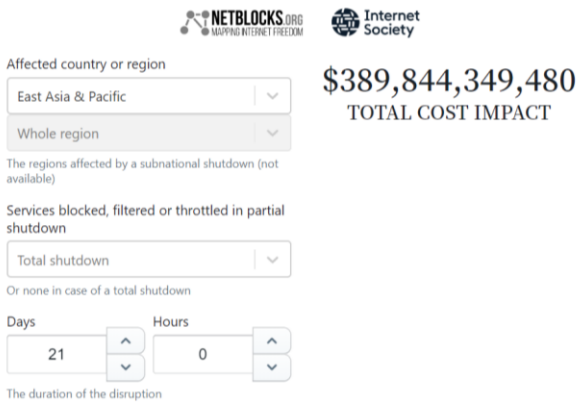
Businesses in the region are significant buyers of cyber security solutions. Cybersecurity expenditure in Southeast Asia alone was estimated at US$1.9 billion in 2017. This is projected to grow to US$5.5 billion by 2025.[15] The cyber security market in APAC was valued at US$22 billion in 2017.[16]

As the Asia Pacific develops its cyber systems, this presents an opportunity for services exports. Countries with leading cyber capabilities may enjoy a competitive advantage and win cyber business in countries with lagging policy and regulatory environments. There is also likely to be participation of cyber experts from mature markets in the US and Europe. Countries will also need to have investment regulation settings right if they wish to encourage global players to establish locally to deliver bespoke cyber services in-market.

Q3 - 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?

As the COVID-19 pandemic has shown, our interconnected world is a fragile place and vulnerable to biological, human and cyber disruptions. Experts have warned that we should prepare for a COVID-like global cyber pandemic that could spread faster and further than a biological virus, with an equal or greater economic impact.[17]

The consequences of a global cyber pandemic are difficult to fathom and potentially devastating. By way of illustration, using the NetBlocks Cost of Shutdown Tool, a single day without the Internet in the East Asia & Pacific Region would cost more than US$18 billion. A 21-day global cyber lockdown would cost almost US$400 billion.[18]



Cyber security is predominantly viewed through lenses of threat and risk. Given that it is a known threat, with fat tail risks, it is entirely rational to take very strong preventative measures. Moreover, where the threat does emerge, early and decisive action is warranted.

[15] https://theaseanpost.com/article/southeast-asiascybersecurity-emerging-concern
[16] https://www.mordorintelligence.com/industry-reports/asia-pacific-cybersecurity-market
[17] https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/
[18] https://netblocks.org/cost/

As demonstrated in the VMware Deloitte Cyber Smart Index, cyber security should not however be viewed *exclusively* as a threat. By becoming more cyber prepared and aware, nations can strategically build digital infrastructure and systems to become more economically competitive.

VMware views the advent of 5G communications as one of the most revolutionary technological advancements of our time. 5G could affect our lives more dramatically than any technology shift since the internet itself, because 5G enables us to realise the potential of a fully connected world.

As the recent Australian Parliamentary Inquiry into the deployment, adoption and application of 5G in Australia noted, "The capabilities of 5G are exciting, and offer the opportunity for innovation and connectivity. We are at a point where enough is known about the standards and safety of 5G technology to allow businesses of all sizes, communities, governments and individuals to imagine new use cases and new opportunities and help them come into being".[19]

The report found significant collaboration opportunities exist between Australia and trusted nations to cooperate on the rollout of 5G. VMware shares this view and believes that 5G should adopt the same open architecture principles and protocols that underpin the Internet.

Effective cyber engagement relies on a more connected world. At a global level, 5G promises to play a major part in providing this connectivity that could create $3.6 trillion in economic output and 22.3 million jobs by 2035.[20]

When coupled with technology solutions such as the internet of things, artificial intelligence, or big data, 5G holds the potential to deliver large-scale societal value. Regulators, industry associations, network operators, service/technology providers and public-private partnership organisations also must engage in continuous dialogue to address the challenges facing widespread 5G adoption worldwide. This collaboration is also needed to maximize the opportunities 5G will bring across sectors.

VMware supports more explicit consideration of the economic, security and geopolitical benefits and implications of 5G in the 2020 CCTIES. There is significant international dialogue on these aspects of 5G and a coordinated whole-of-government approach is warranted to capture the rich 5G cyber engagement opportunities on offer.

