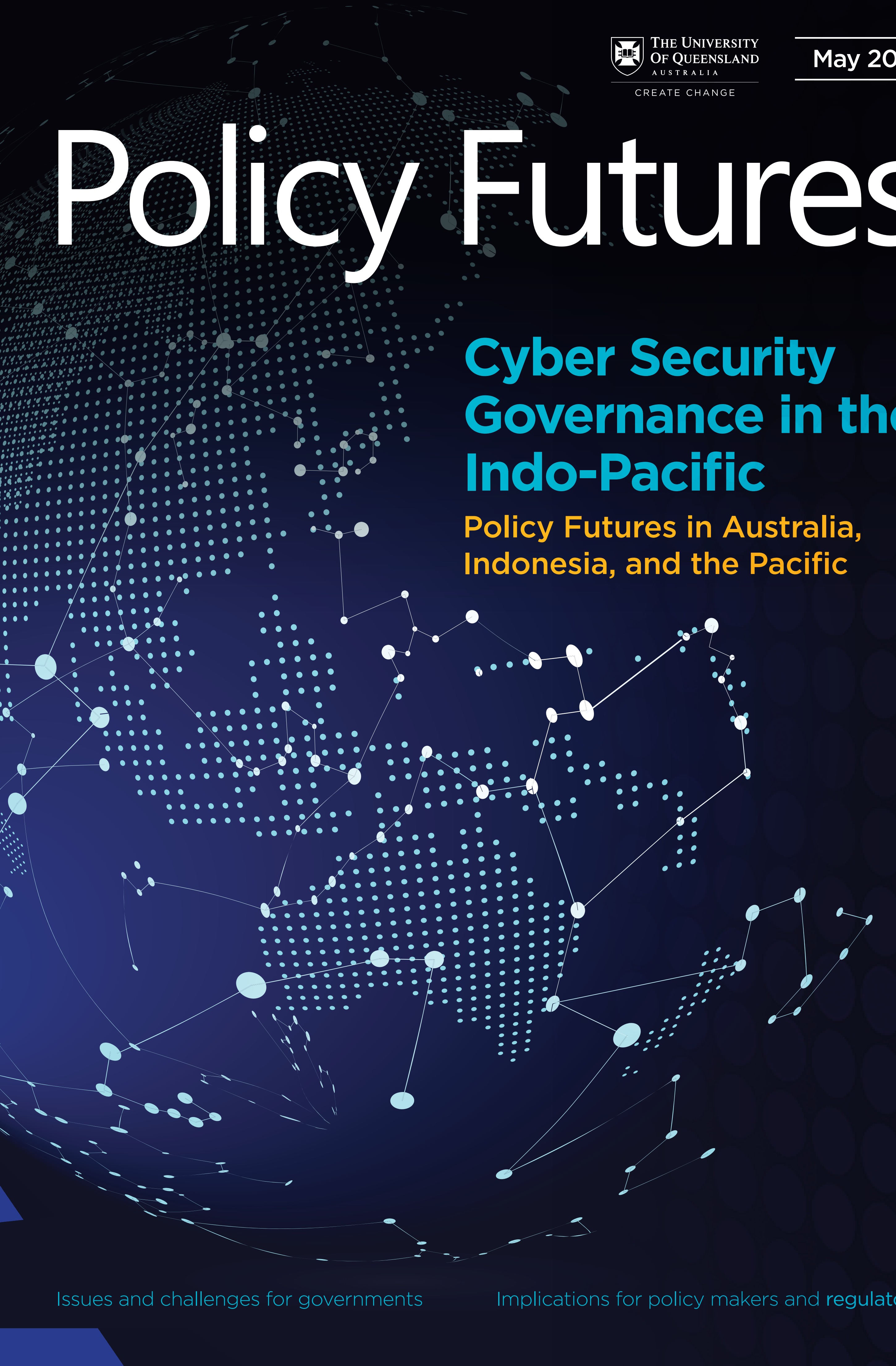
The University of Queensland
Australia
Create Change

May 2021

Policy Futures



Cyber Security Governance in the Indo-Pacific

Policy Futures in Australia, Indonesia, and the Pacific

Issues and challenges for governments

Implications for policy makers and **regulators**

This publication was edited and produced under the direction of the Centre for Policy Futures at The University of Queensland (UQ), St Lucia, Australia.

Date of publication: 10 May 2021.

Coordinating Author and Editor: Dr Greta Nabbs-Keller, Research Fellow Southeast Asia and the Indo-Pacific, Centre for Policy Futures, UQ.

Editor: Dr Jennifer Yarnold, Research Fellow, Centre for Policy Futures, UQ.

Key Contributors: Professor Ryan Ko, Chair and Director Cyber Security, School of Information Technology and Electrical Engineering, UQ; **Ms Tracey Mackay,** Director Cyber Security Strategy and Governance, Australian Department of Home Affairs; **Mr Nur Achmadi Salmawan S.Kom., M.M.,** Director of National Critical Information Infrastructure Protection, Indonesian National Cyber and Crypto Agency (BSSN); **Dr RM Wibawanto Nugroho Widodo**, Vice President Operational (*Pembina Harian*), Democracy and Integrity for Peace Institute (DIP), Indonesia and Expert Advisor to the Head of BSSN; **Dr Agus Hasan Sulistiono Reksoprodjo**, Lecturer in Asymmetric Strategy at Indonesian Defence University (Unhan).

Acknowledgements: The UQ Centre for Policy Futures would like to acknowledge the support of the Cyber, Digital and Technology Policy Division, and the Queensland and Northern Territory Office of the Department of Home Affairs. We also extend our appreciation to Indonesia's National Cyber and Crypto Agency (BSSN), Jakarta and UQ School of Information Technology and Electrical Engineering (ITEE) for assistance on this project. Our gratitude also to Ms Alexandra Kint, a UQ Centre for Policy Futures undergraduate Intern from the UQ School of Political Science and International Studies (UQ-POLSIS), who provided research assistance for this program.

Please cite this work as follows: Nabbs-Keller, G. Ko, R., Mackay, T., Salmawan, N.A., Widodo, W.N and Reksoprodjo, A.H.S. (2021). Cyber Security Governance in the Indo-Pacific: Policy Futures in Australia, Indonesia and the Pacific. *Policy Futures Series*. Nabbs-Keller, G. and Yarnold, J. (eds.). The University of Queensland. https://doi.org/10.14264/4364b42

Disclaimer: This content has been prepared by the UQ Centre for Policy Futures for the purpose of general information. It does not constitute professional advice, nor is it a substitute for such advice. The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the official views or position of The University of Queensland. Questions about the topics discussed may be directed to the UQ Centre for Policy Futures at: policyfutures@uq.edu.au or +61 7 3443 3118.

Contents

List of Acronyms 4

Recommendations 6

Executive Summary 8

Scope and Methodology 10

Introduction. 12

The most salient cyber security threats 13

Differences in threat perceptions between Australia and its regional partners 15

Key legislative and policy gaps in responding to the threats of the information age 17

Current shortfalls in coordination mechanisms among agencies tasked with cyber security responsibilities and how they can be improved. 19

Practical ways to ensure policy makers have a sufficient knowledge base and understanding to meet present and future cyber security challenges. 21

Innovative and practical ways in which governments, industry and the university sector can do more with our cyber security counterparts in Australia, Indonesia and the PICs to fill key capability gaps. 24

