CYBER MATURITY IN THE ASIA–PACIFIC REGION 2017

CREATING AN ASIA–PACIFIC CYBER MATURITY METRIC

ACKNOWLEDGEMENTS

The authors would like to thank several colleagues who generously contributed their time and comments to this report. Peter Jennings was integral to the initial design of this project in 2013, and his ongoing input, insights and guidance have been invaluable. Special thanks are reserved for Sophie Qin for her significant assistance in research and analysis for this report.

WHAT IS ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI INTERNATIONAL CYBER POLICY CENTRE

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

We thank all of those who contribute to the International Cyber Policy Centre with their time, intellect and passion for the subject matter. The work of the centre would be impossible without the financial support of our generous sponsors.

First published December 2017

Published in Australia by the Australian Strategic Policy Institute

ASPI

Level 2,
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
Facebook.com/ASPI.org
@ASPI_ICPC

CONTENTS

INTRODUCTION

In 2016–17, cyber maturity across the Asia–Pacific improved and the region again avoided a major incident, such as an attack on critical national infrastructure. Most online criminal activity continues to be perpetrated by non-state actors who generate significant revenue from illicit behaviour with little risk of prosecution or arrest. With notable exceptions, such as North Korean financial cybercrime and Russia's interference in the US election, countries were not engaged in flagrantly irresponsible actions during the reporting period.

Looking at the big picture, macro trends are pulling in both directions, but the overall trajectory, for now, remains positive.

On the negative side of the ledger, the region has so far escaped a major state-led cyber incident more because of the peaceful macro environment than because of strong defences and resiliency. At the individual level, more than 55% of people in the Asia–Pacific are still not connected to the internet. While this is a massive growth opportunity, it also points towards large-scale early user vulnerability as this population comes online. In the Pacific islands, various undersea cables are set to increase internet access and bandwidth; this will be a great benefit to the region but will require dramatic and rapid improvements to currently low levels of cyber maturity. This reporting period included the rise of crime-as-a-service, allowing non-experts to essentially buy and apply ready-to-use kit. This is expanding lawlessness online and further exposes regional businesses. North Korea continues to build up its malicious cyber capability. It's already been accused of a litany of crimes, including launching an online heist on the Bangladesh Central Bank and the WannaCry ransomware incident that infected over 200,000 computers in more than 150 countries. As sanctions bite, or conflict breaks out, it will do its best to retaliate.

On the positive side of the ledger, China's increasing development of indigenous intellectual property is likely to start to sway it from its past practice of sweeping commercial cyber espionage towards a more status quo power dynamic in which it wants to protect its intellectual property. China has continued to sign binding international agreements, including with Australia in 2017, prohibiting future thefts of intellectual property for commercial purposes.

High-profile ransomware incidents such as WannaCry and NotPetya, while damaging, have had the positive effect of further elevating cybersecurity issues among policymakers, and this is gradually translating into improved preparedness and responses. Some governments, such as those of Australia and the US, have been forward leaning in talking about their offensive cyber capabilities. Launching mature discussions about emerging capabilities and international legal parameters for their use appears intended both to deter and to nudge global norms in a positive direction. The announcement by Australia that offensive cyber capabilities will be used to target some offshore cybercriminals in certain circumstances points to emerging efforts to raise the costs of cybercrime and to reduce lawlessness.

Looking to the future, improvements in artificial intelligence and the development of quantum computing are likely to be initially disruptive as existing defences are outpaced. Another development, the rapid take-up of internet of things (IoT) devices, is expanding the digital attack surface. IoT devices have already been harnessed by cybercriminals and state actors to carry out large-scale distributed denial of service attacks, and in future they could be used as a point of weakness for focused intrusions against a wide range of targets.

The threat landscape and costs being imposed on governments and businesses mean that further investment across a broad front is both necessary and likely over the coming year and beyond.

GAUGING NATIONAL CYBER MATURITY

This report is the fourth in a series of annual reports examining cyber maturity trends across the Asia–Pacific. It surveys a wide geographical and economic cross-section of the region, encompassing 25 countries from South, North and Southeast Asia, the South Pacific and North America.

The International Cyber Policy Centre (ICPC) has developed a 'cyber maturity metric' methodology to assess the various facets of states' cyber capabilities. The model has been refined through engagement with Asia–Pacific experts and stakeholders so that it effectively assesses changes in state approaches and technological developments. 'Maturity' in this context is demonstrated by the presence, effective implementation and operation of cyber-related structures, policies, legislation and organisations. These cyber indicators cover whole-of-government policy and legislative structures, responses to financial cybercrime, military organisation, business and digital economic strength, and levels of social cyber awareness. The research base underpinning each of these indicator groups has been collated exclusively from information in the public domain; that is, this report's conclusions are based solely on open-source material.

To make considered, evidence-based cyber policy assessments in the Asia–Pacific context, both comprehensive data and an effective analytical framework are required. Using the data from the metric, we have also developed a stand-alone 'cyber engagement scale' for government and industry. The scale is intended to be a reference tool for identifying opportunities for the sharing of best practice, capacity building and development, plus commercial opportunities. With this additional layer of analysis, governments and the private sector can tailor engagement strategies to best fit existing levels of maturity in each policy area in each country.

2016–17 MATURITY TRENDS

ASIA–PACIFIC CYBER MATURITY: A GOVERNMENT PERSPECTIVE

The more cyber-savvy Asia–Pacific governments continue to make strides on cyber policy issues as threats and opportunities are better understood. Many less developed countries, however, continue to struggle with policy development and implementation, and the gap between the most and least prepared governments is growing.

GOVERNANCE GROWTH

In 2016–17, new or amended legislation was introduced in a number of states, and several governments enacted organisational changes to better implement cyber policy, although in comparison to last year, this year was more about implementation than the introduction of new legislation.

Australia made progress on implementing its Cyber Security Strategy, which included the appointment of its Cyber Ambassador, Dr Tobias Feakin. Organisational changes that both broadened the remit and strengthened the authority of the Australian Cyber Security Centre were also announced. Australia's mandatory data breach notification law was passed and will come into effect next year.

Organisational and legislative changes also occurred in much of the region. Indonesia created a new cyber agency, the Badan Siber dan Sandi Negara, and Thailand has proposed a National Cybersecurity Committee. Vietnam introduced a draft Law on Cybersecurity, Japan amended its personal data protection laws, and China's Cybersecurity Law came into effect on 1 June 2017.

Trendline data from this report series suggests that governments initially distribute cybersecurity responsibilities broadly across several government ministries, usually those that manage telecommunications, the economy and defence. As the importance of cybersecurity increases, a cybersecurity organisation is formally identified or established, and cybersecurity authority and responsibility are gradually centralised in that organisation. There is also a concerning trend: many governments implement cyber laws with too strong an emphasis on censorship and controlling dissent.

MILITARY USE OF CYBERSPACE

Russian interference in the 2016 US presidential election dramatically illustrated how military understanding of cyberwarfare and influence operations is still in its infancy. In hindsight, the US was caught flat-footed and struggled to mount a timely and effective response. In 2017, the WannaCry and NotPetya global ransomware incidents may also have been state sponsored, but it's difficult to know whether definitive attribution and effective deterrence have taken place.

Military use of cyberspace is still cloaked in secrecy and is often difficult to research, although some Asia–Pacific countries have started to lift the veil. Australia announced the formation of the Information Warfare Division, which is responsible for cyber offence and defence within the Australian Defence Force and will grow to 900 personnel over time. Australia also provided further detail on its offensive cyber capability, announcing that the capability had been used against Islamic State and would be used against overseas cybercriminals targeting Australia.

Recognising the importance of cyberspace in military operations, the US Defense Department has begun to elevate Cyber Command to become a unified combatant command. A number of public—although not official—reports indicate that the senior commanders have been disappointed with the effectiveness of cyber operations against Islamic State. It's also been reported that President Obama ordered the deployment of 'cyberbombs' in Russian infrastructure in response to Russian interference in the 2016 US presidential election.

Many militaries, although they undoubtedly have cyber capabilities, are absent from cyber doctrine or policy discussions, indicating that the military desire for secrecy is so far outweighing broader considerations of economic policy and transparency to reduce the risk of conflict.

As in the 2016 *Cyber maturity report*, some Asia–Pacific countries have previously indicated their intent to establish cyber units but, again, no action has been observed. Japan, by contrast, has proposed expanding its military cyber unit from around 90 to 1,000 personnel, in part to contribute to protecting the Tokyo 2020 Olympic Games from cyber threats.

INTERNATIONAL ENGAGEMENT

In 2016–17, countries such as Australia, Japan and the US that have previously recognised international engagement as a key plank of their cyber strategies continued to lead in bilateral and multilateral activities, dialogues and capacity building in conflict prevention, diplomacy, law enforcement, and computer emergency response teams (CERTs). These countries have recognised that mature cyber capabilities across the region are good for economic growth, reduce the risk of conflict and reduce the cost of cybercrime.

Despite previous progress in the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UNGGE), this year's UNGGE process broke down without agreement. It's currently unclear through which mechanisms the boundaries for international cyber behaviour will be constructed.

A number of high-profile events have underscored the real and potential impact of cyber events. Russia interfered with the 2016 US presidential election, potentially altering the outcome, and the NotPetya and WannaCry global ransomware attacks had isolated but relatively severe impacts. NotPetya and WannaCry can be categorised as near misses; that they didn't have more devastating and more widespread effects has been ascribed to luck rather than good management.

Against this backdrop, cyber espionage has continued unabated, and it's now evident that a number of Southeast Asian governments are conducting very competent cyber espionage operations. It isn't clear whether this news reflects a genuine proliferation of cyber espionage or an improvement in detection capabilities.

China has, however, signed bilateral agreements prohibiting the cyber theft of intellectual property for commercial gain—with the US and UK in 2015, and with Canada and Australia in 2017. Very little hard data is available to confirm that those agreements are being honoured, and anecdotal reports are mixed.

Significant opportunities exist for capacity building, particularly among the smaller Pacific island countries. Tonga has made excellent progress and joined the Budapest Convention on Cybercrime, but the Pacific islands joint CERT, PacCERT, continues to be dormant and without funding. Several Pacific island cable projects will enhance these nations' connections to the internet, and even a modest CERT capacity would be valuable in managing the concomitant threats.

International cooperation among law enforcement agencies has continued to grow and is discussed further in the section on cybercrime.

A BUSINESS PERSPECTIVE

Economic growth in the Asia–Pacific continues to be robust and is forecast to remain the strongest in the world at 5.5% for 2017. The internet is a key enabler of this growth, and governments are recognising the economic benefits that come with secure and reliable internet access. At the same time, however, many countries face large obstacles and must balance investment in the digital economy against requirements for essential services such as health, education and basic infrastructure.

Complaints about a lack of skilled cybersecurity personnel are a constant refrain in developed economies such as Australia, Japan and the US. As the digital economies in the region develop and demand for appropriate skills increases, it's hard to see that demand being satisfied without very significant increases in education efforts across the Asia–Pacific. Japan, motivated by the potential cyber threats that face the 2020 Tokyo Olympic and Paralympic Games, has identified business and management culture as an important point of leverage and has devoted significant efforts towards the education and professional development of senior managers. Other countries have longer term goals and require a portfolio approach towards education that will build skills among a variety of target audiences at different levels. A significant gap in education efforts persists in many Asia–Pacific economies.

There is still tremendous potential for Asia–Pacific economies to leapfrog developed economy paradigms and adopt new technologies and business models. For example, 85% of people in Papua New Guinea are unbanked, but the spread of 3G and other mobile technologies means there's potential for the adoption of mobile financial systems similar to the Kenyan M-Pesa mobile money system or even an app-based mobile payments system, such as that deployed by WeChat in China.

CYBERCRIME

There's an extensive spectrum of cybercrime maturity across the Asia–Pacific region. Countries with lower cyber maturity continue to approach cybercrime as a justification for laws which implement strong online censorship. In some cases, this focuses on censoring or suppressing content that criticises the government, while in others it's concerned with the 'appropriateness' of online information more broadly, cracking down on pornography, gambling and defamation.

In more cyber-mature countries, national police efforts address a broader array of online offences, tackling serious financial cybercrime and identity theft. They demonstrate diversified legal frameworks, strong implementation, clear cross-department coordination and efficient reporting mechanisms.

As cybercriminals have sought relative safety and relocated to jurisdictions with weak cybercrime legislation or weak enforcement, governments have responded with increasing cross-border collaboration. Last year, for example, China and the US Federal Bureau of Investigation (FBI) collaborated on cybercrime arrests; this year, Chinese nationals in Cambodia and Fiji were deported to China for cybercrimes, and Australian metadata was shared with Chinese authorities.

Sophisticated countries continue to work to improve the local cybercrime capabilities of less able countries around the region, so that each state can be effective at policing its own backyard. Tonga, although not covered in the *Cyber maturity report*, became the first Pacific island country to accede to the Budapest Convention and hosted the Pacific Islands Law Officers' Network Cybercrime Workshop. The workshop, which aimed to raise Pacific law enforcers' effectiveness in tackling cybercrime, was co-funded by the Australian Government and the European Global Action on Cybercrime Project.

METHODOLOGY

CHANGES TO THE METHODOLOGY

The ICPC is committed to continual refinement of the method used to develop this report. In 2017, we have adjusted our measure of internet connectivity and have included two additional countries, Vanuatu and Taiwan, bringing the total number of countries assessed to 25.

In 2016, we asked two separate questions to address this: 'What percentage of the population has fixed broadband access?' and 'What percentage of the population has mobile broadband access?' In 2017, the major change is that we measure and score internet connectivity using International Telecommunication Union (ITU) data for the percentage of the population that uses the internet. This change gives a more direct measure of internet usage than measuring two proxies for internet use and is a return to the methodology used in 2015. ITU data for this measure was available for all countries except North Korea and Taiwan.

RESEARCH QUESTIONS

For this report, research questions were oriented to five topics: governance; financial cybercrime enforcement; military application; digital economy and business; and social engagement. A full scoring breakdown for each question is in Appendix 1.