Q4 - How should Australia pursue our cyber and critical technology interests internationally?

Q5 - How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?

Q6 - What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

Australia has a strong history as an advocate for a rules-based multilateral trading system. It has served the national interest and delivered mutual benefits to its trading partners. When pursuing its digital and cyber interests, Australia would be well served by building upon this foundation. The transmission of data and information across borders should be as free and seamless as possible, with intrinsic security and privacy by design.

A positive enabling environment for digital trade includes consideration in trade agreements, harmonisation of standards, low impact regulation and few barriers to entry.[21] Consistency in pursuing these objectives, in

[19] https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024373/toc_pdf/TheNextGenFuture.pdf;fileType=application%2Fpdf
[20] http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf
[21] See Appendix A for a summary analysis of current cybersecurity and data protection arrangements across the Asia Pacific.

partnership with like-minded nations, will build trust that Australia is a genuine advocate for an open and transparent digital trade economy over the longer term.

Already we have seen positive steps with Australia negotiating rules to govern digital trade in the World Trade Organisation and through Free Trade Agreements and the Australia-Singapore Digital Economy Agreement. There is value to continuing to push digital trade onto the agenda of the G7/G20, the OECD and Asia-Pacific Economic Cooperation (APEC).

As a leader within the Asia Pacific, Australia should seek to implement best practice cyber hygiene principles. Not only does this bring benefits to the domestic economy, it allows Australia to export its expertise and cyber governance structures to its partners within the region.

It should be noted the Australian Government does not currently explicitly subscribe to international cyber standards such as *ISO27001* (Information Security Management)[22] or the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*[23]. While the Information Security Manual may seek consistency with these frameworks, the lack of active participation in such globally recognised standards has the potential to constrain Australia's cyber leadership and governance exports in the region.

It is acknowledged that the Australian Government maintains an *Information Security Manual*[24], including *Strategies to Mitigate Cyber Security Incidents* (also known as the *Essential Eight*).[25] While these standards have many properties in common with internationally accepted cyber frameworks, they do not fully conform and are not recognised outside of Australia.

The practice of pursuing its own standards outside international frameworks constrains Australia's ability to advocate for harmonised best practice cyber hygiene standards. Moreover, the *Essential Eight* in its entirety is not mandatory for Australia Government agencies nor for state agencies. This could open Australia to criticism that while it may advocate for best practice cyber principles, its own cyber security standards sit outside globally agreed best practice, are self-regulated and without penalty for non-compliance.

The CCTIES should consider whether this practice is in the national interest in promoting a prosperous and open digital economy secured by best practice harmonised cyber governance.

The CCTIES has correctly noted that the digital economy broadly creates opportunities for SMEs and encourages innovation in their products and services, access to market intelligence, talent, financing and increasing competitiveness in local and global markets. Promoting closer integration of digital economies comes with significantly lower friction and cost than efforts required to enhance movement of physical goods and services.

A study by Data61 and AlphaBeta finds that digital innovation can deliver AU$315 billion in gross economic value to Australia over the next decade.[26] Given this potential, Australia should set a target and hold itself accountable to capturing this value. There is already precedent for such benchmarking activity such as the NSW Innovation and Productivity Scorecard.[27]

However, as is the shown in the VMware Deloitte Cyber Smart Index, the promise of a prosperous digital economy is wholly reliant on a secure cyber sphere and inherent trust in cyberspace. Some practical measures government can take to support a Cyber Smart economy are shown below:

[22] https://www.iso.org/isoiec-27001-information-security.html
[23] https://www.nist.gov/cyberframework
[24] https://www.cyber.gov.au/ism
[25] https://www.cyber.gov.au/publications/essential-eight-explained
[26] AlphaBeta. 2018. Digital innovation: Australia's $315B opportunity. AlphaBeta. Sydney.
[27] https://www.business.nsw.gov.au/support-for-business/innovation-and-research/research-series/scorecard

Integrating Australia's cyber economy into the global trading system through harmonisation and best practice leadership can deliver significant economic gain, as demonstrated in the VMware Deloitte Cyber Smart Index.