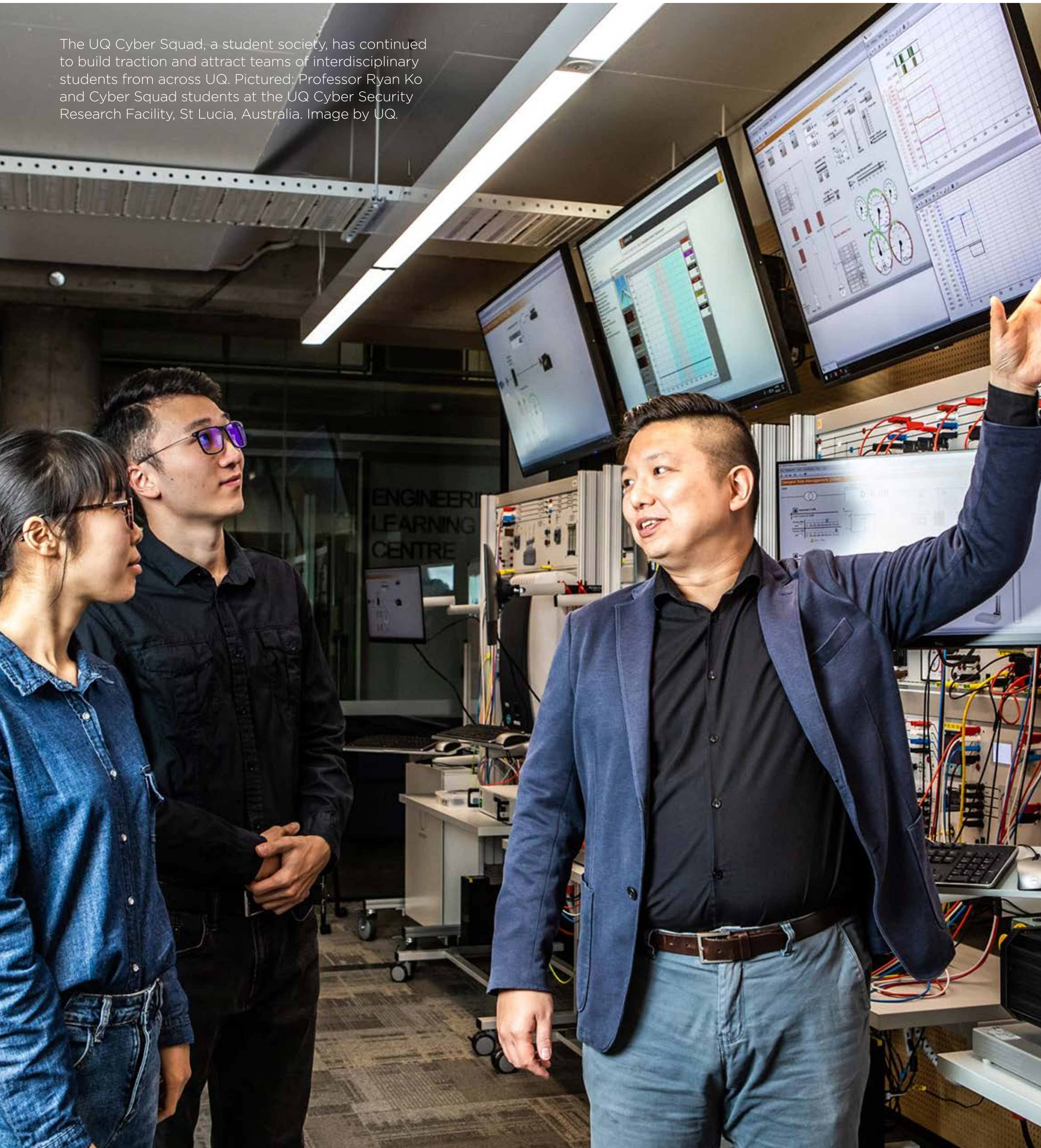
Appendix A: Promotional Flyer. 27

Appendix B: Bios of Chair and Expert Panel. 28

Notes and References 30

List of Acronyms

APNIC	Asia Pacific Network Information Centre
ASEAN	Association of Southeast Asian Nations
BSSN	Indonesian National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*)
BTS	Base Transceiver Station
CAPTCHA	Completely Automated Public Turing Test To Tell Computers and Humans Apart
CPF	Centre for Policy Futures
CERT	Cyber Emergency Response Team
CSIRT	Cyber Security Incident Response Teams
CyCon	International Conference on Cyber Conflict (NATO)
DDoS	Distributed Denial of Service attack
DFAT	Department of Foreign Affairs and Trade (Australia)
DIP	Democracy and Integrity for Peace Institute (Jakarta)
DNS	Domain Name System
DPR	Indonesian Parliament (*Dewan Perwakilan Rakyat*)
DUCTF	Down-Under Capture the Flag competition
FDI	Foreign Direct Investment
IoT	Internet of Things
MFA	Multi Factor Authentication
MSMEs	Micro, Small and Medium-sized Enterprises
NATO	North Atlantic Treaty Organisation
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology (US Commerce Dept)
NSOC BSSN	National Security Operations Centre – BSSN
NZ	New Zealand
NZQA	New Zealand Qualifications Authority
OT	Operational Technologies
PACSON	Pacific Cyber Security Operational Network
PICs	Pacific Island Countries
PROLEGNAS	Priority Legislative Agenda (*Program Legislasi Nasional*)
PUSANSIAD	TNI-Army (AD) Cyber and Crypto Unit
SATSIBER-TNI	Cyber Unit (*Satuan Siber*)
SMTP	Simple Mail Transfer Protocol
SOPs	Standard Operating Procedures
TNI	Indonesian Armed Forces (*Tentara Nasional Indonesia*)
UNHAN	Indonesian National Defence University (*Universitas Pertahanan Indonesia*)
UQ	The University of Queensland
UQ-ITEE	UQ School of Information Technology and Electrical Engineering



The UQ Cyber Squad, a student society, has continued to build traction and attract teams of interdisciplinary students from across UQ. Pictured: Professor Ryan Ko and Cyber Squad students at the UQ Cyber Security Research Facility, St Lucia, Australia. Image by UQ.

Recommendations

As a result of the online Roundtable Discussion and additional written submissions by several of the key contributors, the UQ Centre for Policy Futures presents twelve key policy recommendations that would impact positively on cyber security capability, cooperation and awareness between Australia, Indonesia and our Pacific partners.

Streamed Television Series

To increase public awareness of e-safety and cyber security threats, government could support the creation of a television series similar to the Australian Seven Network's highly popular *Border Security: Australia's Front Line*. This program could be streamed into Southeast Asia and the Pacific, and include subtitles.

Game-Changing Research

Invest in interdisciplinary game-changing research that provides strategic advantage to legitimate, rather than criminal actors, and which, through innovation and discovery, enhances cyber security for end-users and policing tools.

Internet Outage

In partnership with regional countries, prepare for a national and regional communication scenario with a minimal or complete internet outage.

University-based Competitions

Develop a sponsored university-based program in Australia, Indonesia and the PICs to facilitate regional competitions and problem-solving exercises, where students might solve hacking challenges (hack-a-thons), discover vulnerabilities and defend 'sand box' servers.

Centre of Excellence

Create a regional Centre of Excellence (CoE) based on the NATO Cooperative Cyber Defence CoE based in Tallinn, but adapted to the ASEAN, Australia, New Zealand (NZ) and Pacific Island Countries (PICs) context, which could facilitate collaborative research, replicate a conference similar to the NATO International Conference on Cyber Conflict (CyCon), engage in red teaming, live-fire challenges, and provide a safe and unclassified platform for interdisciplinary training and network building. The CoE could also establish a database of publications and national cyber security policy and legal documents, and an International Cyber Law Interactive Toolkit for regional policy makers and legislators.

Micro Credentials

Enhance regional policy makers' cyber awareness through subsidised bursaries for university-delivered online micro-credentialled programs that can quickly and effectively build policy makers' knowledge base and awareness.

Combined Exercises

Facilitate exercises, simulated attacks and war gaming between Indo-Pacific Cyber Security Incident Response Teams (CSIRT), emulating the approach of regional armed forces to combined training exercises.

Efficacy of Treaty Instruments

Consider research on countries who have acceded to The Convention on Cybercrime of the Council of Europe (Budapest Convention) to determine its efficacy for regional cyber security legislation and policy formulation.

Ransomware Data Breach Risk

Apply greater national focus and multinational coordination to take down and pursue malicious cyber actors engaged in data breach-related ransomware through exploitation of individual login credentials.

Institutionalised Regional Coordination and Communication Procedures

Enhance communication and coordination procedures and protocols among the national cyber agencies of Australia, Indonesia and the PICs to enhance emergency responses, including during live incidents.

Public Sector Key Performance Indicators

Consider the introduction of Key Performance Indicators (KPIs) on cyber security awareness for public sector officials, and integrate these into existing competency frameworks across Australia, Indonesia and the PICs.

Legislative Powers

Pass laws which clearly mandate Internet Service Providers' (ISP) and telecommunications companies' (telco) accountabilities and responsibilities to detect and mitigate Distributed Denial of Service (DDoS) attacks and to detect and stop mobile device phishing via text.

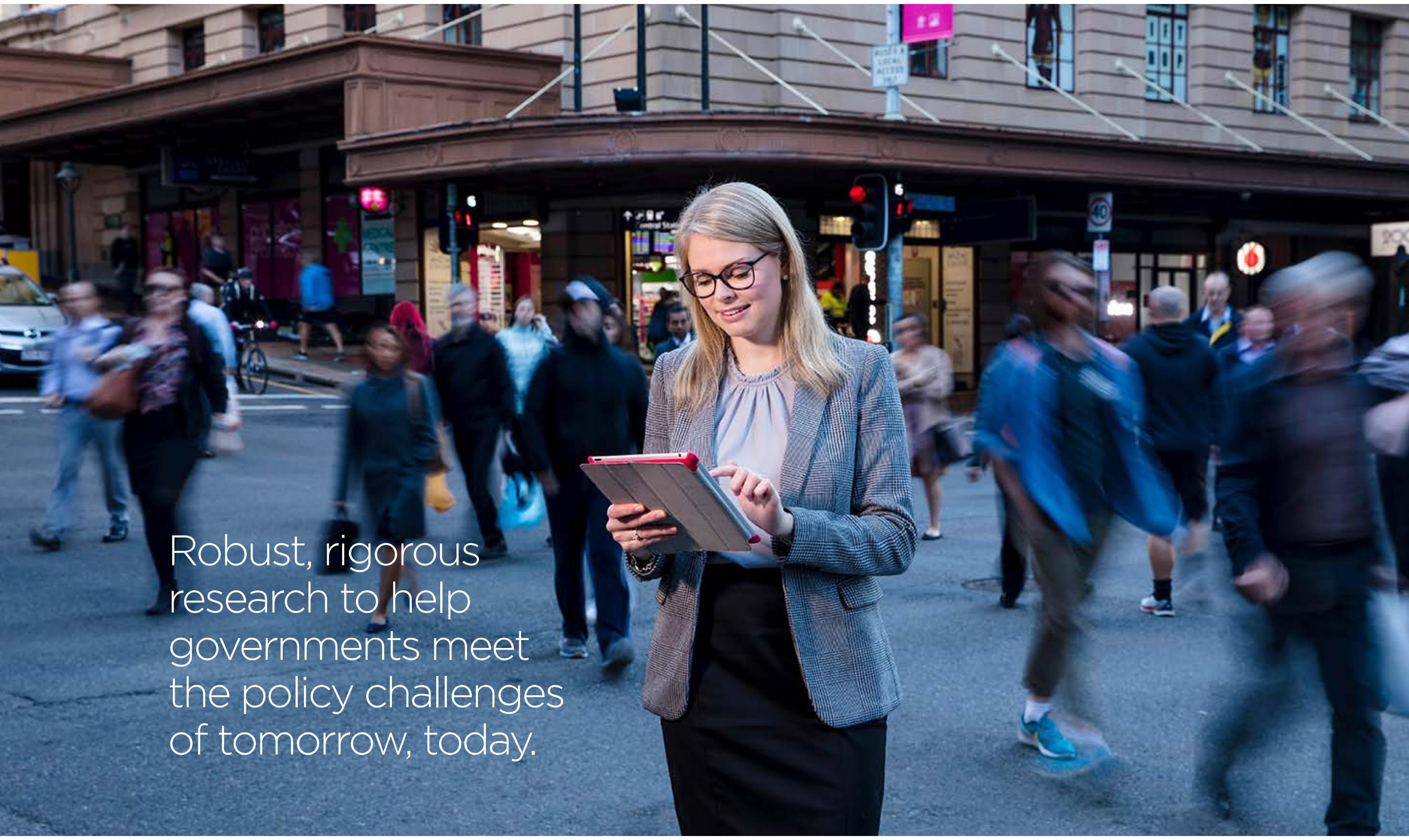
Executive Summary

The 'Cyber Security Governance in the Indo-Pacific: Policy Futures in Australia, Indonesia and the Pacific' Policy Engagement Program highlights strengths and weaknesses in regional cyber security governance. Importantly, it identifies key policy priorities from an Australian, Indonesian and Pacific Island Countries' (PICs) perspective and, through its recommendations, identifies new paths for cooperative engagement between Australia and its regional partners.

Notwithstanding the fact that Indonesia and the PICs have unique socio-political and economic contexts, the online Roundtable Discussion, which formed the foundation of this think piece, highlights many areas of commonality around threats and challenges in the cyber domain. Through an online exchange of ideas between experts from The University of Queensland (UQ), the Department of Home Affairs, Indonesia's National Cyber and Crypto Agency (BSSN), the Democracy and Integrity for Peace (DIP) Institute Indonesia, and the Indonesian Defence University (Unhan), one can see there are models and initiatives that can be replicated by countries pursuing their own paths to cyber security resilience in the face of rapid technological change.

In practical terms, the Roundtable Discussion highlights how Australia has defined its own regulatory and policy approach to defend governments, businesses, and communities from malicious cyber activity. Such an approach has lessons for countries like Indonesia, which is contending with legislative and policy gaps, weak whole-of-government coordination, and a relatively low knowledge base among legislators and policy makers. This is a problem not unique to Indonesia and, indeed, represents a challenge common also to many of the PICs. Ideas and expertise flow both ways, however, and our Indonesian experts have made innovative policy recommendations and identified areas for further engagement.

Based on the contributions of our panellists and contributors, there is clearly scope to further tailor regional capacity building programs through increased coordination, knowledge exchange, and workshopping of national cyber security legislation and strategic guidance. Inherent in *Australia's Cyber Security Strategy 2020* also, are solutions to Indonesia and the PICs' outreach and engagement objectives, particularly in the expansion of Joint Cyber Security Centres (JCSCs), which link federal government agencies to their sub-national counterparts and also to micro, small and medium enterprises (MSMEs). Finally, production of popular cyber security media programs, which could be subtitled and streamed across the region, hold promise for raising vital public awareness. Moreover, the think piece highlights the importance of universities as a source of innovation, interdisciplinary research and as a testbed for cyber security competitions, exercises, and ideas. We commend these recommendations to you.