1 Governance

The governance topic addresses the organisational approach of the state to cyber issues, including the composition of government agencies engaged on those issues; the state's legislative intent and ability; and the state's engagement on international cyber policy issues such as internet governance, the application of international law and the development of norms or principles. These indicators provide guidance for diplomatic, government, development, law enforcement and private-sector engagement in Asia–Pacific states.

a) **What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?**

   Strong organisational structures within government for dealing with cyber matters suggest an awareness of those issues. The effectiveness and breadth of the structures are indicators of the sophistication of governments' awareness of and ability to engage on cyber issues.

b) Is there existing legislation/regulation relating to cyber issues and internet service providers (ISPs)? Is it being used?

Legislation is an indicator of the state's view on cyberspace, its understanding of risks and opportunities and its institutional ability to implement cyber-related programs. This provides guidance for engagement in capacity building and on the effects of legislation on commercial entities operating in the Asia–Pacific.

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

This question produces an understanding of the state's preferred engagement style and views on international security aspects of cyber matters, such as internet governance, international law, norms and principles and confidence-building measures, which can guide diplomatic engagement in the Asia–Pacific on those issues.

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

The existence of a service to help businesses prevent or recover from cybersecurity incidents indicates the state's awareness of that risk to business and the economy.

2 Financial cybercrime enforcement

Financial cybercrime is a critical issue for all states in the Asia–Pacific. The effect of cybercrime on ordinary people in the region is considerable and includes significant financial losses. Understanding the state's capacity to address financial cybercrime can guide engagement on enforcement, including through information sharing and capability development assistance from the public and private sectors.

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The existence of a cybercrime centre or unit indicates that the state is aware of cybercrime threats and has taken some action to address them. Specifying financial cybercrime focuses the question on an area of cybercrime that's common to all states.

3 Military application

This topic addresses the state's military organisational structure (if any) relating to cyberspace and the state's known views on the use of cyberspace by its armed forces. This can guide military-to-military engagement between states as well as diplomatic and political–military engagement. Military uses of cyberspace, particularly national capabilities, are a sensitive topic for all Asia–Pacific states, so this area requires careful consideration before states seek or agree to engagement with one another.

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

An organisational structure within the military devoted to cyber policy or cybersecurity indicates some awareness of cyber threats, and possibly the state's perspective on the use of cyber operations capabilities. This helps to identify states with which military–military engagement may be beneficial and the relevant organisational stakeholders.

4 Digital economy and business

Whether the state understands the importance of cyberspace and the digital economy, and how it understands them to be economically important, is an indicator of cyber maturity. This can guide engagement on capacity building, regional business links and engagement between government and business on cybersecurity.

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

High-quality public–private dialogue on cyber issues demonstrates a mature understanding of cyber risks within government and a good awareness within private industry. A working dialogue indicates either an opportunity for capacity-building or an opportunity to learn and implement similar strategies.

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

A state's engagement with the digital economy indicates its ability to harness the digital economy for economic growth. Comprehension of that nexus can guide government engagement on capacity building, trade development and private-sector investment.

5 Social engagement

a) Are there public awareness, debate and media coverage of cyber issues?

Public awareness of and engagement on cyber issues, such as internet governance, internet censorship and cybercrime, indicate the maturity of public discourse between the government and its citizens. Educational programs on ICT and cyber issues could also indicate a high level of technical and issues-based understanding.

b) What percentage of individuals use the internet?

The proportion of a state's population with internet connectivity indicates the type of business and personal engagement in cyberspace, the quality of ICT infrastructure and the level of citizens' trust in digital commerce. This can guide development agencies seeking to build regional economies and businesses wanting to develop trade in the region.

COMPONENTS OF THE METHODOLOGY

This report builds on the method used in previous years to assess a country's cyber maturity. It considers five key areas that, as a whole, encompass whole-of-nation approaches to cyber policy and cybersecurity. These questions were developed in 2014 through a three-stage process:

- Stage 1: Expert discussion by the ICPC formed an initial set of questions. The ICPC used open-source research and literature to provisionally assess each of the questions.
- Stage 2: The questions and their findings were then shared with a group of government, private-sector and academic experts in a focused workshop. On the basis of that discussion, the ICPC developed nine questions that together provide a reliable representation of a state's overall cyber maturity.
- Stage 3: The indicators were weighted according to their importance to a state's cyber maturity. A group of cyber experts and stakeholders from government agencies and the private sector weighted them on a scale of 1 to 10: 1 was 'not important at all' and 10 was 'extremely important'.

These expert weightings for each category were then averaged to produce a weighting factor that could be used in the calculation of an overall score.

In the final step, each country was then rated against the 10 factors, on a scale of 0 to 10 (10 being the highest level of maturity). The assessments were based on extensive qualitative and quantitative open-source research and, where possible, a comparison with the research and results from 2014, 2015 and 2016.

The overall score for each country was the sum of the scores against each factor weighted by the average calculated importance. To aid interpretation, the overall scores were converted to a percentage of the highest possible score, given the assigned weights:

$$\overline{S} = 10 \times \frac{\sum_i S_i w_i}{\sum_i w_i}$$

where $\overline{S}$ = weighted score, S = score and w = weight.

A score of 100 reflects a score of 10/10 in each category, corresponding to perfect policy formulation and implementation, as judged by the expert group.

In 2015, the factors were distributed to a group of cyber experts and stakeholders from government agencies and the private sector to account for the inclusion of an additional maturity factor (financial cybercrime enforcement). The group rated them on a scale of 1 to 10 (1 being 'not important at all' and 10 being 'extremely important'). The results of this process are shown in Table 1. Table 2 ranks countries according to their weighted scores. Table 3 shows country scores, by category.

TABLE 1: WEIGHTING ASSIGNED TO EACH CATEGORY, 2017

Weighting	Category	
8.0	1a)	Organisational structure
7.8	1b)	Legislation/regulation
7.0	1c)	International engagement
8.0	1d)	CERTs
7.8	2a)	Financial cybercrime
6.8	3a)	Military application
7.8	4a)	Government–business dialogue
7.7	4b)	Digital economy
6.0	5a)	Public awareness
7.0	5b)	Internet usage

TABLE 2: WEIGHTED SCORES, 2017

Country		Weighted score
1	United States of America	90.8
2	Australia	88.0
2	Japan	88.0
4	Singapore	87.7
5	South Korea	86.8
6	New Zealand	82.0
7	Malaysia	73.2
8	China	70.2
9	Taiwan	56.9
10	India	55.8
11	Brunei	54.7
12	Indonesia	54.3
13	Thailand	54.0
14	Vietnam	53.6
15	Philippines	49.9
16	Cambodia	36.2
17	Vanuatu	35.2
18	Bangladesh	33.1
19	Laos	30.3
19	Pakistan	30.3
21	Myanmar	29.9
22	Fiji	28.5
23	Papua New Guinea	23.6
24	North Korea	17.3
25	Solomon Islands	13.8

TABLE 3: COUNTRY SCORES, BY CATEGORY, 2017

Country	1a	1b	1c	1d	2	3	4a	4b	5a	5b	Weighted score
Australia	6.4	7.1	6.3	7.2	7.1	5.5	7.1	6.9	5.4	6.3	**88.0**
Bangladesh	3.2	2.4	2.1	2.4	3.1	0.7	3.1	3.1	3.0	1.4	**33.1**
Brunei	4.8	4.7	2.8	4.8	3.9	2.7	4.7	4.6	1.8	5.6	**54.7**
Cambodia	3.2	3.1	2.8	2.4	3.1	0.7	2.4	4.6	2.4	2.1	**36.2**
China	7.2	6.3	6.3	4.8	4.7	5.5	3.9	6.1	3.0	4.2	**70.2**
Fiji	1.6	3.1	2.8	0.0	3.1	0.7	1.6	2.3	2.4	3.5	**28.5**
India	5.6	3.9	5.6	4.0	3.1	2.1	4.7	5.4	4.8	2.1	**55.8**
Indonesia	4.8	4.7	3.5	4.0	4.7	4.1	3.9	5.4	3.0	2.1	**54.3**
Japan	7.2	6.3	7.0	8.0	6.3	4.8	6.3	6.9	5.4	7.0	**88.0**
Laos	3.2	3.1	2.1	3.2	0.8	0.7	3.1	2.3	1.8	2.1	**30.3**
Malaysia	5.6	6.3	5.6	6.4	4.7	4.8	5.5	6.1	3.6	5.6	**73.2**
Myanmar	2.4	3.1	2.8	2.4	1.6	3.4	0.8	2.3	1.2	2.1	**29.9**
New Zealand	6.4	6.3	5.6	6.4	5.5	4.1	7.1	7.7	5.4	6.3	**82.0**
North Korea	2.4	0.8	2.1	0.0	0.0	5.5	0.0	0.8	0.6	0.7	**17.3**
Pakistan	2.4	3.1	1.4	0.8	3.1	2.7	3.9	2.3	1.2	1.4	**30.3**
Papua New Guinea	3.2	3.1	2.8	0.8	0.8	0.7	1.6	0.8	3.0	0.7	**23.6**
Philippines	4.8	4.7	4.2	2.4	4.7	2.1	3.1	3.8	3.6	3.5	**49.9**
Singapore	7.2	6.3	5.6	5.6	6.3	6.2	7.8	7.7	6.0	6.3	**87.7**
Solomon Islands	2.4	0.0	2.1	0.0	0.8	0.0	1.6	0.8	1.2	1.4	**13.8**
South Korea	6.4	7.1	5.6	6.4	6.3	6.2	7.1	6.9	5.4	7.0	**86.8**
Taiwan	6.4	4.7	2.1	2.4	3.9	3.4	4.7	4.6	3.6	6.3	**56.9**
Thailand	5.6	4.7	3.5	4.0	3.9	3.4	3.1	4.6	3.6	3.5	**54.0**
United States of America	8.0	6.3	6.3	6.4	7.8	6.8	7.1	6.9	6.0	5.6	**90.8**
Vanuatu	4.0	3.1	3.5	0.8	1.6	0.0	5.5	3.1	2.4	2.1	**35.2**
Vietnam	4.8	5.5	3.5	4.8	3.9	2.1	3.9	4.6	2.4	4.2	**53.6**

LIMITATIONS OF THE RESEARCH

Some limitations in this research should be highlighted. First, there are clear limitations to the use of numerical scoring for each state, which the authors acknowledge from the outset. The numbers arrived at aren't meant to be absolute; they're provided as a guideline to the reader so that quick assessments can be made and to indicate the level of maturity within each sub-question. These numbers are intended to promote reflection and discussion and are open to the reader's interpretation. It's expected that the methodology will be refined and sharpened in subsequent iterations of this research.

Second, the data was collected entirely from open-source and unclassified sources. A significant amount of classified information isn't accessible for consideration in assessments of cyber maturity. Also, unless suitable translations could be obtained, the research is from English language sources, limiting the information available for assessments, particularly for those aspects with limited coverage in English.

ENGAGEMENT OPPORTUNITIES

A key aim of this research is to provide an assessment tool for public- and private-sector readers to help identify opportunities for engagement with the countries assessed. Therefore, in each of the 10 questions examined, we assessed the potential for engagement, and particularly the country's ability to share information and best practice or its openness to capacity-building efforts from other governments or the private sector.

Using this scale, the reader can make a quick, evidence-based, initial identification of issues and areas on which they may be able to best engage with countries in the Asia–Pacific.

A colour-coded system (explained in Figure 1) is used to illustrate engagement potential in Table 4. Table 5 explains the indicators used to measure engagement potential in each category in greater detail.

FIGURE 1: COLOUR-CODED SCORING SYSTEM TO SHOW POTENTIAL FOR ENGAGEMENT AND CAPACITY SUPPORT

Mature engagement

Engagement and development

Development

MATURE ENGAGEMENT

Dark blue indicates that the country has a well-developed understanding of the cyber maturity criteria for that particular category. Its mature level of understanding, capability or both suggest a clear avenue for engagement and potential collaboration and cooperation.

ENGAGEMENT AND DEVELOPMENT

Mid-blue suggests that, while the country has an understanding, capabilities or both in the given category, there are barriers to engagement and cooperation. However, opportunities for engagement aren't closed—they might simply require more investment and commitment than for countries with a dark blue rating.

DEVELOPMENT

Light blue suggests that there are significant barriers to engagement arising from lack of understanding, lack of capability, or wider political factors. Major investments and effort will most likely be needed to produce results.

TABLE 4: ASIA–PACIFIC CYBER ENGAGEMENT OPPORTUNITIES, 2017

	1 – Governance				2 – Cybercrime	3 – Military	4 – Digital economy and business		5 – Social engagement	
	a) Organisational structure	b) Legislation / regulation	c) International engagement	d) CERTs	a) Financial crime	a) Military role in cyberspace	a) Govt–business dialogue	b) Digital economy	a) Public awareness	b) Internet connectivity
Australia										
Bangladesh										
Brunei										
Cambodia										
China										
Fiji										
India										
Indonesia										
Japan										
Laos										
Malaysia										
Myanmar										
New Zealand										
North Korea										
Pakistan										
Papua New Guinea										
Philippines										
Singapore										
Solomon Islands										
South Korea										
Taiwan										
Thailand										
United States										
Vanuatu										
Vietnam										

TABLE 5: ENGAGEMENT OPPORTUNITIES INDICATORS

Indicator	Mature engagement	Engagement and development	Development
1 – GOVERNANCE			
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)?	Country has a transparent organisational structure with delineated leadership structure. With clear avenues for engagement and points of contact for cyber issues, there are few barriers to engagement with the government.	Government exhibits some organisational structure, suggesting clear concern about cyber issues. Unclear points of contact or incomplete cyber governance structures are a barrier to whole-of-government engagement on cyber issues. Demonstrated interest in cyber issues and incomplete government implementation offer opportunity for governance-building dialogue and sharing of best practices.	Lack of structure or other challenges are a significant barrier to engagement on cyber issues. Potential for development-based aid on cyber issues.
b) Is there existing legislation/ regulation relating to cyber issues and ISPs? Is it being used? What level of content control does the state conduct or support?	Highly developed cyber legislation, regulation, critical infrastructure policy. Clear evidence of effective implementation. Opportunity for two-way sharing of best practices.	Country has legislative or regulatory planning, but faces clear challenges in implementation, enforcement, or both. Opportunity to assist in further development of legislation, building enforcement capacity, or both.	Lacks proficient legislation, regulation or critical national infrastructure protection policy. Could benefit from external assistance in both policy development and enforcement. Candidate for adoption of existing frameworks or models (e.g. Budapest Convention on Cybercrime).
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	Full multilateral and bilateral engagement on cyber issues. Strong opportunities for constructive engagement on cyber issues. Potential for partnership to further common agendas.	Some opportunity for mainly bilateral engagement on cyber issues on a political level. Potential for dialogue to develop common agendas.	Little opportunity for engagement on cyber issues. Requires dedicated effort to engage government or private sector.
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	Established, internationally engaged CERT present. Opportunity to build CERT-to-CERT partnership and to share best practices and information.	Non-engaged national CERT team present. Opportunity to develop CERT-to-CERT dialogue.	Little or no CERT capabilities. Opportunity to help establish national CERT team.
2 – FINANCIAL CYBERCRIME ENFORCEMENT			
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	Established cybercrime centre with a strong response capability. Clear opportunity and ability to collaborate and share information on financial crimes. Potential for sharing or development of best practices.	Financial crime laws are partially enforced, or enforced domestically with limited international engagement. Opportunity to expand police–police links and establish or build information-sharing channels.	Little or no financial crime law enforcement. Limited demonstrated government interest in developing technical capabilities, anti-financial crime capabilities or both. Opportunity to help train officers and build cybercrime enforcement program.