Delivering cyber protection support to Australia's supply chain can also secure economic benefits as well as critical technology and infrastructure. In light of the COVID-19 pandemic, there has been increased policy focus on securing Australia's critical supply chain, including from the National COVID-19 Coordination Commission[28] and the Australian Parliament 5G Inquiry.[29]

CCTIES should consider the role of government in protecting critical domestic and regional supply chains from cyber-attacks. While industry and individual enterprises must maintain a high degree of responsibility for protecting themselves, there can be much wider economic implications and spillovers from a cyber-attack on critical supply chains. In this respect there is merit in considering more proactive cyber engagement support for the nation's most critical and high value supply chains.

The VMware Deloitte Cyber Smart Index shows that only Singapore and arguably Japan are more cyber prepared than Australia. Fortunately Australia benefits from very strong diplomatic and economic relations with these nations and there is an opportunity for much closer collaboration in achieving best practice approaches to international cyber and technology policy.

[28] https://www.pmc.gov.au/nccc
[29] https://www.zdnet.com/article/inquiry-recommends-australia-reviews-5g-cyber-supply-chain-risks/

As Davis and Pipikaite note[30] "COVID-19 has revealed the importance of international, cross-stakeholder coordination. Cooperation between public and private sector leaders is also critical, particularly when it comes to mitigation." Their research proposes taking the lessons of the pandemic and translating it to cyber policy development and engagement. To that end, Australia could play a role in advocating for institutions that are equipped to address systemic cybersecurity challenges and improve digital trust across institutions, businesses and individuals.

Evolving Australia's diplomatic structures for the digital age is a momentous challenge, but it is also one with near limitless upside and almost no downside. Just as the rules-based multilateral stakeholder system facilitated trade in physical goods and services, with significant economic benefits, a contemporary cyber engagement strategy can unlock an even greater wave of digital trade that if managed properly will deliver tangible improvements for Australia and for the world's sustainable development goals.

[30] https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/

Recommendations

Greater cyber harmonisation

VMware recommends the CCTIES take a more proactive role in internationally advocating for best practice cyber harmonisation

Regulatory approaches to cyber in Asia Pacific are varied and localised, as economies with different levels of risk and preparedness approach the issue differently. While local approaches can be justified, they can have unintended flow-on effects. For businesses operating across borders, they need to understand and comply with varying regulations regionally which can add regulatory burden without necessarily contributing to stronger preparedness. For regulators themselves, fragmentation can make it more challenging to penalise cyber-crime. Finally, as below, for the Australian Government to be perceived as a cyber leader it should consider adopting and implementing internationally recognised cyber security standards beyond the *Essential Eight*.

Leading by example

VMware recommends that the Australia Government set an objective with measurable criteria to be a leader in best practice cyber hygiene principles and adopt internationally recognised cyber standards.

Governments have a significant digital presence and hold a wealth of valuable data about individuals, businesses and national matters. In this context, it is crucial that governments themselves observe cyber security best practice. The CCTIES rightly has an ambition to provide cyber leadership in the Asia Pacific – one the most effective ways to do this is by example – both as signal to business and government partners.

Transparent reporting and measurable targets

VMware recommends that the CCTIES continues to track and report on progress against its broad objectives and specific targets.

VMware recommends consideration of regional targets that can be reported on in partnership through regional institutions such as APEC.

Regular updates on maintaining targeted progress against these CCTIES including promoting confidence in the online environment, increasing economic opportunities, reducing losses attributable to cyber-crime, minimising the risks of strategic miscalculation in cyberspace, promoting multi-stakeholder Internet governance, protecting human rights online and delivering sustainable development outcomes. Most critically, the objectives must connect with and be meaningful to the cyber priorities of other Asia Pacific nations and globally strategic partners.

Promote digital trade agreements in multilateral institutions

VMware recommends that Australia should be a leading advocate for the adopting of digital trade agreements within multilateral institutions.

Australia and its regional partners such as New Zealand and Singapore have shown a genuine commitment to promote digital trade. Already we have seen positive steps with Australia negotiating rules to govern digital trade in the World Trade Organisation and through Free Trade Agreements and the Australia-

Singapore Digital Economy Agreement. There is value to continuing to push digital trade onto the agenda of the G7/G20, the OECD and Asia-Pacific Economic Cooperation (APEC).

Developing Skills

VMware recommends that the CCTIES recognise the opportunity to develop cyber skills for the benefit of the domestic economy, to meet global skills shortages and to export cyber leadership and best practice education to the region.

As cyber defences develop, so too does the nature of cyber-attacks. Countries need to develop the skills to ensure that businesses are prepared for this threat in the future. The current skills shortage for APAC is 2.6 million and rising. This represents the largest regional shortage in the world.