Robust, rigorous research to help governments meet the policy challenges of tomorrow, today.

About the UQ Centre for Policy Futures

The UQ Centre for Policy Futures (UQ-CPF) seeks to enhance the University's position as a key source of ideas and insights on the policy priorities that matter to Australia and the Indo-Pacific region. This is achieved through robust, rigorous and timely research and sustained policy engagement. The 'Cyber Security Governance in the Indo-Pacific: Policy Futures in Australia, Indonesia and the Pacific' Policy Engagement Program brings together educators, expert advisors, and government officials in discussion. It leverages the interdisciplinary expertise of the UQ-CPF and UQ Cyber Security at the School of Information Technology and Electrical Engineering (UQ-ITEE).

For further information on the UQ-CPF, our researchers or specific recommendations in this publication, please email policyfutures@uq.edu.au or visit policy-futures.centre.uq.edu.au.

Scope and Methodology

Roundtable Discussion Format

The ‘Cyber Security Governance in the Indo-Pacific: Policy Futures in Australia, Indonesia and the Pacific’ Policy Engagement Program brought together a panel of four experts in a two-hour online dialogue on 6 October 2020. The event leveraged the interdisciplinary expertise of the UQ Centre for Policy Futures and UQ Cyber Security based at the School of Information Technology and Electrical Engineering (UQ-ITEE). It aimed to benchmark and compare Australian, Indonesian and Pacific Island Countries’ policy responses to the compelling issues of regional cyber security governance and resilience. A select number of invitations were extended to key academics and practitioners working on cyber security to view the discussion and ask questions.

Due to COVID-19 restrictions, the face-to-face format of the Policy Engagement Program’s Roundtable Discussion was adapted to an online format. Subsequently, the Roundtable Discussion provided a more succinct opportunity to elicit some innovative ideas and identify key policy imperatives from an Australian and regional perspective on pressing cyber security governance, policy, and capacity building issues.

Roundtable Panellists

Four expert panellists contributed their insights and recommendations to the Roundtable Discussion. The Australian Government was represented by Ms Tracey Mackay, the Director of Cyber Security Strategy and Governance, Cyber Policy and Strategy Branch, Cyber, Digital and Technology Policy Division at the Department of Home Affairs. Ms Mackay was joined by two Indonesian experts—Mr Nur Achmadi Salmawan, the Director of National Critical Information Infrastructure Protection at the Indonesian National Cyber and Crypto Agency (BSSN), and Dr R.M. Wibawanto Nugroho Widodo, Vice President Operational (*Pembina Harian*), Democracy and Integrity for Peace Institute (DIP) Institute and Expert Advisor to the Head of BSSN.

Professor Ryan Ko, UQ Chair and Director Cyber Security was the fourth panellist. Professor Ko has extensive capacity building expertise in the Pacific in establishing university-wide, multi-disciplinary academic research and education programs in New Zealand and Tonga. The online Roundtable Discussion was organised and moderated by Dr Greta Nabbs-Keller. Dr Nabbs-Keller is an Indonesian defence and foreign policy specialist, currently engaged as Research Fellow Southeast Asia and the Indo-Pacific at UQ-CPF.

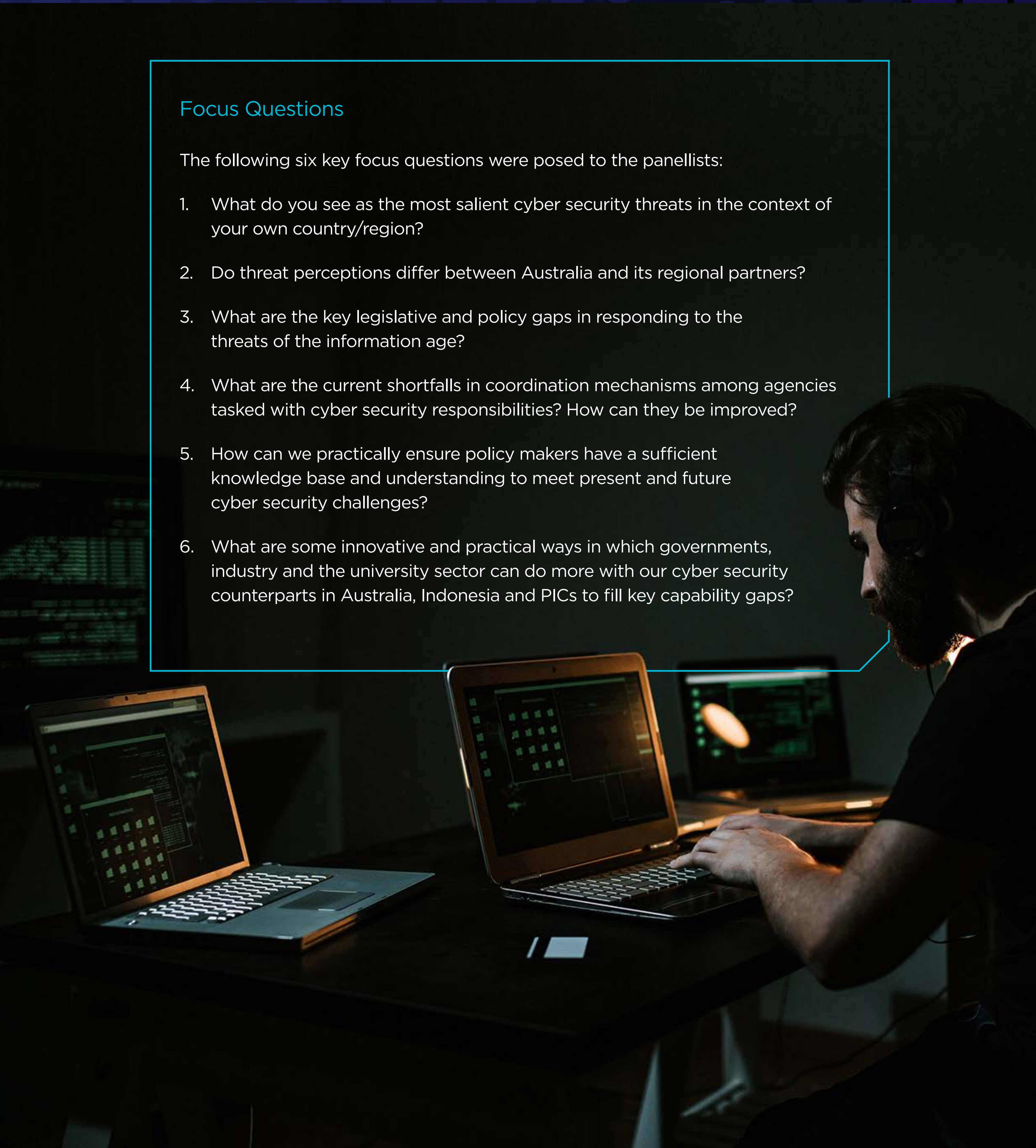
Written Submissions

In addition to the online Roundtable Discussion, this think piece has drawn on the written submission of panellists, Professor Ko, Dr Widodo, and Dr Agus Hasan Sulistiono Reksoprodjo, Lecturer in Asymmetric Strategy at Indonesia’s National Defence University (Unhan).

Focus Questions

The following six key focus questions were posed to the panellists:

1. What do you see as the most salient cyber security threats in the context of your own country/region?
2. Do threat perceptions differ between Australia and its regional partners?
3. What are the key legislative and policy gaps in responding to the threats of the information age?
4. What are the current shortfalls in coordination mechanisms among agencies tasked with cyber security responsibilities? How can they be improved?
5. How can we practically ensure policy makers have a sufficient knowledge base and understanding to meet present and future cyber security challenges?
6. What are some innovative and practical ways in which governments, industry and the university sector can do more with our cyber security counterparts in Australia, Indonesia and PICs to fill key capability gaps?



Introduction

The world is in the midst of a significant transformation. As international power dynamics shift, disruptive challenges in technological transformation, climate change, and socio-political divisions are further compounding the complexity in which policy makers find themselves. The economic, security and socio-political implications of cyber and critical technologies, which cross-cut and transcend traditional sectoral and jurisdictional boundaries, create wicked dilemmas for policy makers. Within the Australian policy-making context, disruptive change requires agility and foresight within public sector institutions, deeper regional engagement with our Southeast Asian and Pacific partners, and closer coordination between government, industry, universities, and communities.

In August 2020, the many security challenges posed by cyberspace were recognised in the Australian Government's release of an updated and fully funded strategy entitled, *Australia's Cyber Security Strategy 2020.* The *Strategy* committed to a A$1.67 billion investment over the next decade to achieve Australia's vision of protecting critical infrastructure, defending against cyber-crime and attacks on government data and networks, and in improving business resilience and community awareness.

The *Strategy* also addressed current deficits in Australia's cyber security governance framework to better respond to an increasingly complex and deteriorating threat environment. It acknowledged the importance that the Australian Government attaches to working with partners in Southeast Asia and the Pacific region to advance their cyber security legal, technical, and policy foundations.[1] Australia has committed A$60 million 'to support cyber capacity building in the Indo-Pacific region to champion an open, free and secure cyberspace'. This includes the A$34 million Cyber Cooperation Program which is 'working with government, industry, civil society and academia to enhance cyber resilience'. Australia has also committed A$14 million for the 'Australia-Papua New Guinea (PNG) Cyber Security Cooperation Initiative to enhance PNG's cyber security frameworks and technical capabilities' and 'A$12.7 million for the Australia-India Cyber and Critical Technology Partnership.'[2]

Indonesia is recognised in Australian foreign policy terms as the linchpin of the Indo-Pacific region and a key diplomatic and security partner for Australia. Yet, as our Indonesian panellists revealed, the absence of an overarching national cyber security legislative framework and attendant cyber security strategy is a key weakness for managing cyber security threats and advancing Indonesia's national interests in cyberspace. In the Pacific islands, Tonga has proved a model for other PICs, having benefitted from targeted capacity building assistance and specialist legal advice under the auspices of the Budapest Convention on Cybercrime.[3] The legal capacity building assistance provided under this treaty-level agreement and other regional initiatives has helped Tonga strengthen its legislative and policy framework to contend with cyber threats. However, greater legislative, policy and technical capacity building assistance is needed in both Indonesia and the PICs to enhance cyber security resilience and awareness.

In this think piece, the UQ Centre for Policy Futures presents a synthesis of discussion points from panellists and contributors who, by virtue of different institutional remits and geographic locations, would not normally engage in an exchange of ideas. Below, our five experts share their perspectives on the regional and global cyber security threat landscape; identify key legislative and policy gaps; and recommend innovative ideas for enhanced cooperation to strengthen Australia, Indonesia and the PICs' collective security in cyberspace.