Indicator		Mature engagement	Engagement and development	Development
3 – MILITARY APPLICATION				
a)	What is the military's role in cyberspace, cyber policy and cybersecurity?	Clear military engagement with cyber issues. Opportunity for dialogue, joint cyber exercises and information sharing.	Clear military involvement with cyber issues. Opportunities to develop or further cyber confidence-building measures.	Little or no opportunity for constructive military-to-military engagement on cyber issues.
4 – DIGITAL ECONOMY AND BUSINESS				
a)	Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	Strong government–business dialogue/interaction. Government responsive to business's cyber concerns. Healthy business environment for investment on cyber issues.	Limited government–business dialogue on cyber issues, characterised by one-sided interactions or inability to act on areas of concern.	Little or no government–business dialogue.
b)	Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	Strong digital economy business culture, including clear concerns about cybersecurity, supply-chain security and other cyber issues. Highly educated and knowledgeable workforce. Solid, digitally developed business environment for investment.	Digital economy is a growth area. Strong potential for investment, especially in digital infrastructure.	Few near-term investment opportunities in the digital economy.
5 – SOCIAL ENGAGEMENT				
a)	Are there public awareness, debate and media coverage of cyber issues?	Strong public awareness of cyber issues through new and traditional media outlets. Cyber-knowledgeable end-users and wide adoption of digital media offer strong opportunities for business-to-customer interactions.	Some awareness of cyber issues, mainly limited to new media (blogs, social media). Opportunity to aid in the building of civic understanding of cyber issues.	Little or no public awareness of cyber issues. Opportunity for wide range of educational, outreach and capacity-building efforts on cyber issues.
b)	What percentage of individuals use the internet?	Strong existing infrastructure to support advanced digital economy.	Some internet infrastructure available, often limited to urban areas. Investment opportunities for infrastructure development.	Development opportunity requiring high-level, long-term investment in basic infrastructure.

COUNTRY PROFILES

AUSTRALIA

Rank **2017:** equal 2nd of 25

2016: 4th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	8
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	9
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	9
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	9
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	8
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	9
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	9
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of individuals use the internet?	9

OVERALL ASSESSMENT

This year, the Australian Government has been focused on the implementation of the Cyber Security Strategy that was released last year, but has also made further significant announcements. On the implementation side, the Cyber Ambassador has been appointed, and both he and the Special Adviser to the Prime Minister on Cyber Security are actively engaging in building local and regional cybersecurity capacity, respectively. The government announced that the Australian Cyber Security Centre will be a focus of accountability for cybersecurity, and that it intends to clarify ministerial responsibility for cybersecurity. Engagement on public–private partnerships is evident, but at times with a lack of focus and direction.

WEIGHTED SCORE 88.0

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Australia has filled the Cyber Ambassador leadership position that was announced in last year's Cyber Security Strategy. A Minister Assisting the Prime Minister for Cyber Security and the Special Adviser to the Prime Minister on Cyber Security were appointed last year. These appointees have been advancing the cybersecurity agenda, but further clarity on roles and responsibilities would be welcome, especially in regard to Australia's cyber offensive capability. Further change is coming: the 2017 Independent Intelligence Review recommended that the Australian Cyber Security Centre have both a broader mandate as the national cybersecurity authority and to combat cybercrime, and also recommended further clarification of ministerial responsibility for cybersecurity.

SCORE: 8

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Australia passed the *Cybercrime Act 2001* to harmonise Australian law with the Budapest Convention on Cybercrime; the Act amended existing legislation for computer offences. This year, the Privacy Amendment (Notifiable Data Breaches) Act, which requires mandatory notification of serious data breaches, was passed. It will take effect in early 2018, but penalties are relatively weak, especially when compared with the European Union's General Data Protection Regulation. Australia has also been foreshadowing legislation that would compel technology and telecommunications companies to allow government access to communications. This legislation, to be modelled on the UK's Investigatory Powers Act, has not yet been introduced to parliament.

SCORE: 9

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

With the appointment of its Cyber Ambassador, Australia's international engagement is increasing, and it has released an International Cyber Engagement Strategy that sets out a broad international agenda with 61 action items. This strategy builds on the Cyber Security Strategy's three key areas of international engagement: championing a free, open and secure internet; preventing cybercrime; and building regional cybersecurity capacity. Significant effort will be required to implement the strategy.

SCORE: 9

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Australia's national CERT, CERT Australia, received additional funding and responsibility in the 2016 Cyber Security Strategy. This year, CERT Australia assumed increased responsibility for government cybersecurity programs and opened its first joint cyber security centres in Brisbane in February and Melbourne in October. The joint centres are to be focal points for collaboration between the business and research communities, along with state, territory and national agencies.

SCORE: 9

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Australian Federal Police (AFP) and state law enforcement agencies deliver a wide range of innovative and effective responses to reduce the impact and threat of cybercrime. The AFP is responsible for enforcing federal criminal law, including investigations into criminal cyber activity that affects critical infrastructure or systems of national significance. In addition, the AFP collaborates with and provides specialist support to partner agencies worldwide in the investigation of serious and organised criminal cyber activity affecting the Australian and international communities. The AFP enhances its capabilities by contributing to the design and development of whole-of-government cybercrime strategies, as well as investing in new technologies to increase its forensic and intelligence capabilities.

SCORE: 9

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

The Australian Government provided further detail on Australia's offensive cyber capability and announced the formation of the Information Warfare Division within the Australian Defence Force. The division will have responsibilities ranging from cyber defence through to cyber offence and is expected to grow to 900 staff. Australia also announced its intention to use cyber capabilities to attack and deter organised offshore cybercriminals in certain circumstances. The Australian Government has consistently stressed the responsible and lawful use of those cyber capabilities in a clear effort to set positive norms and standards. This increased transparency in the military use of cyberspace has raised Australia's score this year, but even greater transparency on the country's approach to cyber operations would be valuable for setting norms in the Asia–Pacific region.

SCORE: 8

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

A 'National Cyber Partnership' between government and the private sector is a key theme in the Australian Government's Cyber Security Strategy, and this year has involved considerable activity. The first two joint cyber security centres for public and private collaboration have been launched in Brisbane and Melbourne. The Australian Cyber Security Growth Network has been established to develop and commercialise the Australian cybersecurity industry. These actions are promising, but progress on education initiatives has been slower. Edith Cowan University and the University of Melbourne have been chosen as Academic Centres of Cyber Security Excellence, and a Cyber Security Cooperative Research Centre with $50 million of funding over seven years has been announced.

SCORE: 9

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Australians continue to embrace the benefits of the digital economy, which is forecast to grow to $139 billion by 2020, making up about 7% of GDP.[1] While Australia's ranking in the World Economic Forum's *Global information technology report* slipped to 18th in 2016, the full implementation of the National Innovation and Science Agenda may improve the forum's assessment. The digital economy is seen as an important avenue to diversify the Australian economy away from its reliance on mining and resource exports, but skills shortages may slow growth in future years if they aren't addressed in the near term.

SCORE: 9

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

The NotPetya and WannaCry global ransomware events gained very broad mainstream media coverage. Privacy, encryption and terrorists' use of the internet are perennially topical issues, and data breaches also receive broad media coverage. Russian interference in the 2016 US presidential election received considerable coverage. Despite strong awareness and media coverage of cyber issues, there's no discussion of international cyber policy and governance issues. Progress on broad-based education and training has also been slow, although there are flagship research efforts such as Data61 and the recently announced Cyber Security Cooperative Research Centre.

SCORE: 9

b) What percentage of individuals use the internet?

Australia has a high rate of internet usage. Some 88% of individuals use the internet, although prices are high and average speeds relatively low (51st in the world). Canada, which is similar in wealth, size and population density, is 24th in the world, with average speeds almost 50% faster.

SCORE: 9

1 Deloitte Access Economics, *Australia's digital pulse 2017: policy priorities to fuel Australia's digital workforce boom*, online.

BANGLADESH

Rank 2017: 18th of 25

2016: 16th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	4
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	3
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	3
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	4
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	4
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	4
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of individuals use the internet?	2

OVERALL ASSESSMENT

The Government of Bangladesh is aware of the opportunities and threats from increased connectivity. It put a Cybersecurity Strategy in place in 2014, has an Information and Communication Technology Act and is drafting a Digital Security Act. International engagement has also increased this year. However, poor infrastructure and uneven and sporadic implementation of cyber strategies mean that Bangladesh's cyber ecosystem remains underdeveloped.

WEIGHTED SCORE 33.1

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

The Bangladesh Government published a Cybersecurity Strategy in 2014, but few of the strategy's prescriptions seem to have been implemented. Bangladesh has many bodies dedicated to communications and technology matters under various ministries, but the relationships between the various bodies are unclear. It appears that cyber matters are largely handled by the Ministry of Posts, Telecommunications and Information Technology, under which are the Bangladesh Computer Council and the bdCERT. There's been discussion of launching a dedicated cybersecurity agency to coordinate the various bodies (as is set out in the Cybersecurity Strategy), but there's no evidence that any such steps have been taken so far.

SCORE: 4

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

The main piece of legislation in cybersecurity is the Information and Communication Technology Act 2006 (amended in 2013). There's significant controversy about article 57 of the Act, which appears to undermine freedom of speech. There are plans to replace the ICT Act with the Digital Security Act, but that legislation has still not been enacted. A draft bill is available, but there have been concerns that article 19 of the new Act will have the same negative effects on freedom of speech as its predecessor. The Pornography Act and the Indecent Advertisement Act are also applied to cyber activities. A designated cyber tribunal has been set up under the ICT Act to deal with cases of cybercrime, and the number of cases being filed to the tribunal is steadily increasing.

SCORE: 3

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Bangladesh is working towards greater international engagement on cybersecurity. It recently signed MoUs on cybersecurity with India and Sri Lanka, and is working towards one with Thailand. Following the cyber robbery of Bangladesh's Central Bank, Bangladesh worked with US law enforcement to track the perpetrators. The Organisation of Islamic Cooperation CERT (OIC-CERT) lists three CERTs for Bangladesh, all of which engage internationally. The BDG eGOV CIRT has signed an agreement with a Northern European consortium to set up a CIRT laboratory in Bangladesh and is a member of OIC-CERT. Bangladesh's CERTs regularly attend regional CERT events. Bangladesh also engages with the Commonwealth Telecommunications Organisation and the ITU for best practice guidance and to build capacity. It recently hosted its first International Cybersecurity Conference, it will host the Asia–Pacific Telecommunity Cybersecurity Forum, and it hosted the 2017 International Conference on Networking, Systems and Security. These activities seem to show that Bangladesh is pushing for greater engagement on cybersecurity.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

OIC-CERT lists three CERTs for Bangladesh: bdCERT, BDG eGOV CIRT and BangladeshCERT. Each appears to operate independently of the others, and each is a member of at least one international CERT organisation. bdCERT is listed by the ITU as the officially recognised CIRT, and BDG eGOV CIRT has recently signed an MoU with the Indian CERT and an agreement with a Northern European consortium to set up a CIRT laboratory in Bangladesh. BangladeshCERT is under the Bangladesh Computer Council and in the Office of the Controller of Certifying Authorities. The various CERTs have uneven capacity, and international engagement is emerging.

SCORE: 3

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Bangladesh Police Criminal Investigation Department has a Cybercrime Investigation Centre. As part of its Enhancing Cyber Investigation Capacity project, the Bangladesh Police constructed the Cyber Training Centre and the Cyber Investigation Centre, both of which opened in March last year. The project was co-funded by South Korea, and the equipment for the centres was bought from Korea, the US and Germany. The investigation centre has been used broadly, and around 100 cases have been investigated so far. Bangladesh also held a three-day international police conference in Dhaka, the declaration from which specifically mentioned increasing cooperation against cybercrime.

SCORE: 4

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

There is limited information available to suggest that Bangladesh's armed forces have an adequate awareness of cyber threats or have taken action to mitigate them.

SCORE: 1

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Despite repeated acknowledgements in the Cybersecurity Strategy of the importance of engaging the private sector, it doesn't seem that there are many specific mechanisms to facilitate dialogue between government and industry in Bangladesh. However, there was significant industry representation at Bangladesh's first International Cybersecurity Conference, and Bangladesh has also engaged foreign firms to assist in building the CIRT laboratory and the CIRT itself.

SCORE: 4

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Bangladesh's digital economy remains a small part of economic activity. The government is very aware of the opportunities that ICT offers for growth. Leveraging ICT to promote growth is one of its key goals. Bangladesh ranks 107th out of 139 in the Global Competitiveness Index, 106th out of 138 in the Networked Readiness Index and 124th in the UN e-Government Survey.