Recognition of 5G communications technology

VMware recommends the CCTIES recognise 5G as a critical technology with consideration of the economic, security and geopolitical benefits and implications.

Significant collaboration opportunities exist between Australia and trusted nations to cooperate on the rollout of 5G. VMware believes that 5G should adopt the same open architecture principles and protocols that underpin the Internet.

Whole of Government Approach to Cyber Security

VMware recommends that the Australian Government adopt a whole of government approach to international cyber engagement.

The creation of Australia's inaugural Ambassador for Cyber Affairs has delivered an ability for the nation to speak with one cyber voice through international diplomatic channels. This approach should be extended across the executive level of government including consideration of reinstating a dedicated Minister for Cybersecurity or Cabinet subcommittee.

Leverage the private sector

VMware recommends that the CCTIES utilise the considerable skills and experience of the private sector to provide ongoing advisory support to effectively guide and implement Australia's cyber strategy. VMware would also welcome being appointed to the Expert Advisory Panel.

As a company with an extensive footprint in the region and as a regular participant in regional and industry dialogue on cyber affairs, VMware is able to provide ongoing feedback to DFAT on key cyber priorities across the Asia Pacific. VMware has a range of internationally engaged and highly experienced executives that would be prepared to assist in expert advisory panels.

Appendix A

Summary Analysis - Cybersecurity and Data Protection in the Asia Pacific

Country	Key points (includes *hyperlinks*)
Singapore	• Leading country in ASEAN with its cybersecurity capacity and leadership • Key laws are *Cybersecurity Act (2018)*, *Personal Data Protection Act (2012)* and *the Computer Misuse Act* • Laws include measures to secure the critical information infrastructure in the country and norms regarding storage, use and disclosure of personal data • Engaging regional and global partners to engage in cybersecurity dialogues to enhance awareness and capacity building • In 2020, *Cybersecurity Labelling Scheme (CLS)* to address a growing area of concern on Internet of Things was launched • *Budget 2020 set aside S$1 billion* over the next three years to build up the Government's cyber and data security capabilities
Malaysia	• The recent cabinet shuffle appointed Datuk Saifuddin Abdullah as the new Communications and Multimedia Minister • Legislations that govern cybersecurity are *Computer Crimes Act (1997)*, the *Digital Signature Act (1997)*, and the *Communications and Multimedia Act (1998)* • Recently the government replaced Domestic Security Policy with the *updated Public Security and Safety Policy* in order to better tackle threats originating from digital activities, including cyber threats. • In 2020, Personal Data Protection Commissioner issued Public Consultation Paper No. 1/2020 to update *Personal Data Protection Act 2010* that also includes provisions on processing of personal data in cloud computing and privacy by design principles
Thailand	• Recently enforced a series of laws related to cybersecurity including the *Cybersecurity Act* and *Personal Data Protection Act (PDPA)*. The effective date of the Personal Data Protection Act B.E. 2562 (2019) (PDPA) has been postponed by 1 year, as proposed by the Ministry of Digital Economy and Society (MDES). • Both laws were announced in May 2019 and stakeholders were given a one-year grace period to adapt. Cybersecurity Act was published in the *Government Gazette* on 27 May 2019 and is in effect • Government has made investments in securing the cloud infrastructure of governance and banking sectors. Recent implementation of the law is predicted to enhance cybersecurity investments in both public and private sector. • Critics view the Cybersecurity law as another tool for silencing dissent in the country. The new law has categorized threats into 3 categories, based on their level of risk or severity: non-critical, critical and crisis • Recruitment for the National Personal Data Protection (PDP) Committee from different groups of stakeholders has commenced in Thailand.
Indonesia	• *Contemplating the draft cybersecurity bill since 2018* but the process has been halted recently • regulations that govern cybersecurity in the country include *Electronic Information Transactions Law (2008)* which is being enforced in several ways • It remains to be seen whether the government will move forward with the bill or make other amendments to the same before enaction • Government will speed up mutual works with the House of Representatives in the deliberations of the bill on personal data protection • The recent replacement of government regulation no. 82 by *government regulation no. 71* and accompanying ministerial regulations in 2020 will form the basis of cyber security and data processing by the cloud service providers
The Philippines	• Launched *National Cybersecurity Plan 2022* to guide legislations and implementation regarding cybersecurity • Country has strong laws in place like the *Cybercrime Prevention Act* and *Data Privacy Act* of 2012 • Critics have pointed out how the law does not sufficiently protect freedom of speech and data privacy • In 2020 Philippines data protection law—Republic Act No. 10173, called the Data Privacy Act of 2012 (DPA), was released for a public consultation. There are two pending bills at the House of Representatives. One (*House Bill No. 1188*) seeks to impose stiffer penalties on violations of the law. The second (*House Bill No. 5612*) covers a wide range of issues and is poised to have a tremendous impact on the implementation of the law
Vietnam	• *Cybersecurity law*, came into effect on January 1, 2019, has been blamed for the overwhelming powers granted to the government, allowing it to investigate online content users and censure digital content that goes against the government's agenda • Law also imposes data localization requirements on foreign service providers • PM requested the Ministry of Public Security to finalize and submit the draft decree guiding the Law on Cyber Security no later than *March 15, 2020*. The government planned to issue this decree no later than April 15, 2020. However, there is no development thereafter. • Cybersecurity Law will result in greater compliance among service providers when the authorities request them to provide service users' identities if a violation of the law is detected