> **“Across the world, trusting the internet for our healthcare and business... has created new vulnerabilities for us and a greater surface for cyber criminals to exploit.”**
>
> —Tracey Mackay, Director Cyber Security Strategy and Governance
> Department of Home Affairs

The most salient cyber security threats

Australia’s Cyber Security Strategy 2020 is clear in acknowledging that the threat to our critical infrastructure, government networks, universities, health and medical facilities, business and communities is worsening.[4] This is the result of increasing digital connectivity, rapid technological advances, and shifts in the broader threat landscape, which have seen state and state-sponsored actors, in addition to criminals and extremists, increasingly test and exploit Australia’s online vulnerabilities. The COVID-19 pandemic has underscored these effects further, with more people working, studying and accessing services online. As the *Strategy* has recognised, it has imposed an overlay to extant threats represented in state-based and state-sponsored actors, criminals and terrorists, who are variously engaged in online disruption, accessing sensitive information; using the dark web for exploitation; and adopting anonymity and encryption to disguise identities and illegal activity.[5]

COVID-19 has further exposed vulnerabilities in existing cyber defences. As Home Affairs representative Ms Tracey Mackay explained, the pandemic has amplified Australia’s risks and vulnerabilities to cyber crime. It has seen new targeting by malicious cyber actors of critical industries, including food, manufacturing, and health supply chains, as well as Australia’s research community engaged in vaccine development.

Indonesia, which is home to approximately 197 million internet users[6], has also experienced a similar spike in targeted COVID-19 cyber attacks. Director of National Critical Information Infrastructure Protection at BSSN, Mr Nur Achmadi Salmawan, noted similarities to Australia’s experience, with examples of theft of COVID-19 patient records and breaches of Indonesian health and research facility data, including from centres of vaccine research. Indeed, this uptick in COVID-19 related cyber attacks is borne out by official figures. BSSN’s National Security Operations Centre (NSOC) recorded a five-fold increase in cyber-attacks from the first half of 2019 to the first half of 2020 (from around 26 million attacks to 133 million attacks), according to DIP panellist and expert advisor to BSSN, Dr R.M. Wibawanto Nugroho Widodo.

The most common type of attacks were Trojan-related activities, which seek to deceive users into loading legitimate looking malicious code or software onto their computers (accounting for 56%), followed by information gathering activities (43%), and web application-related attacks (1%), according to Dr Widodo.

Dr Agus Hasan Sulistiono Reksoprodjo, Lecturer in Asymmetric Strategy at Indonesia's National Defense University (Unhan), pointed to a 'commonality in threats' across nations based on the same types of tools used by malicious cyber actors. He listed Advanced Persistent Threats (APT), cryptomining, data spill, Distributed Denial of Service (DDOS), hacking, identity theft, malicious insiders, malware, phishing (scam emails), ransomware and web shell malware as key threats faced by Indonesia. Dr Reksoprodjo further pointed to vulnerabilities with open Domain Name System (DNS) Servers and Open Simple Mail Transfer Protocol (SMTP) Servers. The risks associated with the increasing use of Internet of Things (IoT) devices and systems was a concern shared by the Australian Government which, in its *Cyber Security Strategy 2020*, cited NortonLifeLock figures indicating there would be an estimated "21 billion Internet of Things devices connected to the internet globally by 2030, with higher predictions of over 64 billion devices".[7]

Professor Ko explained that many Pacific Island citizens were very active on social media and hence, the most common threat points were linked to their mobile devices and related apps. For Pacific peoples, their access to the internet was usually via their own mobile devices, instead of home-based broadband, which is often very expensive. Although not a threat per se, Mr Salmawan and Professor Ko agreed there were parallels between Indonesia's telecommunication infrastructure challenges and that of the PICs with regard to variability in the quality of internet connectivity between islands within each region.

"What we have in Jakarta or Java is not the same quality of connectivity with the islands of Maluku, Papua or Borneo. This different quality represents specific obstacles for us in disseminating information", explained Salmawan.

Salmawan informed the panel that Indonesia's national telecommunications carrier, Telekomsel, had established Base Transceiver Station (BTS) antennas in every district (*kabupaten*) of Indonesia, but acknowledged that the quality in remote areas was still not the same as on the main island of Java.

Infrastructure was also a point of discussion by Professor Ko. He identified deployed critical infrastructure, otherwise known as 'legacy' critical infrastructure, as one of the most salient cyber security threats to the PICs. The industrial control systems (equipment and software) of utilities and other critical infrastructure are usually implemented by Australian and NZ country consultants and as a result, he explained, these systems tend to be similar and can be used as a testbed by malicious actors for larger scale attacks on Australia, NZ, and other Western countries. These utilities and operational technologies (OT) are usually remotely managed by the consultants in other countries over the internet, and these connections via the internet enable opportunities for attackers to access the same OT environments. Professor Ko cited examples of incidents where utilities in an unidentified Pacific Island country had been compromised via their connections to the internet.

Moreover, because the scale and volume of attacks versus the cyber incident response teams formed to counter them are highly asymmetric, Professor Ko forecast an unsustainable future in terms of eradicating cyber threats,

"On a global scale, there is at least one new and unique malware created every half a second, but generally, all countries, and not just people in the Pacific, are ill-equipped to handle the scale of the problem or train and upskill human resources to match the scale of threats."

Professor Ko further noted that although the lack of capacity to respond is a serious issue, in the PICs it is not unique to the region and, indeed, poses a worldwide challenge,

"We are facing a situation where the threats are coming in so fast that you need to change the game rather than always responding and always fighting fires."

Differences in threat perceptions between Australia and its regional partners

The threat posed by state-based cyber actors is of concern to the Australian Government as acknowledged in the *2020 Strategy*. Home Affairs representative, Ms Mackay, acknowledged there was a mix of actors (cyber criminals, state-sponsored and state-based actors) disrupting and intruding on Australia's critical infrastructure and online systems, and acknowledged the 'sophisticated' nature of attacks on medical research facilities and key supply chains during the COVID-19 pandemic.

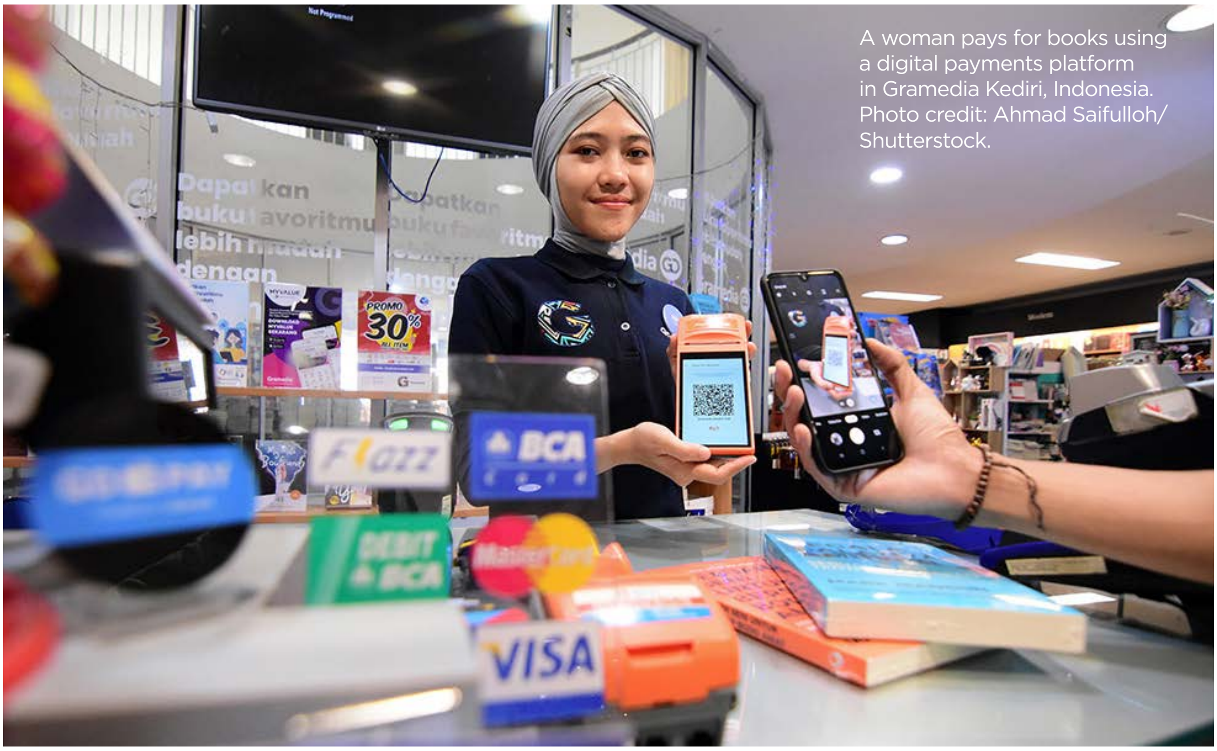
This is partly a reflection of Indonesia's non-aligned foreign policy and historically close ties with Russia as a vital defence partner. Although Indonesia-China relations are more complex, the Indonesian Government maintains a close constructive relationship with Beijing as Indonesia's largest trading partner and second largest source of Foreign Direct Investment (FDI).[8]

Generally, Indonesian panellists and contributors saw Indonesia's threat landscape with respect to cyber criminality in similar terms to Australia's but, in Indonesia's case, there was added emphasis on the ideational and moral threat posed by social media and provocative online content. Cognisant of Indonesia's challenges with violent Islamist extremism, separatism, and ethno-religious conflict, Mr Salmawan cited cyber terrorism, cyber crime, online hoaxes, hate speech, and fake news as a threat to the foundations of Indonesia's democracy and a danger to its citizens. A priority for BSSN, explained Salmawan, was to prevent cyber threats from disrupting national stability and eroding public trust in cyberspace. In a reflection, possibly of Indonesian society's Islamic values, Dr Reksoprodjo revealed that in 2019–2020, pornography was the most reported cyber crime alongside online scams, according to Lokadata figures.[9]

As cyberspace represents a challenge for all democracies, it presents particular dangers for young democracies like Indonesia, which are highly heterogeneous in ethnic and cultural terms. For example, Dr Widodo noted how the cyber domain provided a platform not only for political contest between nation-states, but between internal stakeholders competing for political influence.

In Indonesia, social media and online disinformation has played a critical role in recent elections, as hardline Islamist groups and other opposition forces have mobilised against the Joko Widodo-led government through online campaigns.[10]

> **"Since the type of tools used are mostly the same all over the world, the types of threats are more or less the same for each country. The difference is if the attack is more politically motivated than a criminal act, either from within or outside the country."**
>
> —Dr Yono Reksoprodjo, Lecturer in Asymmetric Strategy, Unhan



A woman pays for books using a digital payments platform in Gramedia Kediri, Indonesia. Photo credit: Ahmad Saifulloh/ Shutterstock.

"We are still in the phase of maturing as a democratic society", stated Dr Widodo. "Many Indonesians are high internet users, but their literacy rate is very low. They are vulnerable to be incited and influenced by anything that goes through cyberspace in political terms."

In this context, Dr Widodo argued that it was incumbent upon Indonesian governments to be less defensive to criticism and see the use of the cyberspace beyond a technical and short-term perspective. A constructive, non-repressive approach through education, political leadership, and cyber literacy was important in building a more civilised cyberspace, Dr Widodo contended. He highlighted the importance of an open, reliable, and interoperable cyberspace as a place to shape a global future, and said it was incumbent upon governments to formulate and execute cyber governance that would enable citizens to engage in cyberspace with more constructive values.