SCORE: 4

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Cybersecurity was covered in the media following the 2016 Bangladesh Central Bank hack as well as during the introduction of new cybersecurity legislation. The media closely follows the development of Bangladesh's digital economy and reports widely on digital/cyber issues. On the public debate side, there's concern about freedom of speech provisions in current and proposed legislation. There are also complaints about slow progress on government policies for cyber promotion. Grassroots movements designed to fill gaps left by the government also appear to be emerging. One example is the Bangladesh Cyber Army, which claims to be hacking back against other countries that target Bangladesh.

SCORE: 5

b) What percentage of individuals use the internet?

Only 18.2% of Bangladeshis use the internet. Despite high population densities, fixed-line broadband penetration is very low (3.8 active subscriptions per 100 inhabitants) and declining. Mobile broadband is growing strongly and is now at 17.8 active subscriptions per 100 inhabitants.

SCORE: 2

BRUNEI

Rank 2017: 11th of 25

2016: 13th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	6
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	6
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	5
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	4
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	6
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	6
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	3
b) What percentage of individuals use the internet?	8

OVERALL ASSESSMENT

Brunei continues to show slow progress in its cyber maturity. Strong censorship stifles social debate on cyberspace issues. Although Brunei's 2016 ICT White Paper recognised the need to involve business in the development of a digital economy, indicators of progress are not apparent. International cooperation and engagement remain limited and technically focused.

WEIGHTED SCORE 54.7

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Brunei has a relatively developed and effective governance structure for cyber matters in which responsibility is shared between the Prime Minister's Office, which oversees the E-Government program, and the ICT Department, the National Security Committee and the Ministry of Communications. The Minister for Communications also chairs the Brunei Information Technology Council, which includes representatives from government, industry and NGOs. The Authority for Info-Communications Technology Industry is an independent authority that handles industry regulation. Brunei published a National ICT White Paper in 2016, setting the direction for ICT policy until 2020.

SCORE: 6

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Brunei's key piece of cyber legislation is the Computer Misuse Act, enacted in 2000 and revised in 2007. The Act prohibits, among other things, unauthorised access to, modification of and use of computer materials. Other relevant pieces of legislation are the Electronic Transactions Act, the Internet Code of Practice and the Telecommunications Order. Brunei's ICT White Paper recognises the need for increased legislation on cyber matters.

SCORE: 6

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Most of Brunei's international engagement on cyber issues is focused on the Asia–Pacific region and conducted through multilateral forums. Brunei is active in ASEAN's growing cybersecurity discussions. The 16th ASEAN Telecommunications and IT Ministers Meeting was held in Brunei in November last year. BruCERT is also active in multilateral CERT forums such as APCERT, OIC-CERT and the Forum of Incident Response and Security Teams (FIRST). However, Brunei's ICT White Paper suggests little intention to leverage international engagement to develop ICT proficiency beyond using international standards as yardsticks to measure growth.

SCORE: 4

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Brunei's national CERT, BruCERT, was established in 2004. BruCERT has a well-structured and developed response capability and functions as Brunei's hub to deal with various international CERT organisations and domestic cyber stakeholders. BruCERT also plays a role in promoting awareness of cyber issues in Brunei and works with police on issues of cybercrime.

SCORE: 6

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

There is no evidence of a dedicated cybercrime centre or unit in the Royal Brunei Police Force. Brunei enforces domestic cybercrime laws through the Commercial Crime Investigation Division. Internationally, Brunei has engaged multilaterally with Interpol by attending the Interpol Asian Regional Conference and cyber training events. Brunei has also engaged with Aseanpol, which has taken steps to increase cybercrime cooperation between ASEAN states.

SCORE: 5

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Brunei's military is clearly aware of cybersecurity threats. The Defence White Paper of 2011 makes mention of cyber threats, and the Ministry of Defence newsletter and events often address the topic. The Brunei Minister of Defence travelled to Singapore for the International Cyber Week Conference, and the National Security Committee is a key player in Brunei's cyber governance structure. However, there's little evidence that Brunei has taken concrete steps to adapt to meet cyber threats. The ICT White Paper doesn't address national defence against cyber threats.

SCORE: 4

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

The Brunei Information Technology Council, which comprises government and industry representatives, is dedicated to discussing cyber issues. Not-for-profits, such as InfoCom Federation Brunei, also play a role in promoting ICT in Brunei. On the whole, however, government control in Brunei seems very pervasive, so the government dictates direction. The ICT White Paper enumerates various planned government programs to foster an ICT industry and create a digital economy. The private sector was involved in creating the White Paper, but the government doesn't seem to have accounted for businesses providing significant input in developing this part of the economy.

SCORE: 6

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Brunei's economy relies heavily on natural resources, and crude oil and natural gas extraction and production make up 90% of exports and 60% of GDP. The ICT White Paper expresses concern at Brunei's reliance on those resources and explicitly seeks to develop the digital economy to provide an alternative source of income. According to the White Paper, Brunei will try to leverage the ICT sector and the nation's geographical and political position to take 'non-traditional' routes and grow the Bruneian economy.

SCORE: 6

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Debate and media coverage in Brunei are stunted by heavy government control. Many media outlets are state-owned, and others self-censor. Therefore, genuine public awareness of cyber issues is difficult to gauge. The liberalisation of online discussion forums and a relaxation of regulations will be necessary to help overcome this problem and strengthen the national cyber debate.

SCORE: 3

b) What percentage of individuals use the internet?

Brunei has a well-developed telecommunications market, and 75% of the population has internet access. Mobile broadband is the default mode of internet access (116 subscriptions per 100 inhabitants), and fixed-line broadband access is experiencing a significant decline (it's now at fewer than 10 subscriptions per 100 inhabitants, down from 20 per 100 in 2011).

SCORE: 8

CAMBODIA

Rank 2017: 16th of 25

2016: 15th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	4
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	3
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	4
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	3
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	6
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of individuals use the internet?	3

OVERALL ASSESSMENT

Cambodia has made impressive gains in some key cyber policy and cybersecurity areas. However, the recently passed Telecommunications Law and draft copies of upcoming cybercrime legislation continue to cause concern among the Cambodian media and international commentators. Leaks have suggested that the Cambodian Government is using cyber teams and means to disrupt and defame its opposition. On the positive side, the government has unveiled an ICT development policy and a series of innovation growth initiatives, which have accelerated the progress of e-commerce in Cambodia. Cambodia has improved its cybercrime cooperation through capacity-building engagements and cooperation with international investigations. Continuing problems of poor awareness, poor infrastructure, skills shortages and weak international engagement from its national CERT detract from Cambodia's positive developments elsewhere.

WEIGHTED SCORE 36.2

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

The Ministry of Posts and Telecommunications continues to play a leading role. Supplementary roles are played by the Ministry of Commerce, the Ministry of Culture and Fine Arts and the National ICT Development Authority. The ministries have helped with the passage of new cyber laws, but there's little to suggest that there's been effective implementation of those laws. Some controversy has arisen after details of a government 'Cyber War Room Strike Team' were leaked, and it was alleged that the team was looking for means to justify the arrest of an opposition leader using digitally obtained evidence. This comes in addition to other reports of surveillance of social media for political posts. Cambodia's organisational structure remains similar to the structure in previous years, and last year's characterisation of it as merely a 'paper trail' without substance remains applicable.

SCORE: 4

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

The Cambodian Government is implementing its new national Telecommunications Law. Criticism of the new law's broad surveillance powers and significant potential penalties continues. Surveys have found that online political participation and free expression have been adversely affected by the passage of the law, finding that most respondents don't feel free to express their views online. The law has attracted the concern of the UN Human Rights Council, and there's been little work by the Cambodian Government to clarify the law's implications or to effectively communicate on the progress of its implementation. Cambodia has yet to pass an e-commerce law or a series of other laws noted as being in progress in 2016, so gaps in its cybersecurity legal framework remain.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Cambodia has been more active in engaging in multilateral forums on cybersecurity. It has taken part in ASEAN ministerial conferences on the issue, as well as in more specific, technical and capacity-building forums with Singapore, Japan and China. Overall, Cambodia has increased its international activity beyond ASEAN forums, engaging on a more granular and diverse level in 2017 compared to 2016.

SCORE: 4

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Cambodia's CERT, CamCERT, continues to issue regular monthly security alerts and receive online incident reports from the public. After a burst of international engagement in 2015–16, there's little evidence of international engagement through 2016–17. CamCERT is still not a member of APCERT, FIRST or other regional CERT groups or associations. Overall, Cambodia's CERT response capability and international engagement remain the same as last year.

SCORE: 3

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Cambodia's financial crime and intelligence units have been active in cooperating with international financial and cybercrime investigations and enhancing their capability. Cambodia cooperated with Chinese law enforcement to deport Chinese nationals found guilty of fraud in telecommunications contracts. Concerningly, some of those remanded were Taiwanese residents but were sent to the People's Republic of China. The Australian Transaction Reports and Analysis Centre (AUSTRAC) and Cambodia's Financial Intelligence Unit signed an MoU on financial intelligence information-sharing arrangements. Cambodia has also become a member of the Egmont Group, which is a regional association for financial intelligence bodies. Cambodia is conducting a second review into anti-money-laundering and counterterrorism financing (AML/CTF) approaches for its central bank, and is cooperating with the Asia–Pacific Group on Money Laundering to improve AML/CTF frameworks. Overall, while Cambodia doesn't have an explicitly designated financial cybercrime unit or team, it has significantly improved its engagement on financial intelligence issues and cooperation.

SCORE: 4

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Cambodia's military hasn't exhibited any awareness or concern about cyber threats. It has made no direct mention of the use of cyberspace, and neither senior military commanders nor the civilian defence leadership have made even veiled references to cyber capabilities and red lines. There has been some mention of networked computer capabilities in deals for military modernisation with China. However, overall, there's been almost no mention of military approaches to cyberspace.

SCORE: 1

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

After improving the quality of interaction between public and private actors through the ICT Federation, Cambodia hasn't made much appreciable progress in increasing such engagement this year. While the Ministry of Posts and Telecommunications has listed public–private partnerships as one of its key focus areas, evidence of measures to increase such partnerships remains limited. However, the ministry has stated publicly that private industry should take the lead to develop applications and products, and that government regulation will follow afterward, to avoid stifling innovation. Several large public undersea cabling projects have involved some increases in public–private dialogue, but the dialogue remains limited to specific projects. Overall, there's little evidence of an improvement in the level or quality of public–private interaction since 2016.

SCORE: 3

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Cambodia is investing heavily in e-commerce and digital economy initiatives, and there are significant grassroots digital economy ventures. The leading telecommunications company in Cambodia, Smart, has set up the Digital Innovation Fund and an innovation incubator program to improve young professionals' contributions to the digital economy. In a promising step, Cambodia has published a new Telecommunication and ICT Development Policy that identifies a series of statistics to measure the rate of digital penetration and the growth of the digital economy and sets out initiatives to develop ICT industry, literacy, e-commerce and e-government. Industry studies and public commentators continue to identify Cambodia's infrastructure, payment mechanisms and skills shortages as key barriers to a digital economy. Overall, Cambodia has made significant moves to improve on its digital economy policy. Its awareness was already high in 2016, so the substantive moves in digital economy policy push its score up significantly, doubling it for this year.

SCORE: 6

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Cambodia's awareness of cyber issues remains limited. WannaCry did not significantly affect Cambodia, and there was little media coverage of its effects. The media has been more active in covering the implications of the Telecommunications Law and draft Cybercrime Law, as well as the political controversy over the government's use of cyber means to stifle opposition. Awareness of basic safeguards remains low, and studies show that the vast majority of Cambodian computers use pirated software, contributing to the nation's high vulnerability to malware. In a positive note, Geeks in Cambodia hosts a blog featuring comprehensive coverage of conferences, award programs and other events that can improve community collaboration and education on cybersecurity. Cambodia has partnered with Microsoft to deliver better digital education and cyber skills. However, overall, there's been little change in the focus, quantity, quality or sources of coverage of cyber issues.

SCORE: 4

b) What percentage of individuals use the internet?

About a quarter of Cambodians use the internet. Mobile broadband is growing strongly, fixed-line broadband is growing moderately, and the number of fixed telephone lines is slowly declining.

SCORE: 3

CHINA

Rank 2017: 8th of 25

2016: 8th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	9
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	6
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	6
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	8
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	8
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of individuals use the internet?	6

OVERALL ASSESSMENT

Cybersecurity continues to be a hallmark of Chinese President Xi Jinping's tenure. In 2017, the legislature passed a hardline cybersecurity bill that tightened restrictions on online freedom of speech and imposed new rules on ISPs. On the international front, the country sought to promote its own 'China solution' to global cyber governance through the launch of a strategy paper that emphasised its doctrine of 'cyber sovereignty'. Chinese citizens' social engagement with cyber issues was further constrained by strict new rules that shift the censorship burden from media providers onto the users themselves. Their ability to engage with the global internet was further constricted after a crackdown on the unapproved distribution of virtual private network services.

WEIGHTED SCORE 70.2

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

China continues to step up governance efforts, including with a sweeping Cybersecurity Law that took effect on 1 June 2017. The law looks set to create an even more cloistered Chinese internet with tightened restrictions on online freedom of speech and new rules for service providers. The Cyberspace Administration of China (CAC) was formed in 2014 and has since absorbed various other agencies that were responsible for online matters. It's overseeing the implementation of the new rules at home and promoting the idea of 'cyber sovereignty' overseas. CAC struck a hard line in the country's first strategic report on cybersecurity, which aims to make a 'secure and controllable' internet.

SCORE: 9

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

The National People's Congress passed China's first and long-awaited Cybersecurity Law in November 2016. The law, which came into effect in June 2017, drew heavy criticism internationally for tightening restrictions on online freedom of speech. Included in the law are provisions that effectively kill online anonymity by forbidding unidentified netizens to post anything on internet platforms. Chinese Communist Party members have also been banned from visiting 'illegal websites' and need permission from the party before registering social media accounts. The publishing of a wide variety of information, including anything that damages 'national honour', has also been banned. Chat group administrators are now to be held personally responsible for any undesirable messages posted in their groups. The new regulations require internet companies to establish credit-rating systems for chat group users and deduct points from them when they say anything politically incorrect online. The law also requires data on Chinese citizens and other sensitive information to be stored onshore. The CAC Bureau of Cybersecurity produced the country's first National Cybersecurity Strategy Report in December 2016, outlining a plan to adopt a review process for 'key information products and services' from both domestic and foreign companies before they are sold in the Chinese market. New powers available to authorities include being able to request access to any app's or service's source code.