Country	Key points (includes *hyperlinks*)
Cambodia	• Cambodian *ICT Masterplan 2020* by Ministry of Posts and Telecommunications • Currently reviewing a draft law on cybercrime by referring to other such laws enacted in the region and beyond • Cambodia has experienced relatively low cyber threat, *especially decreasing from 2017 to 2018*. Yet, nearly 68% of the population still experiences some form of cyberattack every year • Cambodia's *E-commerce Law* regulates the activities of e-commerce service providers and intermediaries and imposes consumer protection obligations, including data protection and cybersecurity obligations, on all e-commerce businesses
Myanmar	• Attacks on networks and devices within Myanmar appear to be on the rise, as they are globally. However, Myanmar does not currently have in place an overall cyber security framework, nor specific laws for cybercrime or data protection • *e-Governance Master Plan (2016-2020)* Draft by Ministry of Communications and Information Technology • Japanese government is providing *support to Myanmar* to come up with a cybersecurity law that will govern internet-related activities, particularly e-commerce.
Lao PDR	• Has a *national policy on cybercrime* however it is insufficient to address the growing landscape of cyberthreats in the region • More comprehensive cybersecurity policy is lacking at this point
Brunei	• In March 2019 declared that it plans to *establish a National Cybersecurity Center* for tackling cyberthreats • National policy in this regard is yet to be drafted • *Takaful Brunei* Am Sdn Bhd (TBA) recently developed an innovative *Takaful* protection scheme to tackle the increasing risks of cyber threats where the TBA's Cyber Security Takaful protection scheme assists large business entities, large private companies and government-linked companies • *Protection scheme* is also developed for SMEs, in managing risks that arise from breached critical information infrastructures. Protection scheme covers Privacy Liability, Network Security Liability, Media Liability, Cyber Extortion, Data Asset Loss and Business Interruption
South Korea	• South Korea recognizes that cyber-security is a matter of national security. Although the country boasts one of the world's fastest and most mobile IT infrastructures, it also has an insecure infrastructure that is vulnerable to cyber-attacks. The frequency and gravity of cyber-attacks has prompted the South Korean government to re-evaluate its cyber-security strategy. There are three agencies equipped to handle issues of cyber-security: The National Cyber-Security Center, the Korea Internet and Security Agency (KISA), and the National Police Agency's Cyber Terror Response Center. These agencies are responsible for identifying, preventing, and responding to cyber-attacks and security threats. • Key regulations include the *Personal Information Protection Act (PIPA)* and the "*Act on Information Network Promotion and Safety Act*" (Network Act) • Laws apply to any "Personal Information Controller" which can be "a public institution, legal person, organization, individual that processes personal information directly or indirectly to operate the personal information files for official or business purposes." With this broad scope, PIPA has a very direct impact on all businesses in South Korea or doing business with South Korean citizens. • On January 2020, *Korean National Assembly passed amendments (collectively, the 'Amendments') to three major data privacy laws*: the Personal Information Protection Act ('PIPA'), the Act on the Promotion of Information and Communications Network Utilization and Information Protection ('Network Act') and the Act on the Use and Protection of Credit Information ('Credit Information Act').

Ends

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.