Although nations have particular threat perceptions associated with their individual political, socio-cultural, and economic circumstances, Professor Ko noted that geography was irrelevant for many cyber criminals, as distinct from state and state-sponsored actors, who had political motivations for targeting specific countries,

"Most countries are consistent with respect to threat perceptions as most cyber threats stem from the global connectivity of the internet, and computing services and devices used globally. Ultimately, threat perceptions are strongly linked to, and depend on, the type of threat actors such as so-called script kiddies,[11] criminal gangs, and state-sponsored actors." he stated.

Consistent with criminology research, Professor Ko contended most cyber criminals were opportunistic. Hence, there is a need to increase awareness that most threat actors do not differentiate between countries unless they are state actors.

"They [cyber criminals] do not differentiate whether a computer is in the Pacific Islands, Indonesia or Australia. They are just looking for a point where they can leverage, and maybe, take over some of the computers." [Professor Ko].

> **"The house is built, but it is empty."**
>
> —Dr RM Wibawanto Nugroho Widodo, Director of International Engagement at the Democracy and Integrity for Peace (DIP) Institute and Expert Advisor to the Head of the National Cyber and Crypto Agency, Republic of Indonesia (BSSN).

Key legislative and policy gaps in responding to the threats of the information age

Indonesian regulatory context

In Indonesia, the absence of a coherent legislative, regulatory, and policy framework remains a key weakness, constraining effective governance of Indonesia's cyberspace and its national capacity to leverage opportunities and effectively deal with threats. Dr Widodo drew upon the empty house metaphor to convey the fact that despite Indonesia having established a number of government cyber security entities, including BSSN, the Ministry of Defense's Information and Data Centre (*Pusdatin*), the Indonesian Armed Forces (TNI) Cyber Unit (*Satsiber Tugas TNI*), and the TNI-Army (AD) Cyber and Crypto Unit (*Pusansiad*), they were, in his opinion, established without first having:

"A set of strategic policies at the national level, a cyber law or comprehensive set of cyber strategies."[12] **[Dr Widodo].**

A comprehensive draft cyber security bill—the Cyber Security and Resilience Bill (*Rancangan Undang-Undang Keamanan Siber dan Ketahanan*), which includes provisions for cyber diplomacy, national critical information infrastructure, codification of BSSN powers, cyber governance, and cyber intelligence provisions, was originally included in the Indonesian parliament's (DPR) priority legislative agenda (*Prolegnas*) for 2020, but was delayed due to COVID-19 priorities.[13]

Mr Salmawan highlighted the complexity of the regulatory process in Indonesia which is influenced by many factors, including vested political interests,

"There are 16 main political parties in Indonesia who need to work together to formulate and pass legislative bills and regulations," Mr Salmawan explained.

Without a national cyber security law the authority of BSSN, relative to other national security agencies vested with cyber security responsibilities, remains somewhat ambiguous. In a country sensitive to its authoritarian political past and prone to intra-bureaucratic and inter-elite contest over national security powers, the Bill remains somewhat contentious.

"The absence of a top to bottom approach causes everyone to feel that they can go their own way without dependence on a single agency or [coordination] with other organisations," asserted Dr Reksoprodjo.

In April 2021, the President, faced by delays in legislative consideration of the cyber security bill, moved to cement the authority of BSSN as the principal agency invested with authority over cyber security policy matters, through presidential decree.[14] The decree formalises BSSN's authority as an agency reporting directly to the President.

At present, Indonesia has an Electronic Information and Transactions (ITE) Law and various ministerial regulations, but 'privacy, personal data protection, and cyber security are embodied in an array of general and sector-specific laws,' rather than overarching cyber security legislation.[15] According to Dr Widodo, the President plans to issue three more Presidential Decrees (*Perpres*)[16] in addition to the April 2021 BSSN decree. These pertain to: 1) the formulation of a national cyber security strategy (in draft form); 2) enhancement of national cyber incident management provisions; and 3) recognition of eleven types of critical infrastructure.[17]

Dr Widodo explained that the release of a national cyber security strategy in combination with the BSSN presidential decree would boost Indonesia's ability to develop a coherent national strategy to better protect the national interests of Indonesia's homeland and population through securing data, networks, information, and national information systems, and by realising Indonesia's digital economic power through innovation. He contended that the presidential decrees would also enhance Indonesia's cyber defence capabilities, with a significant level of deterrent effects, and advance Indonesia's wider interests at the global level. BSSN will be transformed into an agency more like Britain's Government Communications Headquarters (GCHQ) or the Australian Signals Directorate (ASD), explained Dr Widodo. BSSN would become the highest coordinating agency for Indonesia's cyber security governance.

Australian regulatory context

Although Australia is more advanced in cyber specific legislative and policy terms, *Australia's Cyber Security Strategy 2020* has also identified the need for further amendments to legislative and regulatory frameworks. The *Strategy* has committed to the *Telecommunications Sector Security Reforms* and *Security of Critical Infrastructure Act 2018,* the terms of the latter of which will be expanded to include other critical sectors and cyber specific obligations for owners to protect critical systems.[18] In an assertion of Commonwealth national interest provisions, the *Strategy* also stipulates that,

"The Australian Government has an obligation to act in the national interest when the threats of consequences are too high for individual entities to manage without its unique capabilities."[19]

Through the *The Telecommunications and Other Legislation Amendment (Assistance and Access) Act*, the *Strategy* states that the:

"Australian Government will ensure law enforcement agencies have appropriate legislative powers and technical capabilities to deter, disrupt, and defeat the criminal exploitation of anonymising technology and the dark web."[20]

Still in the Australian context, Professor Ko flagged further regulatory reform measures to enhance compliance. In reference to the Australian Government's Notifiable Data Breaches (NDB) scheme,[21] which mandates that organisations which experience data breaches notify authorities about the breach, the legal penalties focus only on penalising organisations for not informing about the breach, but not for the breach itself, explained Professor Ko.

"Organisations hosting critical infrastructure and systems should be liable for a high level of information assurance and should be held accountable in a legal way. This will encourage boards and senior executives to put cyber security on the agenda and recognise cyber risks as business risks," Professor Ko contended.

With respect to the Cloud and data, Professor Ko stated that Cloud service providers which store or process the sensitive data of Australian citizens and residents or hosting services should be able to provide the Australian Government and people with full transparency about the provenance of data, the location where the data will be stored and accessed from, and should have high accountability and auditability.

Current shortfalls in coordination mechanisms among agencies tasked with cyber security responsibilities and how they can be improved

Indonesian interagency coordination

Dr Reksoprodjo suggested there was a critical need to engender a common purpose among Indonesian agencies. He attributed current shortfalls in coordination mechanisms to knowledge gaps, regulatory overlap, intra-bureaucratic rivalries (sectoral egos),[22] and a lack of leadership. For example, Reksoprodjo explained that those who determined cyber security legislative and policy frameworks lacked sufficient area knowledge. This, when combined with laws and state regulations that were formulated long before the cyber era, mean that:

"[Indonesia's regulatory framework is] not fit for purpose for the needs of the information age," Dr Reksoprodjo said.

Moreover, as BSSN seeks to grow its nascent influence and authority as Indonesia's principal cyber security agency, challenges will remain in other agencies' willingness to share respective roles and responsibilities, explained Dr Reksoprodjo. Improved communication and common understanding of cyber security roles and responsibilities of each agencies is required.

"Indonesian agencies need to come together and establish a common understanding of vulnerabilities," explained Reksoprodjo. "They need to be open to opportunities to ask other agencies what help can be proffered."

Dr Widodo called for a more strategic approach to cyberspace, anchored in Indonesia's total defence doctrine (*pertahanan semesta*),[23] that would enable Indonesia to fulfil its security needs and national potential. He argued there was incoherent interaction between three strategic means at the national level. These were: 1) the lack of an adaptive legal system to respond to the dynamics of the cyber world; 2) the failure to mobilise all national resources (both effective bottom-up and top-down efforts) to build Indonesian cyber power based on the principle of total defence; and 3) the lack of public private partnerships and a whole-of-government approach.

"Securing the cyberspace of a nation is a shared responsibility that requires a greater internal collaboration among government agencies, and between government and non-governmental sectors," stated Dr Widodo.

The lack of capacity and capability of Cyber Emergency Response Teams (CERTs) and CSIRTs of government agencies, other than BSSN, makes them very vulnerable to cyber-attack, noted Dr Widodo. He suggested Indonesia needed to develop a hierarchical structure of cyber security mechanisms, which link the BSSN, NSOC, and NCISRT to Security Operations Centres (SOCs) with their own CISRTs at the level of central and local government, to critical infrastructure owners and private sector entities.

> **"The absence of a top to bottom approach causes everyone to feel that they can go their own way without dependence on a single agency or … [coordination] … with other organisations."**
>
> —Dr Yono Reksoprodjo, Lecturer in Asymmetric Strategy, Unhan

Dr Widodo also recommended greater access for Indonesian agencies to international cooperation and training through scholarships and exchange,

"BSSN needs to be given more room for constructing engagement and cooperation with global counterparts. Not only in real technical capacity, but also in the non-technical aspects of cyberspace," Dr Widodo explained.

Pacific Interagency Coordination

Professor Ko drew on Tonga as an exemplar in legislative coherence and whole-of-government cyber security coordination among the PICs. As a small country, Professor Ko noted, Tonga has been able amend laws to enhance its cyber security relatively easily. Led by the then Deputy Prime Minister, The Honourable Siaosi Sovaleni, ratification of Tonga's Computer Crimes Bill in 2017 set a gold standard in the country's intent to increase the efficiency of whole-of-government coordination of cyber and cyber-enabled criminal investigations, explained Professor Ko.[24] At the same time, the NZ process represents another positive example, given its leadership in Indigenous data sovereignty and recognition that "one size does not fit all". NZ's approach to cyber security legislative and policy formulation has been a consultative and consensus-building one, according to Professor Ko. The government has carefully considered what laws mean for different community sectors and listened to stakeholder aspirations via workshops and focus groups.

Drawing on Tonga's experience, Professor Ko called for a current gap in cyber security research to be addressed. He called for additional research into countries that have acceded to the Budapest Convention (presently Tonga and NZ are the only Pacific countries to have acceded), to determine the Treaty's efficacy for cyber security legislation and policy formulation.

"No one has empirically analysed or measured whether countries in the Budapest Convention are, in fact, more cyber resilient and whether there is a substantive difference or just additional paperwork." [Professor Ko]

This is an area that should be explored further, stated Professor Ko, given there are 78 signatories to the Convention representing less than half of all countries.[25]

Australian Interagency Coordination

Ms Mackay explained that Home Affairs, which leads cyber security policy development for the Australian Government, is very focussed on enhancing whole-of-government coordination. According to Ms Mackay, there is now improved coordination across government on different cyber and digital work, and this had been a priority for the government for some time. Ms Mackay listed a number of examples, including substantive collaboration between Home Affairs and the eSafety commissioner to develop an online safety campaign which includes cyber security, but covers the whole spectrum of online safety issues, particularly for more vulnerable Australians such as children and teenagers. Home Affairs is also looking at digital economy packages and how Australians use the IoT, internet and digital platforms. In addition, she noted that there are a lot of whole-of-community efforts.