SCORE: 8

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

China actively participates in international cyber discussions, promoting the concept of cyber sovereignty in opposition to the US model of multistakeholder internet governance. It propagates its views on cyber sovereignty through international institutions such as the ITU and ASEAN. China has established new bilateral cybersecurity agreements with Australia and Canada covering issues that include intellectual property theft, cybercrime and norms. These relationships show a strong focus on high-level political engagement. China's score could be raised if it were to demonstrate more effective multilevel cooperation and regional capacity building.

SCORE: 9

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

China's National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT) remains active and released a report in April. It was mobilised during the WannaCry ransomware outbreak in May. The Office of the Central Leading Group for Cyberspace Affairs released a new nationwide cyber emergency response plan in June. In September, the Ministry of Industry and Information Technology said that it was creating a national data repository for information on cyberattacks. Telecommunications firms, internet companies and domain name providers are required to report threats to their platforms.

SCORE: 6

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Interpol is now headed by Meng Hongwei, who is also Vice Minister of Public Security in China. President Xi Jinping has pledged to fully back Interpol in its efforts to combat terrorism and cybercrime. More than 150 Chinese nationals were deported from Indonesia over a US$450 million cyber fraud ring in July. Others were deported from Cambodia and Fiji for running online scam operations. Domestically, inspection teams are expected to be sent out into far-flung provinces in late 2017 to check on the implementation of the country's first Cybersecurity Law. Online companies such as Baidu, Tencent and Sina Weibo have already been fined for not filtering undesirable content from their platforms.

SCORE: 6

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

The country's first strategic report on cybersecurity emphasised using all means necessary to protect its information security, including the use of its military. The People's Liberation Army Strategic Support Force is spearheading efforts to improve the country's offensive and defensive cyber capabilities. After two years in development, the Strategic Support Force continues to mature and is focused on streamlining efforts to leverage space, cyber, electronic and information warfare techniques. China also unveiled plans to become a frontrunner in artificial intelligence by 2030, which has obvious military implications.

SCORE: 8

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

The Cyber Security Association of China was established in May 2016 to engage the private sector, academia and government in the development of China's cyber policy. This industry association, which is led by the Chinese Communist Party and features Chinese tech giants Alibaba, Baidu and Tencent, is a positive development in China's cyber maturity. Foreign businesses operating in China's internet industry expressed concern that the new Cybersecurity Law would inhibit innovation and restrict trade, and more than 40 foreign companies have written to the Chinese Government, seeking to postpone the law's entry into force. In general, government–business dialogue remains one-directional in China, with a focus on compliance.

SCORE: 5

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

China's digital economy continues to be one of the most dynamic sectors in the country's overall economy. Its rapid development is helped along by government funding and a protected domestic market. In a 2017 national plan, Beijing identified artificial intelligence as an area in which the country can leapfrog the rest of the world. Online businesses faced increased regulatory imposts in 2017, and major players such as Tencent, Baidu and Sina Weibo were punished by regulators for failing to remove information posing a threat to national security from their platforms. Foreign companies are expected to comply with the new Cybersecurity Law, which requires data on Chinese citizens and other sensitive information to be stored onshore. In late July, California-based Apple removed virtual private network apps from its Chinese app store.

SCORE: 8

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

China is funnelling resources into cybersecurity education, and a cybersecurity institute is slated to open in Wuhan, Hubei Province, in 2019. The CAC also announced a major education campaign to take place in residential communities, schools and companies to raise cybersecurity awareness. Debate and media coverage in China are stunted by heavy government control. Strict new laws look set to shift the censorship burden from media providers to individual users. Chat group administrators will now be held responsible for messages containing politically sensitive material, rumours and violent or pornographic content. Chinese Communist Party members will need approval to register social media accounts and face punishment for visiting 'illegal websites'. This ever-developing architecture of surveillance is likely to have a further chilling effect on political discussion online in China.

SCORE: 5

b) What percentage of individuals use the internet?

The number of Chinese citizens using the internet continues to rise, reaching 751 million in June 2017 and making China's online population the world's largest. With a penetration rate of 53.2%, there's still plenty of room to grow. Rural areas in China account for only 27.4% of all Chinese internet users. Smartphones continue to be the device of choice for China's online population (over 95% of users access the internet via their phones). The Chinese Government expects the country's fixed-line broadband and mobile broadband penetration rates to reach 63% and 75%, respectively, by the end of 2017.

SCORE: 6

FIJI

Rank 2017: 22nd of 25

2016: 19th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	2
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	4
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	3
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of individuals use the internet?	5

OVERALL ASSESSMENT

Fiji has taken initial steps in developing its cybersecurity ecosystem, with the Cyber Security Working Group at its centre. However, governance structures, legislation and police response capability remain underdeveloped. Awareness about the need to improve in these areas is increasing, and Fiji's improving international engagement will help supply the tools required.

WEIGHTED SCORE 28.5

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Fiji's cyber governance structure remains underdeveloped. The key body is the Cyber Security Working Group, which is a multistakeholder body headed by the Fiji Police Department's Cybercrime Unit and the Ministry of Defence. The police are assisted by Fiji's Financial Intelligence Unit and Ministry of Immigration, National Security and Defence in developing legislation for cybersecurity. Last year, Fiji was reported to have been working with the Commonwealth Telecommunications Organisation (CTO) on a national development strategy, which was to be a model strategy that could be applied across the Pacific islands. To improve in this category, Fiji must both develop long-term cyber strategies and flesh out government cyber structures.

SCORE: 2

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

There's no specific cybercrime legislation in Fiji. Cyber issues are covered by Division 6 of Fiji's Crimes Decree of 2009 and the Financial Transactions Reporting Act of 2004. Although there were reports of a Cybercrime Bill and a Cyber Security Bill being drafted last year, those bills are yet to materialise. The Fiji Government recognises the importance of increased regulation in this area, particularly with cybercrime on the rise, but there appears to be little action to match that awareness.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Fiji has been active in its international engagement on cyber issues. On the multilateral front, Fiji was elected Vice-Chair of the Executive Committee of the CTO, hosted a CTO event in Fiji in September 2016 and is working with the CTO to develop a cybersecurity strategy. Fiji is also a member of ITU-IMPACT, works with an EU–ITU initiative in the Pacific islands, participates in Asia–Pacific CERT forums, and works with the World Bank and Asian Development Bank to develop infrastructure. Bilaterally, Fiji works particularly closely with Australia and China. Fiji's international engagement, however, is largely aid-based and technically focused.

SCORE: 4

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Fiji still doesn't have a CERT. It was a member of the Pacific islands' PacCERT, which has ceased operation due to lack of funding. The ITU has performed a CIRT assessment for Fiji as a first step towards developing a national CERT, but there don't appear to be further plans.

SCORE: 0

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Fiji Police Force's Cybercrime Unit is an integral part of Fiji's cybersecurity structures. The police work closely with the Financial Intelligence Unit to combat cybercrime. Fiji police have also worked closely with Australian authorities and conducted a joint operation with Chinese police, which resulted in the deportation of 77 suspected hackers to China. Despite police efforts, lack of public awareness of safe behaviour online has contributed to a rise in cybercrime, particularly phishing and cyber deception.

SCORE: 4

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Other than the Fiji military's role in forming the Cyber Security Working Group in 2011, there's no evidence to indicate that the military has a significant awareness of cyber threats or the capability to defend itself from them. Defence collaborates with the police Cybercrime Unit but does not appear to be working towards the development of a cyber strategy or military cyber capabilities.

SCORE: 1

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

In Fiji, dialogue between government and industry seems mainly confined to the Cyber Security Working Group. This public–private body, formed in 2011, includes the Ministry of Defence, the Cybercrime Unit, the Financial Intelligence Unit, licensed operators, network service providers and banks. Dialogue beyond this body seems limited.

SCORE: 2

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The digital economy isn't a significant part of economic activity in Fiji. There's evidence of awareness of the economic benefits of the digital economy and there's a desire for Fiji to develop into a financial hub for the Pacific islands. However, implementation doesn't match aspiration in this regard. Fiji lacks a long-term strategy and the requisite infrastructure to leverage the digital economy for growth.

SCORE: 3

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

There's evidence of increased media coverage of cyber issues in Fiji. Several local news sources report on cyber matters, with particular emphasis on the financial aspects of cybercrime and the expected legislation. However, public awareness of cyber matters in Fiji appears to remain low, which contributes to the increasing incidence of cybercrime in the country.

SCORE: 4

b) What percentage of individuals use the internet?

Fiji benefits from being connected to the Southern Cross fibre-optic cable, and 46.5% of Fijians use the internet. Fiji is a leader in this area among the Pacific island nations covered in this report.

SCORE: 5

INDIA

Rank 2017: 10th of 25

2016: 10th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	7
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	5
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	8
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	5
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	4
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	3
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	6
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	7
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	8
b) What percentage of individuals use the internet?	3

OVERALL ASSESSMENT

India has progressed steadily in cyber maturity during the past 12 months. Arguably, the biggest change in cybersecurity was the introduction of the National Cyber Coordination Centre, which became operational in August 2017. The government's biometric ID plans have been disrupted after the Indian Supreme Court ruled that privacy was a right of all citizens. India has prioritised its international cyber engagement in recent months: Prime Minister Narendra Modi has conducted dialogues with the UK, the US and Israel, and CERT-In has continued to collaborate with other CERTs. India has also announced plans to form CERT-Fin, which will be a CERT dedicated to financial cybercrimes. India's young population is likely to give rise to a working generation that has increased digital capabilities, resulting in great promise for the digital economy.

WEIGHTED SCORE 55.8

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

India has a complex web of cyber policies and government structures, but it lacks streamlined implementation that would allow for improved performance. The National Cyber Coordination Centre was implemented by CERT-In and became operational in August 2017. Improved delivery of the centre's cybersecurity coordination role would be welcome. In 2016, the Department of Electronics and Information Technology was promoted to ministry status, becoming the Ministry of Electronics and Information Technology.

SCORE: 7

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

The Information and Technology Act of 2000 is India's primary cybersecurity law, but it hasn't been updated since 2008. India's cybersecurity laws have been criticised for being outdated and for failing to protect citizens from cyber-bullying and online harassment. The Supreme Court recently ruled that privacy is a fundamental right of India's citizens, and that ruling will have implications for the use of Aadhaar ID cards. India enacted its National Cyber Security Policy in 2013, but in August 2017, Rudra Murthy of Digital India called for a review of the policy, which he claims isn't keeping pace with global cyber threats.

SCORE: 5

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

India has continued to engage in cyber discussions over the past year. International engagement on cyber issues is a focal point, as demonstrated by the number of MoUs signed and international trips undertaken by Prime Minister Modi. The second of a series of annual cyber dialogues with Australia and Japan was conducted in 2017. In addition, Modi has held talks with leaders from the UK, the US and Israel to discuss cyber issues. India will host the Global Conference on Cyberspace in November 2017.

SCORE: 8

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

India's national CERT, known as CERT-In, signed three new MoUs with Bangladesh, the US and Vietnam in the past 12 months. Also in the past year, the Indian Government established a botnet cleaning service known as Cyber Swatchhta Kendra that works with internet providers and anti-virus producers to protect citizens from botnet attacks. The number of incidents handled by CERT-In increased from 49,455 in 2015 to 50,362 in 2016. Incidents reported were related to website defacement, malicious code, and distributed denial of service and similar attacks. CERT-In continued to offer cyber workshops to key stakeholders in 2016, although fewer were offered than in 2015.

SCORE: 5

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The National Cyber Crime Coordination Centre was established in 2015 to focus on reducing cybercrime, particularly crime relating to child pornography. There's no significant evidence to show that the centre has made any notable progress. It was reported that cybercrime rates in India have increased from one incident every 12 minutes in 2016 to one incident every 10 minutes in the first half of 2017. India has confirmed that it will develop a financial CERT, known as CERT-Fin, to handle cyber issues relating to the financial sector. Until CERT-Fin becomes active, the Reserve Bank of India will take the lead role in policing cyber issues through its finance division. The bank has created a division that focuses specifically on monitoring the cybersecurity practices of financial institutions, and has an interdisciplinary standing committee on cybersecurity.

SCORE: 4

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

In early 2017, the Indian Army began testing the Bharat Operating System Solutions to safeguard its information from cyberespionage. Reports in March 2017 suggested that the army, navy and air force have started to collaborate on cyber issues as part of the proposed new integrated defence staff tri-service arrangements. There's been no indication that the initiative, which has been pending since the idea was introduced in 2012, is fully operational.

SCORE: 3

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

The Reserve Bank of India has continued to be a strong advocate for cybersecurity laws in the financial sector. Startup India, an entrepreneurial advocacy initiative of the Indian Government, developed a new online hub in June 2017 to increase communication among industry stakeholders. There has been criticism about the slow execution of Digital India, a once-hyped product of the Ministry of Electronics and Information Technology that has failed to significantly reduce the digital divide in India. In October 2016, it was reported that the Data Security Council of India, which is part of an industry body known as NASSCOM, is collaborating with the Department of Electronics and Information Technology (now the Ministry of Electronics and Information Technology) to fund domestic cybersecurity companies. The ministry and the Data Security Council will also work together to train and equip companies to handle security threats.

SCORE: 6

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Tech firms believe that India's digital economy has the potential to grow to US$4 trillion by 2022, but the Indian Government is more modest in its evaluation of the digital economy, predicting a worth of US$1 trillion in that time. India was labelled in the 'break out' category for the 2017 Digital Evolution Index, with a high potential for digital advancement. India has huge potential to improve its digital economy because of its 1.29 billion population. KPMG estimates that the proportion of people who own mobile phones in India will increase fourfold in the next 10 years, which will boost online banking and shopping. With 70% of India's population under the age of 45, we're likely to see the rise of a digitally capable generation that will boost the digital economy. The Data Security Council believes that the Indian market for cybersecurity will grow to $35 billion by 2025.