Although government plays an enabling role, business and community play the key role, explained Ms Mackay. The formulation of the *Strategy,* for example, involved extensive public and industry consultation with over 1,400 individuals and over 200 submissions.[26] The Minister for Home Affairs has subsequently announced a new Industry Advisory Committee which will shape delivery of actions set out in the *Strategy* and provide advice on updates to the *Strategy's* Action Plan. Through the Committee mechanism, Home Affairs aims to ensure that legislation and policies will not be over-burdensome, costly or detrimental to business, stated Ms Mackay.

Practical ways to ensure policy makers have a sufficient knowledge base and understanding to meet present and future cyber security challenges

Indonesian policy makers

According to Dr Widodo, Indonesian policy makers needed to be more critical, historically minded, responsive, systematic, creative, and futuristic in foreseeing the cyber attacks of the future. Since cyberspace is a global domain formed by the interaction of IT infrastructure, internet and computer systems, the cyber challenges faced by other nation-states are relatively identical to one another. The global community needs to help educate political elites and policy makers in Indonesia about the strategic importance of the cyber domain through various formal and informal engagements.

"A nation perceives threats based on the level of understanding of its policy makers to perceive certain phenomena," postulated Dr Widodo, and "most Indonesian elites do not see the cyberspace as a potential warfare domain."[27]

Based on his interactions with a range of legislators, policy makers and security professionals, Dr Widodo contended that elites are not yet at a level of understanding where they appreciate how Indonesia can shape the global cyberspace. Dr Widodo identified awareness raising as a key mandate for BSSN in educating and explaining the strategic importance of cyberspace for the advancement of Indonesia's national interests. Similarly, Mr Salmawan acknowledged that educating Indonesian policy makers was a significant challenge for BSSN, and called for more seminars on cyber security awareness that could educate policy makers and the public, not only in Jakarta, but at the regional and local government level. Salmawan underscored the importance for BSSN officials to travel outside Indonesia's capital, Jakarta, so that they can share their cyber security knowledge with local government officials to build trust in regulatory frameworks.

"BSSN must work on disseminating information to both policy makers and parliamentarians," Mr Salmawan asserted.

> **"It is a big challenge to educate policy makers. We actively hope for cyber security seminars on cyber security awareness to provide education to policy makers and the public, not only in Jakarta, but local government, small cities, and regencies outside Java."**
>
> —Nur Achamdi Salmawan, Director Critical Information Infrastructure BSSN

> **“If cyber security was just a technical problem we would have solved it about two or three decades ago.”**
>
> —Professor Ryan Ko, Chair and Director of UQ Cyber Security

Pacific policy makers

Based on his Pacific capacity building experience, Professor Ko is a strong advocate of bringing a more interdisciplinary approach to courses and training programs. He was involved in the drafting of the New Zealand Qualifications Authority (NZQA) Level 6 qualification in Cyber Security (equivalent to a CERT IV qualification in Australia) and recognised the need to focus on communication and client-facing skills, in addition to technical course content. There is significant potential to upscale existing training of Pacific public servants through train-the-trainer type courses, contended Professor Ko. Building the knowledge of public servants, who can then implement policies to increase awareness, not just of regional governments, but also that of citizens and industry, is the inherent value of such programs. Professor Ko acknowledged the cyber security capacity building activities of the Asia Pacific Network Information Centre (APNIC) in the Pacific region and its work alongside partners such as the Asian Development Bank and the Pacific Cyber Security Operational Network (PACSON) commissioned by DFAT. For Professor Ko, the main challenge was ensuring training was translated into implementation and impact.

“Some of the key players are currently not as deeply engaged as they should be,” stated Professor Ko.

He cited the example of the Telco networks in the Pacific which are run by a handful of providers and have an almost-monopolistic share.

“Governments have to find creative ways to engage them to be part of this movement and to help increase regional cyber security awareness,” Professor Ko said.

Building an Australian knowledge base

The importance of government, industry and universities working together was something Ms Mackay acknowledged as very important to the Australian Government. She cited several initiatives under the *Strategy* which aimed to build a skilled workforce and encourage academia and industry to work more closely together. These included the A$50 million Cyber Security National Workforce Growth Program and the A$26.5 million Cyber Skills Partnerships Innovation Fund, which will ‘encourage businesses and academia to partner together to find innovative new ways to improve cyber security skills.’ The Workforce Growth Program complements work being conducted by the Department of Defence in upskilling Australian Defence Force recruits as part of the government’s commitment to build the defence cyber workforce, explained Mackay. In terms of policy makers having a sufficient knowledge base, she said that a broad and extensive effort was required,

“It’s really important and necessary effort if we are going to be able make good decisions,” Ms Mackay explained.

The *Strategy* also includes a Cyber Security Best Practice Regulation Taskforce to examine the issues facing industry in cyber security and how best to implement them. The *Strategy* contains recommendations on critical infrastructure and systems of national significance in Australia,

“But for those businesses outside critical infrastructure and national significance categories, the Taskforce will also develop ideas to ensure that other businesses are cyber secure,” said Ms Mackay.

Educating users across the Indo-Pacific region

Professor Ko noted that education imperatives extended far beyond policy makers. He said that currently there is a large responsibility placed on the end-users, but cyber security awareness was a responsibility for all. Fundamentally, Professor Ko says, there are three key actors:

1. Technology providers are also responsible for increasing awareness.

"We see them becoming more influential than governments, since their devices and websites are influencing the daily lives of citizens. The technology providers need to be able to provide data control to users, governments and law enforcement agencies monitoring more extreme behaviour—they need to be able to take that down." Professor Ko explained.

2. Governments. Governments can increase awareness by creating policy, norms and legal frameworks to increase accountability and also enable the right to take down some of the more objectionable content in a balanced and timely manner.

"That cannot be achieved by just one country; it is a regional effort and international effort. Tech companies are quite clever with regard to this. For example, when you upload a file online, particularly in the Cloud, you have four or five copies of the same content in different servers, hosted across different countries and continents. If a government in one continent objects to the way the tech companies operate, then they can simply stop hosting in that continent to evade penalties or repercussions," Professor Ko noted.

3. Individuals. An end-user has to be aware of all risks, and must always be sceptical, seeking verification and asking questions such as: "why has this file been sent to me at this time?"

All three actors need to be aware of their roles and responsibilities, explained Professor Ko.

Students from Tonga's Tailulu College making the most of new high-speed broadband services at 2013 World Telecommunication and Information Society Day celebrations in the Tongan capital, Nuku'alofa. Photo: Tom Perry / World Bank.

Innovative and practical ways in which governments, industry and the university sector can do more with our cyber security counterparts in Australia, Indonesia and the PICs to fill key capability gaps

> **“Community and industry consultation and outreach will continue to be a cornerstone of what we do in Australia and something that is critical. A lot of the new policies developed by government are tailored to support particular segments of the Australian community — for instance, big industry, SMEs or households. But, together, this cyber security agenda literally touches everyone who connects online to the internet.”**
>
> —Tracey Mackay, Director Cyber Security Strategy and Governance, Department of Home Affairs

Online courses

In the Pacific, there is much potential to upscale online short courses, explained Professor Ko. With COVID-19, universities have had to adjust quickly to offering courses online. The greater agility in course provision means education providers can scale more and overcome the tyranny of distance. Governments across the region can explore programs which provide bursaries for certain courses and then over time allow their staff to gain a degree through micro credentialling arrangements, explained Professor Ko. The people who are training for cyber security short courses are usually all busy individuals, so taking one course per year online is manageable. As they progress over time, they can gain a degree or some other kind of accreditation, he said.

University sector

Universities and tertiary institutions in general should start looking at addressing cyber security as a truly interdisciplinary problem, argued Professor Ko.

“The way to approach this is to approach the problem similar to how the medical and health sciences train clinicians and non-clinicians to address health research challenges, or how engineering schools start with common engineering training before specialising into specific engineering majors (e.g. software engineering, civil engineering, etc.),” Professor Ko said.

Since 2019, UQ has offered a truly interdisciplinary cyber security education program, which fits into the postgraduate and the higher-level undergraduate (e.g. honours) programs. While this is facilitated by the School of Information Technology and Electrical Engineering, there are several schools across UQ which are involved in this interdisciplinary degree aligned with US Department of Commerce's National Institute of Standards and Technology (NIST) and National Initiative for Cybersecurity Education (NICE) frameworks, according to Professor Ko.[28]

He explained that students commenced with an interdisciplinary core of four courses in the UQ Postgraduate Cyber Security Program, covering the geopolitical, legal, technical, business and ethical aspects of cyber security, before branching into their specialisations in Cyber Defence, Cyber Criminology, Leadership and Cryptography. The program is taught by experts from UQ Business School, UQ Law School, the Criminology Department in the School of Social Sciences, UQ Centre for Policy Futures, and the School of Mathematics and Physics; the latter of which teaches into the cryptography aspects of the program. The program ends with a capstone (internship) program which addresses the experience requirement of almost all cyber security jobs, including that required by employers looking for new graduates, explained Professor Ko. While UQ is leading this approach, this model could be replicated across other universities in Australia and the region.

"Our Master's program has been taking in students from non-technical backgrounds looking to branch into technical specialisations and vice versa. When we proposed it, it was somewhat 'heretical', since we proposed that people from all different backgrounds can participate in our Master's degree," Professor Ko explained.

"Unknown to many", noted Professor Ko, this was actually reflective of the realities of the industry, where many cyber professionals come from non-computer science-related degrees.

"The focus is on developing leaders who will, in turn, train the people they lead in the future," Professor Ko stated.

Professor Ko also identified cyber security skills development through the conduct of cyber competitions such as the Capture the Flag (CTF) competition or Cyber 9/12, as a further key area for universities to contribute to. He explained that, in Australia, students had recently come together from 13 different universities to run the Down Under CTF (DUCTF), which has replaced the now-inactive Cyber Security Challenge Australia (CySCA).[29] The UQ Cyber Squad, a student society, has continued to build traction and attract teams of interdisciplinary students from across UQ. Professor Ko recounted the Squad's success in the Cyber 9/12 challenge held by the Atlantic Council.[30]

The UQ Cyber Squad participates in national and regional CTF competitions where they solve hacking challenges, discover vulnerabilities and defend 'sand box' servers.[31] Through these activities, they understand how to work together as a team with different areas of expertise. According to Professor Ko, universities are ideal places to hold such exercises and competitions, since they can raise awareness and conduct realistic exercises in unclassified and non-sensitive environments.

> **"We are facing a situation where the threats are coming in so fast that you need to change the game rather than always responding and always fighting fires."**
>
> —Professor Ryan Ko, Chair and Director of UQ Cyber Security

"There is definitely much scope for more defence or government-led exercises," Professor Ko noted.