SCORE: 7

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

India continues to engage moderately on cyber issues in the public sphere. The Observer Research Foundation has a dedicated cyber and media focus and produces publicly available cyber reports. The foundation also holds a CyFy conference each October in New Delhi. Privacy laws in India received significant publicity in 2017, mainly because a recent ruling calls into question Narendra Modi's plan to make biometric ID cards mandatory for all Indian citizens. India continues to adopt smart technology. Cyber Safe India, an NGO that exists to spread awareness about cybersecurity issues, has produced policy recommendations for the government and offers cybersafe resources and workshops.

SCORE: 8

b) What percentage of individuals use the internet?

Although starting from a low base, India is one of the world's largest and fastest growing telecommunications markets. As in much of the Asia–Pacific region, mobile access dominates. Mobile broadband is expected to grow strongly from 16.8 subscriptions per 100 inhabitants. Fixed-line broadband is low at only 1.4 subscriptions per 100 inhabitants.

SCORE: 3

INDONESIA

Rank 2017: 12th of 25
2016: 12th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	6
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	5
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	5
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	6
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	6
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	7
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of individuals use the internet?	3

OVERALL ASSESSMENT

Indonesia has brought into force a new cyber agency and a new Telecommunications Law, which are designed to improve the country's institutional response to cyber threats and to improve data protection and privacy, respectively. While the delivery of these initiatives is promising, they come belatedly, after a series of delays in 2016. Indonesia has taken effective steps to improve its response to financial cybercrime and to engender broader digital economic development. However, the high level of state control of online content and activity has continued to increase, without a commensurate increase in Indonesia's transparency on cyber issues. A more coordinated, transparent and contestable approach to cyber issues would improve Indonesia's cyber maturity.

WEIGHTED SCORE 54.3

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Indonesia has set up a new cyber agency, the Badan Siber dan Sandi Negara (BSSN). The BSSN is designed as a supranational coordinating body with umbrella responsibility across all cyber organisations, and is under the jurisdiction of the Ministry of Communication and Informatics (Kominfo), the Encryption Agency (Lemsaneg), and ID-CSIRTII/CC, one of Indonesia's national CERTs. The BSSN has a responsibility to protect government institutions from unauthorised access and to monitor online news for false stories. The BSSN was previously set to be established in 2016 but was delayed due to a lack of funding and a general moratorium on new government agencies. While the BSSN has been empowered to play a better coordinating role, a number of organisations are working on cyber issues and the responsibilities of each haven't been clearly delineated. Indonesia continues to lack a national governance road map for cybersecurity, which has been identified as an urgent and pending priority since 2015. Moreover, it continues to lack national cybersecurity frameworks, certifications and accreditations, and instead draws its standards largely from regional or international entities. More effective coordination and governance frameworks, such as a national-level cyber strategy, would prove beneficial for Indonesia's cyber maturity. Indonesia's score for this category increased this year, returning it to the 2015 baseline.

SCORE: 6

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

The Indonesian legislature has revised its Information and Electronic Transaction Law (2008) because of the law's overly harsh penalties and vague language on how data is used. The law also sets out rights and measures in line with the EU General Data Protection Regulation's provisions for mandatory breach notification, individuals' right to be forgotten, and resolution measures for disputes over data. The law's provisions are being implemented through the Regulation on Personal Data Protection in Electronic Systems. The absence of a law on data protection was identified as a key gap in the 2016 *Cyber maturity report*, and the passage of this revised law is a positive step in cyber law in Indonesia. More could be done to coordinate and consolidate the current piecemeal legal framework on cyber issues, which spans provisions from the criminal code, business administration laws, consumer protection laws, and telecommunications, banks, human rights, corruption, freedom of information, AML/CTF and other professional regulation laws. The successful amendment of previous laws and the delivery of new data protection laws mean that Indonesia's cyber legislation has notably improved.

SCORE: 6

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Indonesia has maintained its bilateral cyber engagements with Australia, Japan and China. It has also engaged in bilateral cooperation on countering cyber-enabled violent extremism with Singapore, as well as a trilateral agreement on similar issues with the Philippines and Malaysia to counter Islamic State activities in Marawi. Indonesia has agreed to enhance cooperation and intelligence sharing with India and has taken part in multilateral discussions with Interpol and ASEAN. A pre-existing bilateral relationship with Australia has been strengthened, and Indonesia has been conducting more mature and structured dialogues with bilateral partners on a wider range of cyber issues.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Indonesia has two national-level CERTs and 14 additional CERTs covering government agencies or specific regions of the country. The Indonesia Security Incident Response Team of the Internet Infrastructure/ Coordination Centre (ID-SIRTII/CC) continues to play a leading role, providing training and education on technical capacity and cyber research and representing Indonesia's CERT community at APCERT, OIC-CERT and FIRST. ID-SIRTII/CC also organises the flagship Cyber Jawara hacking event, which is designed to increase cyber skills. The Indonesia Computer Emergency Response Team (ID-CERT), the other national-level CERT, performs a more public-facing function in publishing threat advisories, engaging stakeholders at events and sharing news. Although ID-SIRTII/ CC plays an active role in APCERT and OIC-CERT, evidence of substantially increased international engagement is limited.

SCORE: 5

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Indonesia has demonstrated a strong response capability through its cooperation with international cyber and financial crime investigations. Indonesia detained 153 Chinese members of an online fraud syndicate based in Indonesia and deported 143 of them at the request of Chinese authorities. The syndicate targeted businessmen and politicians in China and earned about US$450 million through 2017. Indonesia's law enforcement representatives have also taken part in conferences with ASEAN, Interpol and regional countries on how to counter violent extremist movements and their online activities. Indonesia's financial intelligence unit, Pusat Pelaporan Dan Analisis Transaksi Keuangan, has cooperated closely with Australia's AUSTRAC to improve financial intelligence and AML/CTF frameworks. Indonesia continues to be a leading source of malware in Southeast Asia, which suggests that Indonesia's law enforcement efforts against cybercrime could be improved.

SCORE: 6

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Indonesia's military continues to be guided by its November 2015 Defence White Paper. Indonesian military commanders have provided guidance to their troops on the dangers of 'cyber narcoterrorism' (as an extraordinary crime) and the spread of false news online. The Indonesian National Armed Forces have established their own cyber body, but its functions will also include missile tracking and satellite surveillance. Branches of the Indonesian military are reportedly looking at standing up their own dedicated units on cyber issues. After significant gains in structuring the military's role in cyber issues in 2016, there's been little activity since. More updates on programs and developments in military uses of, and thinking on, cyberspace would improve Indonesia's performance on this indicator. A clarification of the role of the military in defending networks and conducting offensive operations, and how it conceptualises its own vulnerabilities to cyber threats, would also be beneficial. Currently, cyber issues seem to be considered as a niche area within electronic and information warfare.

SCORE: 6

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Indonesia has signed a long-planned and long-awaited e-commerce road map that aims to improve interaction and reporting mechanisms between government and e-commerce actors. Indonesia's establishment of the BSSN reportedly involved some stakeholder consultation and discussions. However, most non-government actors have noted that it's difficult to be involved in cybersecurity policy discussions, and that interpersonal connections have mattered more than organisational engagement in resolving or discussing cyber issues. Indonesia has demonstrated some interest in cooperating with industry on cyber issues, such as by agreeing with Google to set up a trusted flagger and legal removal program, with moderators drawn from Indonesia's community, to flag and filter out extremist and obscene online content. Overall, evidence of public–private interaction and private-sector leadership on cyber issues remains limited, and the BSSN hasn't delivered appreciable increases in public–private interactions.

SCORE: 5

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Indonesia's e-commerce road map aims to boost the e-commerce sector and stimulate the country's overall digital economy. The road map also provides regulations on technology, logistics, cybersecurity, tax relief for tech companies, skills building and consumer protection, in addition to funding and incubation programs for innovation and digital talent. More importantly, the road map provides a means to establish a trusted national gateway for e-payment and e-commerce to improve on the infrastructure necessary for widespread digital economic activity. The gateway involves an industry-built logistics system, a national bank-built trading and payment system, and back-end transactions recording systems from the finance and statistics agencies of Indonesia. Jakarta is also looking to improve its taxation regulation of tech companies and is investigating Google for billions of dollars in unpaid taxes. Indonesia has ambitious goals in digital economic development, aiming to develop a thousand digital start-ups, a million 'digital farmers and fishermen', and 8 million digital small and medium enterprises. The significant growth in government policy for digital economic development is promising. However, ongoing problems with telecommunications infrastructure and skills shortages remain unaddressed, and proposed plans to improve e-payment remain unimplemented.

SCORE: 7

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

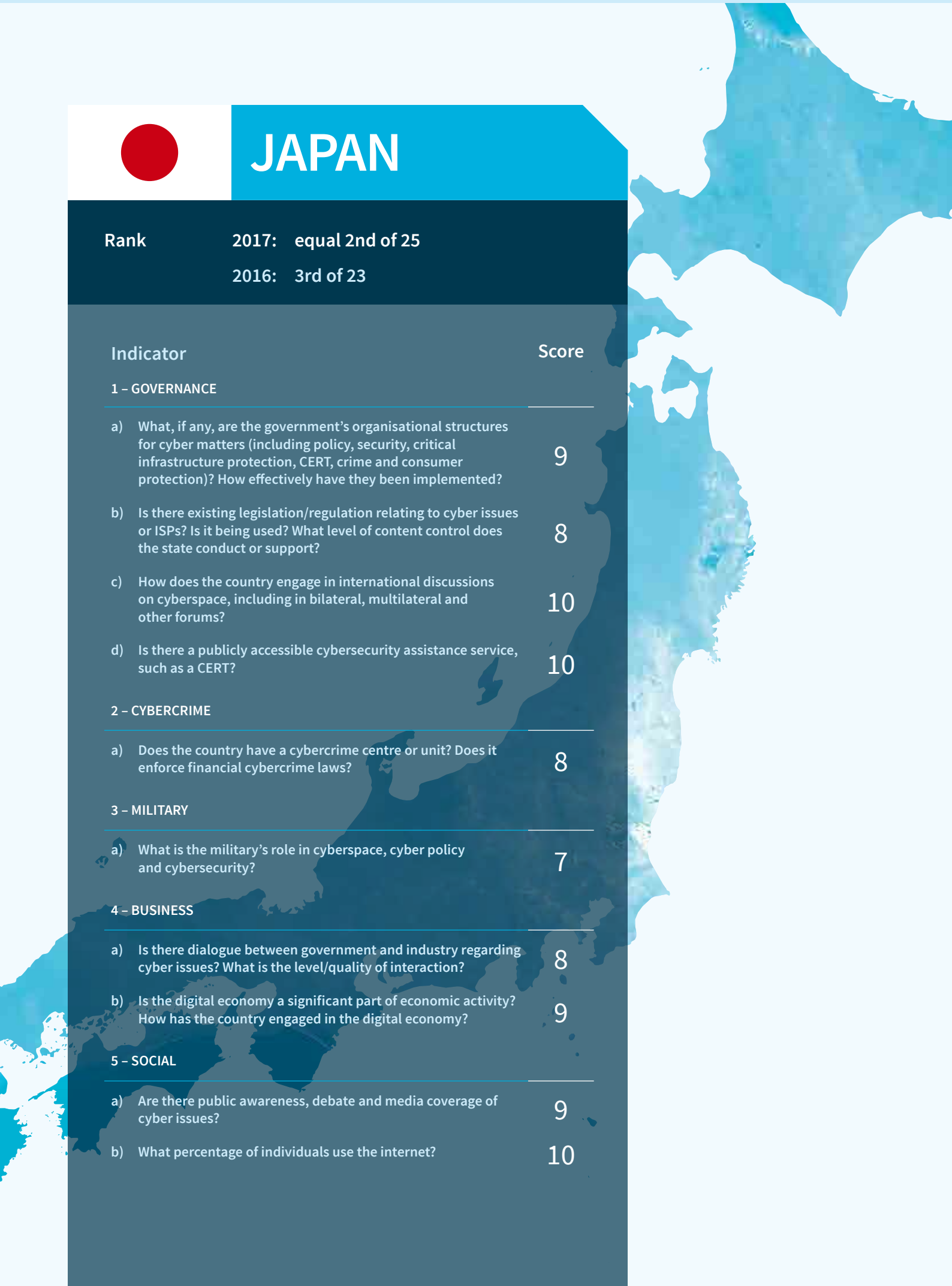
Public awareness of cyber issues has increased. Major events such as WannaCry and NotPetya were covered in depth in most sectors of the public and civil society. Ongoing government programs to restrict hate speech and extremist content online, which would go so far as to ban noncompliant websites, appear to have public support. However, journalistic and digital rights associations note that there have been instances of corrupt officials using the Information and Electronic Transaction Law to pursue other goals. Freedom of expression and government censorship remain predominant themes of the public debate on cyber issues. Despite improvements in Indonesia's data protection laws, few public-sector communities have had the chance to be actively involved in cybersecurity issues. The lack of transparency and communication from the government on these measures has dominated the public debate. Public-facing awareness initiatives have continued to expand and develop within Indonesia and spread through the region. However, freedom of the internet in Indonesia will continue to be an issue, and the lack of diversity of sources or grassroots discussion on cyber issues means that Indonesia's performance on this indicator hasn't significantly improved.

SCORE: 5

b) What percentage of individuals use the internet?

Strong mobile broadband growth has reached 67.3 subscribers per 100 inhabitants of Indonesia, although only 25.4% of the population uses the internet. As in much of the Asia–Pacific, fixed-line broadband access lags, with only 1.9 subscribers per 100 inhabitants.

SCORE: 3



JAPAN

Rank 2017: equal 2nd of 25

2016: 3rd of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	9
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	10
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	10
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	8
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	7
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	9
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of individuals use the internet?	10

OVERALL ASSESSMENT

In 2017, Japan saw further implementation and work on the country's Cybersecurity Strategy and a continuing increase in public awareness of cyber issues. Japan continued its already impressive international engagement efforts with several bilateral and multilateral meetings and a new policy on capacity building in developing countries. JPCERT/CC maintained its position as a regional leader in CERT/CSIRT best practice with an impressive domestic and international engagement program. Business engagement is also growing, including through the release of guidelines aimed at changing traditional Japanese views that cybersecurity is solely an IT problem. The Tokyo Olympic and Paralympic Games in 2020 are seen as a significant target for cyberattacks and are acting as a catalyst for improved cyber efforts.

WEIGHTED SCORE 88.0

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

The Cyber Security Strategy Headquarters is the central authority for Japan's cybersecurity and reports directly to the Japanese cabinet. Through its secretariat, the National Information Security Center implements Japan's Cybersecurity Strategy, which aims to develop and advance a free, fair and secure cyberspace to promote economic advancement. Current efforts focus on IoT security; promoting security in business; protecting citizens, critical infrastructure and government; and promoting peace and stability in the international community. This structure has proven to be responsive to events: after the high-profile hack of the Japan Pension Service in 2015, Japan's Cybersecurity Basic Act was amended to allow increased auditing and monitoring of government-affiliated agencies.

SCORE: 9

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Japan's Cybersecurity Basic Act was adopted in 2014 and amended in 2016. The Act clarified cybersecurity responsibilities and authorities and reorganised information security organisations into the Cyber Security Strategy Headquarters. Supported by the National Information Security Center secretariat, the headquarters reports directly to the Japanese cabinet. The amendment gave the centre greater powers to audit and monitor the security of government entities. Other laws also deal with cyber issues. The Japanese Government recently amended the Personal Information Protection Act to establish the Personal Information Protection Committee as an independent supervising authority and to further define how big data and transfers of personal information to third parties and across national borders should be handled.

SCORE: 8

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Japan runs a very robust program of multidimensional cyber engagement that stretches across the policy, technical and legislative realms. In the past year, this included signing the Cyber Memorandum of Cooperation with Singapore; the 2nd ASEAN–Japan Cybercrime Dialogue; the 2nd Japan–India Cyber Dialogue; the 5th Japan–US Cyber Dialogue; JPCERT technical workshops in Indonesia; hosting the Asia–Pacific CERT (APCERT) AGM and conference; and providing cyber defence training to Cambodia, Indonesia, Laos, Myanmar, the Philippines and Vietnam. In late 2016, the government issued the Basic Policy to Support Cybersecurity Capacity-Building in Developing Countries, adding to its International Strategy on Cybersecurity. This work is supported by an ambassador in charge of cyber policy and a newly established 'cyber office for national security policy' in the Ministry of Foreign Affairs. Japan is a member of the Global Forum on Cyber Expertise and has been a member of two UN groups of governmental experts on cyberspace and international security. Japan frequently discusses whole-of-government cyber issues at international high-level bilateral and multilateral political dialogues and at cyber-specific dialogues with subject-matter experts.

SCORE: 10

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Established in 1996, JPCERT/CC is Japan's national CERT and serves as the coordinating centre for all other CSIRTs in Japan. It works with government agencies, critical infrastructure operators, security vendors and broader civil society. Since the inception of APCERT, JPCERT/CC has been a steering committee member, hosted the secretariat, and been chair of the body from 2011 to 2015. JPCERT hosted the 2016 APCERT AGM and conference in Tokyo. JPCERT/CC is also a member and on the board of directors of FIRST. JPCERT/CC created the TSUBAME packet traffic monitoring system, which now serves to promote collaboration across the region and enhance the sharing of threat information. It undertakes expansive capacity building across and outside the region, lending expertise and technical training to other CERTs/CSIRTS, and also engages with higher level policy and confidence-building efforts. JPCERT/CC is working with global partners on a 'Cyber Green Initiative' to help create a 'healthy' cyberspace based upon internationally gathered and shared metrics and statistics.

SCORE: 10

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The 9th (cybercrime) division of the Criminal Investigation Bureau and the Hi-Tech Crime Technology Division of Japan's National Police Agency are responsible for investigating and prosecuting cybercrimes. The cybercrime division houses cyber experts who speak English, Chinese, Korean and Russian and is used in the defence of government organisations, defence contractors and critical national infrastructure operators. The National Police Agency is active internationally, engaging in bilateral dialogues and exchanges with other regional police forces on hi-tech crime issues. The Japan Cybercrime Control Center tackles cybercrime through collaboration between industry, academia and law enforcement.

SCORE: 8

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

The Japanese Ministry of Defense Cyber Defence Unit, which currently numbers around 90 people, is tasked with the protection of military installations, the ministry and critical infrastructure. This very limited military involvement looks like it will be expanded. It's proposed to increase staff numbers to around 1,000 and to create a working group to study cyberwarfare techniques. This is part of the government's efforts to boost cybersecurity in the lead-up to the 2020 Tokyo Olympic Games. Japan's military role in cybersecurity is complicated by the country's pacifist Constitution and its legal categorisation of cyberattacks, even when committed by nation-states, as criminal acts rather than acts of war. Further investment in military cyber defence would be welcome. Japan would also benefit from a more defined doctrine or strategy outlining how cyberspace is used in warfare and a more robust approach to protecting the defence industry.

SCORE: 7

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Business is a key stakeholder and partner in Japan's Cybersecurity Strategy. A key initiative is to change Japanese business culture, which sees IT as a cost centre rather than an area of investment and sees cybersecurity solely as an IT problem. This year, the government released *Cybersecurity guidelines for business leadership* and a draft Program to Develop Cybersecurity Human Resources. The government is also investing in developing Japan's cybersecurity industry, funding industry pavilions at overseas trade shows and establishing the Industrial Cybersecurity Center of Excellence, which will have a role in corporate cybersecurity professional development. Japanese business has responded in kind. The Japanese Business Federation, or Keidanren, has established the Advisory Board on Cybersecurity. Separately, the Industry Cross-Sectoral Committee for Cybersecurity Human Resources Development has been formed. These business groups have sent cybersecurity recommendations to the Japanese Government.

SCORE: 8

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Japan's Global ICT Strategy Bureau, housed in the Ministry of Internal Affairs and Communications, coordinates much of the Japanese Government's outputs on digital economic policy and strategy. Japan has prepared several strategies to help bolster its digital economy, including the ICT Growth Strategy II (2014), ICTs for Inclusive Social and Economic Development in Japan, the Japan Revitalisation Strategy, the 2013 Declaration to be the World's Most Advanced IT Nation, the Ministry of Internal Affairs and Communications White Paper on ICT and the Smart Japan ICT Strategy. Barriers to further growth stem from a reluctance in some sectors to adopt IT solutions, lack of skilled labour and a tradition of strong regulatory environments that inhibit change.

SCORE: 9

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

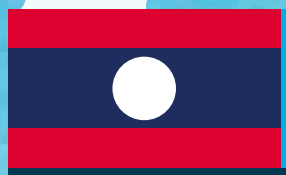
Public, business and government focus on cyber issues remains very high following high-profile hacks such as those on Sony Pictures and the Japan Pension Service and, more recently, the WannaCry and NotPetya ransomware events. There are also increasing concerns about cyber resilience in the lead-up to the 2020 Tokyo Olympic Games and the rollout of the My Number social security program. Japan has a well-developed academic research culture on cyber issues in which many universities partner with government and the private sector to develop skills programs to help fill the country's growing skills gap. Media reporting on threats and infiltrations and on new local to national government policies and organisational changes remains plentiful.

SCORE: 9

b) What percentage of individuals use the internet?

Japan's telecommunications market is one of the most developed in the world, and 92% of the population uses the internet. There are 132 mobile broadband subscriptions and 30 fixed-line broadband connections per 100 Japanese residents.

SCORE: 10



LAOS

Rank 2017: equal 19th of 25

2016: 20th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	4
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	4
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	1
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	4
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	3
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	3
b) What percentage of individuals use the internet?	3

OVERALL ASSESSMENT

The Laotian Government clearly recognises opportunities in ICT to boost development and is putting in place structures and planning to help attract investment in this area. However, connectivity remains low and there are significant geographical, economic and technical barriers to Laos achieving its goal of being a digital country. Heavy government control of industry and censorship are also concerns in Laos.

WEIGHTED SCORE 30.3

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Laos's cyber governance is spread over two ministries. The Ministry of Posts and Telecommunications is the primary ministry for cyber matters. The e-government program, the ICT Department and the Lao National Internet Centre (including LaoCERT) all fall under its purview. The ministry also sets the long-term direction of Laos's ICT industry, producing yearly and five-yearly plans. The Ministry of Science and Technology also plays a role in cyber governance. It's responsible for the macro management of information policy and the regulation of science and technology. The National ICT Development Strategy and National ICT Masterplan appear to still be under development.

SCORE: 4

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Laos has passed several cyber-related laws in recent years. In November 2016, the Laotian National Assembly passed specific legislation on ICT matters. This law and the 2015 Law on Prevention and Combating Cyber Crime, which is based on European cybercrime legislation, are positive steps towards the creation of a legislative cyber framework in the country. However, concerns remain that cyber legislation is being used to allow the Laotian Government, which strictly controls traditional media, to expand its control of online media.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Laos's international engagement in cyber matters has had a regional and technical focus. China is Laos's main partner on cyber matters, and Laos launched its first communications satellite with China's assistance in 2016. Laos also regularly engages in ASEAN ministerial meetings on cyber issues, and LaoCERT is a member of APCERT. Laos participates in capacity-building exercises with Cambodia, Malaysia and Vietnam, and ITU recommendations guide its cyber policymaking.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

LaoCERT, established in 2012, was officially announced as Laos's national CERT in 2016 and moved to the Ministry of Posts and Telecommunications. It has expanded its capabilities somewhat in the past year, providing network vulnerability assessments and advice on internet use. LaoCERT engages internationally through multilateral forums such as APCERT.

SCORE: 4

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Laos doesn't appear to have a dedicated cybercrime unit. The Law on Prevention and Combating Cybercrime states that the police should cooperate with 'the sector of posts and telecommunication and other sectors concerned' when dealing with cybercrime. Laos's police force and the Bank of Laos have a Financial Intelligence Unit for AML/CTF work. Laos has engaged both bilaterally, with regional countries, and multilaterally, through ASEAN, to combat cybercrime.

SCORE: 1

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

The Laos military and Ministry of National Defence appear to have devoted limited thinking to cybersecurity threats. Older national documents stipulate that the military has been assigned responsibility to coordinate responses to information security incidents that threaten 'national stability', but there's no evidence that this has been acted upon organisationally in any way.

SCORE: 1

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Laos is working with industry to expand connectivity and encourage investment in the ICT sector. The local industry is dominated by the government, which has a majority share in three of the six telecommunications operators / ISPs in Laos. Laos is also working with various international companies to improve connectivity.

SCORE: 4

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The Laotian Government recognises the opportunity of leveraging ICT to create a digital economy and spur growth and has a five-year ICT strategic development plan called ICT Vision 2030. There are several e-programs designed to integrate the digital revolution into various aspects of Laotian society. However, the digital economy remains only a very small part of Laos's economy. Under 25% of Laotians have access to the internet, and a lack of ICT technical capacity and infrastructure is a key hurdle to the country's progress in this area.

SCORE: 3

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

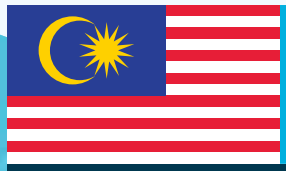
Genuine domestic debate and media coverage of cyber issues in Laos are stymied by low levels of internet connectivity. There's some discussion of ICT issues online, particularly about significant events and recent legislation. The Ministry of Posts and Telecommunications has also made significant efforts to increase digital literacy and awareness of cyber issues through the e-Education program.

SCORE: 3

b) What percentage of individuals use the internet?

Just under 25% of Laotians use the internet. Although mobile broadband subscriptions are growing strongly, the mobile market as a whole has been stifled by price regulation.

SCORE: 3



MALAYSIA

Rank 2017: 7th of 25

2016: 7th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	7
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	8
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	8
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	6
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	7
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	7
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	8
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of individuals use the internet?	8

OVERALL ASSESSMENT

Malaysia has continued to implement a comprehensive approach to cyber policy and security issues domestically and to engage on technical and policy issues with international partners. Cyber Security Malaysia (CSM) operates a range of services to assist the Malaysian public and business communities with technical cybersecurity advice and incident response. Malaysia has steadily increased its international engagement and digital economic development this year. However, slated updates to the country's cybersecurity policy, such as the introduction of a national cryptography policy, the introduction of new cyber-related laws, and policies concerning the Malaysian military's cyber operations, have yet to materialise. Their introduction would increase the maturity of Malaysia's cyber policy and security framework.

WEIGHTED SCORE 73.2

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Malaysia's score for this category remains steady in 2017, reflecting consistent progress by the Malaysian Government in the development and implementation of cyber policy. CSM, an agency of the Ministry of Science, Technology and Innovation, remains at the centre of the government's approach to cyber policy and cybersecurity issues and is working to implement a number of provisions relating to cybersecurity standards and the protection of critical national information infrastructure. CSM is also looking to enact a new National Cryptography Policy. The Malaysian Government announced that the National Security Council will be a central body for cyber governance in Malaysia and has established the National Cyber Security Agency under its guidance to better coordinate across the government. The aim is for the agency to become the 'sole agency' with experts on cyber issues in the Malaysian Government. However, the agency's coordinating strength remains unclear, which means that Malaysia's score for this category hasn't increased for this year.

SCORE: 7

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Malaysia has worked on introducing significant changes to its cyber-related legislation in 2017. A new Cybersecurity Bill was discussed and tabled in the July–August sitting of parliament. Although the details and contents of the bill haven't been publicly released, it will reportedly give authorities the ability to hamper recruitment drives by extremist groups and interfere with their online fundraising, and will set out preventive measures against money laundering and online gambling. A special 'cyber court', with judges and lawyers specially trained in cyber law, was introduced in September 2016. A similar special court has been introduced to govern the recently introduced Sexual Offences Against Children Act 2017. Amendments to the Land Public Transport Act 2010 and Commercial Vehicles Licensing Board Act 1987 were passed to make ride-sharing services legal and better regulated. These new laws and special courts are promising. However, the lack of transparency of the new Cybersecurity Bill, and the controversial use of the special cyber court to adjudicate defamation cases on behalf of the Prime Minister against individual Facebook users, pose obstacles and potential risks to the effective implementation of Malaysia's freshly updated cybersecurity legislative framework.