After listening to Professor Ko, Dr Widodo characterised his ideas as a strategic opportunity for Indonesia,

"We need to be proactive in absorbing all these opportunities. It is not just about formal or certificate courses, but instilling a culture of innovation and excellence within universities. Indonesian universities need to be more open to academics from overseas," Dr Widodo stated.

In a written submission, Dr Reksoprodjo suggested active capacity-building training between regional nations through simulated cyber attacks to create an atmosphere that encouraged and enhanced mutual understanding and a spirit of cooperation. Such training exercises can be conducted online with desktop exercises and field simulations, he wrote. Reksoprodjo considered that the application of disaster management Standard Operating Procedures (SOPs) to cyber security contingency planning, including training in individual and team preparation to understand a contingency from the beginning, preparing mitigation, emergency response, rehabilitation and reconstruction, was needed in the Indonesian context. An "observe, orient, decide and act model" was required for continuous improvement in cyber incident response procedures, he argued.

Game-Changing Research

Professor Ko recommended greater investment into game-changing interdisciplinary research that could,

"**Create a new chessboard so that the attackers have to play cat and mouse with us rather than the other way around."**

By example, he described the problem of web spam in the early days of the internet when a lot of people used machines to automatically fill in online forms. This spam became a significant problem for the feasibility of online forms. The innovation that overcame this was the 'Completely Automated Public Turing Test To Tell Computers and Humans Apart' (CAPTCHA), which allowed websites to authenticate the user as human.

"It [CAPTCHA] was a simple innovation," explained Professor Ko, "but totally wiped out web spam."

Professor Ko added that the lack of funding for fundamental and applied research, as well as resources dedicated to inspire game-changing interdisciplinary research, such as policing of the dark web, which required collaborative research by criminologists, computer scientists and legal experts, remained a significant impediment to cyber security resilience.

Media

Professor Ko also saw a key role for the mainstream media in improving cyber awareness and e-safety.

"Australia and NZ have popular television programs focussed on biosecurity, border patrol and border security" [such as the Australian Seven Network's highly popular *Border Security: Australia's Front Line*], Professor Ko said.[32] "These kind of TV programs shown on prime time television, usually after dinner time, mean that people stay on, watch and understand more about border policing."

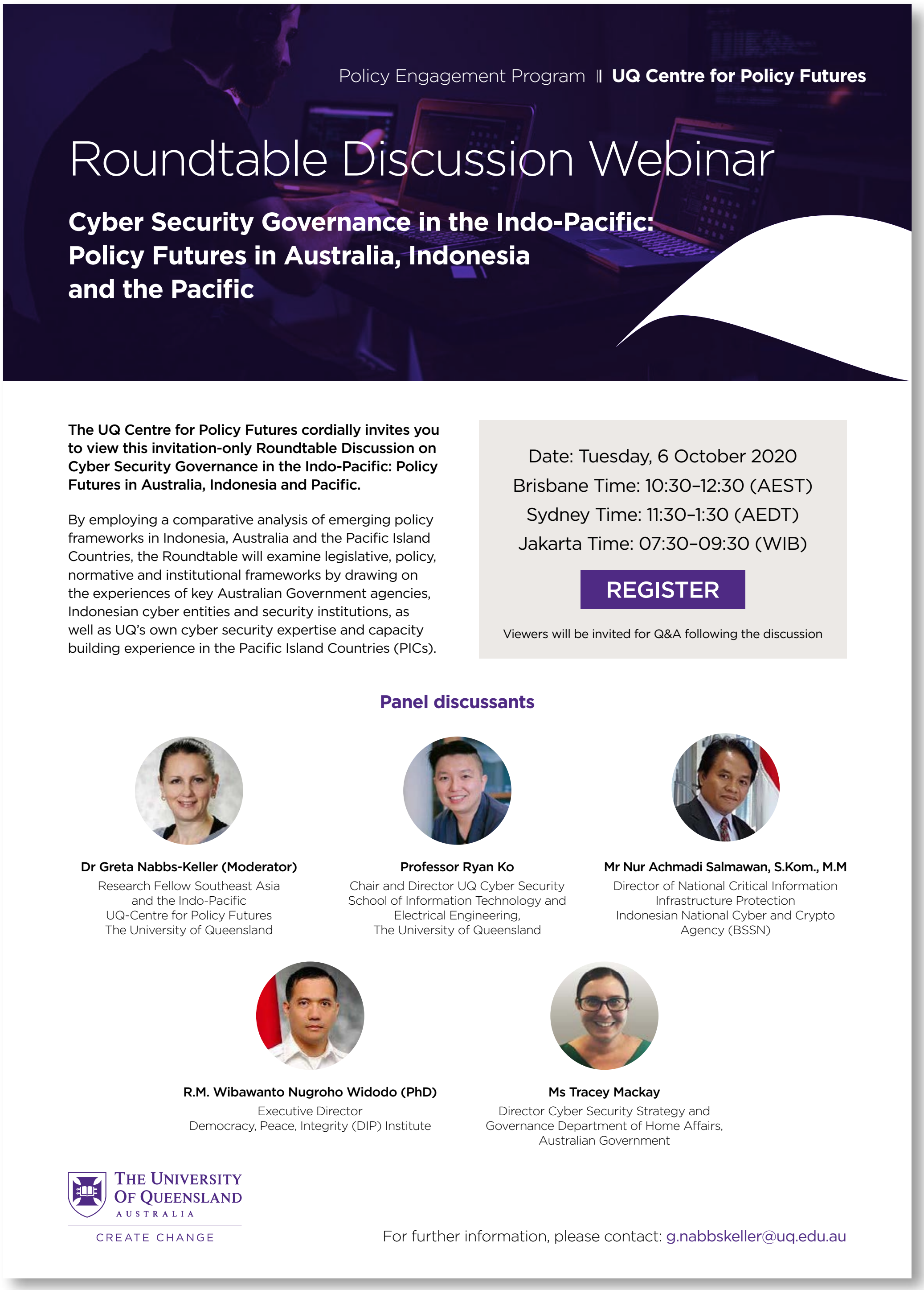
He recommended governments consider developing a television series similar to *Border Security* focussed on increasing awareness of e-safety and cyber security. This program could be readily streamed into the region and subtitled in Southeast Asian and Pacific languages.

Political leaders also have an important role to play on cyber security awareness in concert with the media. Professor Ko recounted how, on the 19th of June 2020, the Australian Prime Minister made a public announcement about a major cyber attack on Australian government and industry that could only be conducted by a state actor. Branded the 'copy-paste compromises',[33] Professor Ko recounted how, overnight, Australia witnessed a heightened awareness, with lots of providers and end-users patching their servers.

"Sometimes, the top down approach works well," Professor Ko reflected.

Annex A

Promotional Flyer



Policy Engagement Program ‖ **UQ Centre for Policy Futures**

Roundtable Discussion Webinar

Cyber Security Governance in the Indo-Pacific: Policy Futures in Australia, Indonesia and the Pacific

The UQ Centre for Policy Futures cordially invites you to view this invitation-only Roundtable Discussion on Cyber Security Governance in the Indo-Pacific: Policy Futures in Australia, Indonesia and Pacific.

By employing a comparative analysis of emerging policy frameworks in Indonesia, Australia and the Pacific Island Countries, the Roundtable will examine legislative, policy, normative and institutional frameworks by drawing on the experiences of key Australian Government agencies, Indonesian cyber entities and security institutions, as well as UQ's own cyber security expertise and capacity building experience in the Pacific Island Countries (PICs).

Date: Tuesday, 6 October 2020
Brisbane Time: 10:30–12:30 (AEST)
Sydney Time: 11:30–1:30 (AEDT)
Jakarta Time: 07:30–09:30 (WIB)

REGISTER

Viewers will be invited for Q&A following the discussion

Panel discussants

Dr Greta Nabbs-Keller (Moderator)
Research Fellow Southeast Asia
and the Indo-Pacific
UQ-Centre for Policy Futures
The University of Queensland

Professor Ryan Ko
Chair and Director UQ Cyber Security
School of Information Technology and
Electrical Engineering,
The University of Queensland

Mr Nur Achmadi Salmawan, S.Kom., M.M
Director of National Critical Information
Infrastructure Protection
Indonesian National Cyber and Crypto
Agency (BSSN)

R.M. Wibawanto Nugroho Widodo (PhD)
Executive Director
Democracy, Peace, Integrity (DIP) Institute

Ms Tracey Mackay
Director Cyber Security Strategy and
Governance Department of Home Affairs,
Australian Government

The University of Queensland
AUSTRALIA
CREATE CHANGE

For further information, please contact: g.nabbskeller@uq.edu.au

Annex B

Bios of Chair and Expert Panel

Dr Greta Nabbs-Keller is Research Fellow Southeast Asia and the Indo-Pacific at The University of Queensland's (UQ) Centre for Policy Futures. Her research agenda focusses on how Southeast Asian states are managing major power contests in the Indo-Pacific and what this means for Australia's policy choices. The nexus between domestic political imperatives and foreign policy decision-making in Indonesia's relations with major powers China, India, Japan and the US is a focal point of her research. Greta contributes regularly to media and think-tank analysis on regional strategic, political and foreign policy issues, and engages with policy communities through submissions, dialogues, conferences and executive educations programs. Her recent publications include: "ASEAN Centrality and Indonesian Leadership in the Indo-Pacific", published in the August edition of *Security Challenges* and "Understanding Australia-Indonesia relations in the post-authoritarian era: resilience and respect", published by the *Australian Journal of International Affairs.*

Ms Tracey Mackay is the Director of Cyber Security Strategy and Governance at the Australian Department of Home Affairs. She has diverse public sector experience in national security and foreign policy across a range of Australian Government agencies, including the Department of Foreign Affairs and Trade, Department of Defence, the former AusAID and the former Department of Climate Change. Ms Mackay has represented Australia in a range of United Nations fora and for two years coordinated the Foreign Affairs and Trade portfolio for the Federal Budget. Previously, Ms Mackay worked with UNESCO's Asia Pacific Regional Office for Education in Bangkok, Thailand. She holds a Master of Public Policy, a Bachelor of Social Science Honours (first class) in international relations, and a Bachelor of Arts.

Mr Nur Achmadi Salmawan is the Director of National Critical Information Infrastructure Protection at Indonesia's National Cyber and Crypto Agency (BSSN). He has been serving in his current position since January 2020. He has held several other positions at BSSN and started his career as an Indonesian Civil Servant in 1992. Mr Salmawan also worked for the Indonesian Ministry of Foreign Affairs from 1996 to 2003 in the Information Security field. He strengthened information security at the Indonesian Mission to the United Nations in New York for several years. During his career from 2004 to 2019, Mr Salmawan has held various positions mostly in the government sector. He provides services in the field of information security not only for government offices in the capital city, but also in various local government agencies across Indonesia. Mr Salmawan was involved in the President's information security for several years during the Yudhoyono administration and led an agency team to strengthen Indonesia's maritime security operations. In 2018, he led the Indonesian delegation to initiate talks on Cyber Security between BSSN and the Australian Cyber Security Centre (ACSC) in Canberra. And in 2019 he also led the Indonesian delegation on a discussion on cybersecurity between BSSN and the British Government's National Cyber Security Centre (NCSC) in London.

Dr R.M. Wibawanto Nugroho Widodo is Director of International Engagement at the Democracy and Integrity for Peace (DIP) Institute and Expert Advisor (Staf Ahli) on national ideology to the Head of the State Cyber and Crypto Agency, Republic of Indonesia (BSSN), Lieutenant General (ret) Hinsa Siburian. Dr Widodo is an expert in politics, national security, defence, strategy, and leadership. He has represented the Republic of Indonesia at the "US Army Global Symposium on the Challenge of the Future Joint Operational Environment (JOE): 2009–2024" in 2008, and at the "US National Defense University Global Alumni Quadrennial Reunion and International Security Symposium" hosed in 2017 by the US Department of Defense. Dr Widodo has also been a consultant for the World Bank Group, the lecturer at the Indonesian National Defence University (Unhan) in the field of cyber and asymmetric warfare, has appeared as a speaker for the Indonesian National Resilience Institute (Lemhannas), the Vice Chairman of National Defense and Security at Indonesian National Resilience Institute Alumni Association Strategic Center (IKAL SC), and is a non-resident senior fellow at the Westminster Institute, Washington. Dr Widodo also lectures at Pelita Harapan University in the field of global political leadership, strategy, diplomacy, and political economy in international politics. He earned his PhD from the University of Exeter, UK with the dissertation of "Understanding the Existence and Latent Threat of Islamist Terrorism through a Multidimensional Analysis: The Case of Republic of Indonesia," an MPP from Schar School of Policy and Government at George Mason University, an MA and War College Diploma from U.S. National Defense University with the dissertation of Indonesian Armed Forces' Roles, Strategies, and Capabilities in Counter Terrorism within a Changing National Security: Looking Forward 2007–2017," and an MA in International Business & Management from University of Bradford, UK.

Professor Ryan Ko Chair and Director UQ Cyber Security, School of Information Technology and Electrical Engineering. Professor Ko is a computer scientist who has rich technology commercialisation and leadership experience across academia, industry, and entrepreneurship. He brings direct experience in delivering capacity development activities in the Pacific having contributed to the establishment of CERT Tonga, the first national CERT in the Pacific Islands, and CERT New Zealand (NZ). Currently Professor, Chair and Director of UQ Cyber Security at The University of Queensland, Australia, he continues to serve as an expert advisor to INTERPOL, the NZ Defence Force, the NZ Minister for Communications' Cyber Security Skills Taskforce, and he is one of four nationally-appointed Technical Advisers for the *Harmful Digital Communications Act 2015*, Ministry of Justice. Prof Ko has a strong record in establishing university-wide, multi-disciplinary academic research and education programs, including, but not limited to, NZ's first cyber security graduate research program and lab, Cybersecurity Researchers of Waikato (CROW); and NZ's first Master of Cyber Security (encompassing technical and law courses). He also has a strong track record developing international and national cyber security curricula, including the cocreation of the gold-standard International Information System Security Certification Consortium (ISC)2 Certified Cloud Security Professional (CCSP) curriculum, and authoring the initial NZ Qualifications Authority's Level 6 Cybersecurity Diploma qualification.

Dr Agus Hasan Sulistiono Reksoprodjo, **Lecturer in Asymmetric Warfare at the Indonesian National Defense University (Unhan).** Dr Reksoprodjo graduated as a Naval Architect from the University of Indonesia and continued his degree as Doctor of Philosophy in Computer Aided Engineering Systems with emphasis on reverse engineering technology from Imperial College, University of London. He has extensive experience ranging from engineering design works to general management in many world class industries such as the Indonesian Aerospace (PTDI), Rolls Royce Aero Engine UK, Rover UK, Milliard Design Australia, Shinwa Engineering (SEI) and ARACO Japan. Dr Reksoprodjo has served previously in a number of key advisory roles, including as advisor on C4ISRNET to the TNI Commander, Indonesian Disaster Management Agency (BNPB), and State Intelligence Agency (BIN). In 2011, He was a Visiting Fellow to the Department of Defence where he engaged with key stakeholders from the Department of Prime Minister & Cabinet; the Secretariats of the Parliamentary Joint Committee on Intelligence and Security, and the Standing Committee on Foreign Affairs, Defence and Trade; the Office of National Assessments; and the Ambassador for Counter-Terrorism, DFAT. Dr Reksoprodjo is also a current member of Ikahan, the Indonesia-Australia Defence Alumni Association.

Notes and References

1 For extant regional engagement programs and commitments see page 27-28 of Commonwealth of Australia, *Australia's Cyber Security Strategy 2020*, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

2 *Australia's Cyber Security Strategy*, page 28.

3 The Convention is the first international treaty on crimes committed via the Internet and other computer networks. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. Council of Europe, Treaty Office, 'Details of Treaty No.185, Convention on Cybercrime', https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

4 *Australia's Cyber Security Strategy*, pages 15, 28.

5 Facebook and Google's adoption of end-to-end encryption has become a source of friction between the Australian Government and major tech companies. Paul Smith, 'Facebook and encryption experts unite against 'Sith Lord' Dutton', *Australian Financial Review*, 23 October 2020, https://www.afr.com/technology/facebook-and-encryption-experts-unite-against-sith-lord-dutton-20201023-p56814

6 Figure based on 2020 Indonesian Internet Service Providers Association (APJII) data, Herman, 'Indonesia Has 197 Million Internet Users in 2020, APJII Survey Shows', 9 November 2020, *The Jakarta Globe*, https://jakartaglobe.id/tech/indonesia-has-197-million-internet-users-in-2020-apjii-survey-shows

7 *Australia's Cyber Security Strategy*, page 31.

8 China is Indonesia's largest training partner and second largest source of Foreign Direct Investment. '*Kepala BKPM Sebut Virus Korona Bisa Turunkan Investasi China ke Indonesia*' [BKPM Head Says Coronavirus Could Reduce Chinese Investment in Indonesia], *Okezone*, 29 January 2020. https://economy.okezone.com/read/2020/01/29/20/2160140/kepala-bkpm-sebut-virus-korona-bisa-turunkan-investasi-china-ke-indonesia

9 Lokadata is an Indonesian data analytic and research company. *Jenis kejahatan siber di Indonesia*, 2019–2020', [Types of cyber crime in Indonesia 2019-2020'], May 2020 data, *Patroli Siber* [Cyber Patrol], Lokadata, https://lokadata.id/artikel/indonesia-jadi-negara-dengan-serangan-siber-tertinggi

10 See for example, Sheany, 'Muslim Cyber Army More Harmful than Saracen Says Human Rights Group', *The Jakarta Globe*, 2 March 2018, https://jakartaglobe.id/news/muslim-cyber-army-more-harmful-than-saracen-human-rights-group-says/

11 A script kiddie, also known as a "skid" or "skiddie," is a person who lacks programming knowledge, but uses software developed by others to launch an attack.

12 A national cyber security strategy [*strategi kemanan siber nasional republik Indonesia*] has been drafted and is under consideration by government.

13 See Galih Gumelar, 'House drops fast-tracking of data protection bill', *The Jakarta Post*, 17 November 2020, https://www.thejakartapost.com/news/2020/11/16/personal-data-protection-bill-to-be-concluded-next-year-amid-fears-of-data-breach.html

14 Presidential Decree No. 28/2021 [*Peraturan President Nomor 28/2021 tentang Badan Siber dan Sandi Negara*] was signed into force by President Widodo on 13 April. Both the Cyber Security and Resilience Bill and the Personal Data Protection Bill (*RUU Perlindungan Data Pribadi*), the latter of which provides for enhanced personal data protection and strengthening of enforcement measures, have been delayed by the DPR citing COVID-19 impacts on the legislative process

15 'The Privacy, Data Protection and Cybersecurity Law Review', Edition 7, *The Law Reviews*, Indonesia, October 2020, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-7/1234233/indonesia;

16 A Presidential Decree (*Peraturan President, Perpres*) is an executive order which does not require parliamentary approval and on occasion has been issued to circumvent delays and impediments in the legislature (DPR).

[17] Dr Widodo listed Indonesia's eleven types of critical infrastructure as: law enforcement; energy and mineral resources; transportation; finance and banking; health; information and communication technology; food (agriculture); defence and strategic industries; emergency services (social); water resources; and government.

[18] The Security Legislation Amendment (Critical Infrastructure) Bill 2020 was introduced to Parliament in 2020. The Bill enhances the existing regulatory framework by introducing a positive security obligation for critical infrastructure, including a risk management program; enhanced cyber security obligations for assets of national significance; and government assistance to relevant entities for critical infrastructure sector assets in response to significant cyber attacks. See Department of Home Affairs, 'Security Legislation Amendment (Critical Infrastructure) Bill 2020, Explanatory Document, https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf

[19] *Australia's Cyber Security Strategy*, page 29.

[20] *Australia's Cyber Security Strategy*, page 24.

[21] Office of the Australian Information Commissioner, 'About the Notifiable Data Breaches Scheme', https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/

[22] Sectoral egos (*ego sektoral*) is the Indonesian term for intra-bureaucratic rivalries.

[23] Indonesia's total defence doctrine (*pertahanan semesta*) is a holistic approach to defence which incorporate military elements, reserves and all sectors of society in a layered defence strategy. See *Kementerian Pertahanan Republik Indonesia* [Indonesian Ministry of Defence], *Buku Putih Pertahanan Indonesia* – 2015 [Indonesian Defence White Paper – 2015], https://www.kemhan.go.id/wp-content/uploads/2016/04/BPPI-INDO-2015.pdf

[24] Australia has worked with Tonga's Attorney General's Office (AGO) to draft a Computer Crimes Bill that ensured Tonga's legislation met its obligations under the Budapest Convention; and assisted Tonga's AGO with its consultations on the new Computer Crimes Bill prior to its introduction to Parliament during 2017. See page 37, DFAT, *Australia's International Cyber Engagement Strategy*, 2017, https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf

[25] Australia and Indonesia are not signatories to the Convention. See Council of Europe, Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime, Status as of 10/11/2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=KFxV3dzy

[26] See *Australia's Cyber Security Strategy*, section 15, 'Consultation'.

[27] Cyberspace is referred to as the fifth domain in military parlance after the other battle domains of Land, Air, Sea, and Space.

[28] See US Department of Commerce, 'National Institute of Standards and Technology (NIST)', https://www.nist.gov/

[29] See DownUnderCTF, https://downunderctf.com/

[30] See 'Cyber 9/12 Strategy Challenge', Atlantic Council, https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/cyber-912/https://www.atlanticcouncil.org/

[31] For definition of a sandbox server see Cloudshare, 'What is a Sandbox Environment?', https://www.cloudshare.com/virtual-it-labs-glossary/what-is-a-sandbox-environment#:~:text=What%20Are%20Sandbox%20Environments%3F,easily%20reformatted%20for%20repeated%20use.

[32] 'Border Security: Australia's Frontline', *episodate*, https://www.episodate.com/tv-show/border-security?season=16

[33] Australian Signals Directorate, Australian Cyber Security Centre, 'Advisory 2020-008: Copy-paste compromises - tactics, techniques and procedures used to target multiple Australian networks', https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks

THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

policy-futures.centre.uq.edu.au