SCORE: 8

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Malaysia has continued its steady program of international cyber engagements in bilateral and multilateral forums. It has taken leadership roles in APCERT and OIC-CERT and supported additional efforts through the ASEAN Defence Ministers' Meeting Plus cyber working group in partnership with Singapore. A series of bilateral outreach programs has produced new agreements with the Philippines, France, Singapore, China and the UK. Malaysia has also set out clear paths for future bilateral engagement with Laos, Myanmar, Cambodia, Thailand and Vietnam. It has leadership roles in APCERT (steering committee, working groups) and OIC-CERT. Malaysia's score for this category would improve if there was further evidence of Malaysian leadership in Asia–Pacific capacity building.

SCORE: 8

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Malaysia's national CERT, MyCERT, plays an active role in Malaysia and in regional CERT associations, APCERT and OIC-CERT. Moreover, MyCERT remains part of a wider ecosystem of response agencies under the umbrella of CSM, which provides a number of other services for data recovery, a help centre, awareness, professional development, technical assessment and assurance, security evaluation and standards, vulnerability assessment, research, and complaints handling. CSM is well represented in regional events. Malaysia's performance in this category remains excellent, providing a diverse range of response capabilities and international CERT engagement and leadership.

SCORE: 8

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Malaysia's cybercrime response framework remains largely unchanged this year. The Royal Malaysian Police hosts several units that investigate and prosecute financial cybercrime, which have increased the level of their international engagement and committed to improved cooperation and data sharing with Interpol and cooperation with Australia on countering extremist funding, with New Zealand on chemical, biological, radiological and explosive elements, and with the UK and France on cyber and other global crime issues. Bank Negara Malaysia is planning to issue guidelines on cryptocurrency by the end of the year, with a focus on producing a policy to guide AML/CTP initiatives. Further evidence of an increased Malaysian role in leading Asia–Pacific responses to cybercrime and in information sharing would increase Malaysia's score for this category.

SCORE: 6

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Malaysia's score for this category has increased to reflect active improvement in the Malaysian Armed Forces' awareness of cyber threats and evidence of action to mitigate them. The Minister of Defence has publicly explained the role of Malaysia's military in cyberspace, building on a well-defined strategic conceptualisation outlined in last year's National Defence Policy. The Armed Forces Cyber Defence Operations Centre was made operational in September 2017 after nine months of testing and development and is helping the armed forces with technical training. Further enhancement of the Malaysian Armed Forces' cyber operations capability would increase Malaysia's score in this category.

SCORE: 7

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Public–private dialogue on cyber issues remains strong in Malaysia, and engagement between the government and industry through forums, conferences and other dialogues has increased sharply. Public consultation has been opened up for a number of bills and initiatives, including on a cybersecurity resilience regulatory framework and the national Industry 4.0 policy. The legislation that Malaysia has introduced this year has been well received by private-sector partners, particularly the provisions in the country's most recent budget for investment in broadband and other necessary infrastructure for the digital economy. More evidence of two-way dialogue on broader policy issues would improve Malaysia's score in this category.

SCORE: 7

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The Malaysian Government is six years into an ambitious 10-year digital economic transformation plan and has introduced several policies to realise the potential of the digital economy. The Malaysian Digital Economy Corporation has been the lead agency on this issue since 1996 and supports a number of initiatives that seek to enhance digital business, including MSC Malaysia Cybercentres, Digital Hubs and Cybercities; the Commercial Vehicle Licensing Framework for ride-sharing services such as Uber; the P2P Financing Framework; and the Fintech Regulatory Sandbox. The country's budget sets out a series of initiatives to improve youth engagement with digital technologies, with a view to improving innovation output in future generations and to address a shortage of over 1 million digital workers. Malaysia has discussed and is considering new types of taxation on foreign companies that operate in the nation's digital economy. However, it has also focused on dissolving the barriers that obstruct innovation, and has introduced the Malaysia Digital Free Trade Zone to provide physical and virtual zones for small-to-medium enterprises to start up and trade with regional partners. The zone was constructed in cooperation with noted Chinese billionaire and philanthropist Jack Ma. There's increasing discussion about Industry 4.0, building on older dialogue about the promise of e-commerce, for which a strategic road map was released this year. Malaysia is also looking to lure foreign knowledge tech entrepreneurs via a special visa/citizenship category. These measures have been well received in external studies: the World Bank has ranked Malaysia 2nd in ASEAN and 23rd in the world for digital economic development, and the Wharton School of Business has ranked it best in the world for investment. A complete integration of these separate policies and initiatives would improve Malaysia's score in this category.

SCORE: 8

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Malaysians remain concerned about cyber threats and are well supported by a number of awareness initiatives from the Malaysian Government, such as BeSmart, CyberSafe and Cyber999. Malaysia is well represented in and often hosts regional conferences and gatherings on cyber issues, especially on areas such as big data and cryptocurrency. However, surveys indicate that general cybersecurity hygiene and practice remain poor among Malaysians, suggesting that the awareness campaigns are limited in their effectiveness. Public dialogue on cyber issues seems to be in line with dialogue in other countries, being focused on WannaCry, cyber-bullying/harassment and other generally accessible cybersecurity topics, such as awareness of increased risk of attacks after a diplomatic falling out with North Korea. There's little evidence of healthy back-and-forth debate on broader cyber policy and internet governance involving a number of stakeholders and little input from academia or other civil society actors.

SCORE: 6

b) What percentage of individuals use the internet?

Malaysia has a well-developed telecommunications market, and 78% of Malaysians use the internet. Fixed broadband is growing only moderately, but mobile broadband subscriptions have grown very strongly to 92 subscribers per 100 inhabitants.

SCORE: 8

MYANMAR

Rank 2017: 21st of 25

2016: 17th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	3
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	2
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	5
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	1
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	3
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of individuals use the internet?	3

OVERALL ASSESSMENT

Myanmar's awareness of cyber matters is impeded by an organisational architecture that shows little evidence of efficient policy implementation. Myanmar's international engagement centres on receiving training from regional partners and the development of ICT infrastructure. While its military retains a strong cyber capability, the ability of authorities to respond to cybercrime is limited. The development of ICT infrastructure and increased internet access would facilitate the presence of a digital economy in Myanmar and lead to greater social engagement on cyber issues.

WEIGHTED SCORE 29.9

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Myanmar's organisational structure for cyber matters is centred on the Ministry of Communications and Technology, which houses the Myanmar Post and Telecommunications Department and Myanmar CERT. The ministry is charged with implementing a national cybersecurity strategy, policy and road map. It also maintains the Computer Science Development Council and the Computer Federation, which are designed to develop ICT policy in the country. While the work of these agencies indicates an awareness of the need to address cyber issues, and they have presented on actions taken to develop telecommunications, policy architecture would be improved through the implementation of the national Telecommunications Masterplan. The establishment of a proposed national cybersecurity centre would also improve Myanmar's score in this category.

SCORE: 3

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Myanmar's legislation to regulate cyber issues, which was developed during the country's military dictatorship, remains largely focused on censoring content. It includes the 1996 Computer Science Development Law, the 2013 Telecommunications Act and the 2014 Electronic Transactions Law. In 2017, the legislature passed the new Law Protecting the Privacy and Security of Citizens, which is designed to improve protections for privacy and against detention. However, the law has been criticised for a lack of clarity on warrant-based search and detention, which civil society advocates warn may limit freedom of expression. Myanmar's score for this category would be improved by greater evidence of effective implementation and a broader focus of legislation to address cybercrime.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Myanmar participates in some international discussion on cyberspace as a member of ASEAN, IMPACT and TSUBAME under APCERT. It has a relationship with Singapore to develop its military cyber capabilities and receives training through the Myanmar–Singapore Training Compendium. It has continued to work with Japan to develop its cyber policy. It was part of a multilateral with Cambodia, Laos and Vietnam that discussed cybersecurity policy and building norms, operational links and capabilities. Myanmar's NGOs have participated in international Track 1.5 and Track 2.0 dialogues and forums. Broader international engagement beyond Myanmar receiving training and technical expertise would increase the country's score for this category.

SCORE: 4

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Created in 2004 by the e-National Task Force, Myanmar's mmCERT works to create public awareness about cybersecurity and to provide technical assistance. It has worked with JPCERT to establish guidelines of best practice for the public and private sectors in Myanmar. It provides regular security alerts and hosts capture-the-flag exercises, drills, and exercises designed to increase cyber skills and to share knowledge and best practice. While mmCERT publishes regular security alerts, the lack of clarity on its capacity to respond to incidents limits its score for this category.

SCORE: 3

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Myanmar Police Force Criminal Investigation Department and Department of Transnational Crimes are responsible for the enforcement of cybercrime legislation in Myanmar. The police force has a 'Cybercrime Police' Facebook page. There have been continuing discussions on a possible new cybercrime body that can directly access and monitor user data from telecommunications providers for law enforcement purposes. Myanmar has taken part in regional conferences and programs designed to combat cybercrime and has received assistance to develop a stronger and more proactive crime prevention strategy. Myanmar's score for this category would increase if international engagement extended beyond Myanmar Police receiving training and if the police force enforced financial cybercrime law.

SCORE: 2

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Myanmar's military, the Tatmadaw, is reported to have a strong cyber capability that enables it to monitor online content, government opposition and dissidents in exile. It's believed that Myanmar developed this capability with assistance from Singapore and China. While the Tatmadaw exhibits an understanding of potential cyber threats and the development of capabilities to respond, its score for this category would be improved if there were greater transparency on the measures that it has adopted.

SCORE: 5

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Lack of development of Myanmar's ICT industry means there's little dialogue between government and industry on cyber issues; for example, the Law Protecting the Privacy and Security of Citizens was passed without much public consultation. The government has formed the ICT Sector Working Group with members from government and the private sector to discuss how to improve e-government coordination and how to develop the ICT sector. A new e-governance road map seeks to improve the government's engagement with the private sector on e-governance. mmCERT provides some additional contact for the private sector on technical issues, but both government and industry will need to become more active in this space to improve Myanmar's score for this category.

SCORE: 1

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Lack of infrastructure and low internet penetration prevent the development of a digital economy in Myanmar. The introduction a fourth and non-state-owned ISP has improved diversity in the telecommunications sector. There have been efforts to improve opportunities for private investment through the ongoing activities of the Phandeeyar community tech hub, which is Myanmar's first start-up accelerator. Myanmar is currently receiving assistance from the Asian Development Bank to improve its ICT development, but the bank notes that digital economic development remains challenging in Myanmar.

SCORE: 3

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Restricted internet access, limited ICT infrastructure and strong state regulation reduce public awareness, debate and media coverage of cyber matters in Myanmar. Discussion is largely focused on the development of ICT infrastructure and the digital economy and is led by external groups. Public awareness is being improved by new public–private dialogue through the ICT Sector Working Group. The government's new e-governance road map suggests that developing public awareness and debate will be a key focus. Improving these avenues for public awareness and debate, and reducing the chilling effect of strict penalties on speech online, would improve Myanmar's score for this indicator.

SCORE: 2

b) What percentage of individuals use the internet?

A quarter of the population uses the internet. Starting from a very low base, mobile broadband now reaches 48 subscribers per 100 inhabitants. Fixed-line broadband, however, is very scarce, at only 0.1 subscriptions per 100 people.

SCORE: 3

NEW ZEALAND

Rank	2017:	6th of 25
	2016:	6th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	8
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	8
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	8
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	7
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	6
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	9
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	10
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of individuals use the internet?	9

OVERALL ASSESSMENT

New Zealand has been active in implementing its Cyber Security Strategy this year, making progress in several areas. New Zealand continues to provide annual updates on the progress of the strategy and stood up a CERT on schedule. It has the new Intelligence and Security Act 2017, which consolidates and updates intelligence and national security laws and sets out the information assurance and cybersecurity role of the Government Communications Security Bureau. Studies have rated New Zealand highly for its policies on the digital economy. Ministerial briefings indicate that cybersecurity initiatives are being implemented.

WEIGHTED SCORE 82.0

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

New Zealand continues to operate a strong governance model for cyber issues, with some additions this year. The National Cyber Policy Office, within the Department of the Prime Minister and Cabinet, remains the focal point for cyber policy. The National Cyber Security Centre (NCSC), within the Government Communications Security Bureau, provides malware detection and disruption services to a select group of public- and private-sector organisations of national importance. The newly introduced computer emergency response team (CERT NZ) serves as a central point for the reporting of cybersecurity incidents. The Department of the Prime Minister and Cabinet has released the *Action Plan annual report* for 2016, providing a comprehensive update on the implementation of the Cyber Security Strategy. New Zealand continues to implement its protective security requirements. Ambitious changes in digital economic policy and social outreach are also being well implemented, which is reflected in New Zealand's scores for those indicators. New Zealand's overall organisational structure seems to be set and is implementing policies effectively.

SCORE: 8

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

New Zealand has continued to enforce robust legislation from the previous year, such as provisions in the Crimes Act 1961 and the Telecommunications (Interception and Capability and Security) Act 2013. It has taken landmark steps this year, passing the new Intelligence and Security Act 2017, which consolidates intelligence, security and oversight laws into a single Act. New Zealand also updated its *Information security manual* to provide guidance on cloud computing security. Further reviews are being undertaken into the Search and Surveillance Act 2012 on measures to preserve data prior to a warranted search; the Telecommunications Act 2001 on network infrastructure; the Customs and Excise Act 1996 on personal device access and searches; and the Privacy Act 1993 on establishing protections and penalties. New Zealand's Privacy Commissioner has expressed a desire for parliament to pass a new Privacy Act in the next year. The Law Commission review into the Extradition Act 1999 and the Mutual Assistance in Criminal Matters Act 1992 has recommended updates to simplify provisions and modernise language. The Harmful Digital Communications Act 2015 continues to operate, and its provisions have been used in public cases. While New Zealand's legal framework on cyber issues has undergone valuable review in a number of areas, evidence of effective implementation remains limited.

SCORE: 8

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

New Zealand has continued to engage with Australia, Canada, China, Singapore, the UK and the US on cyber issues, and also sent a delegation to Israel's Cyber Week. It has increased its participation in multilateral forums discussing cyber issues, has played a leadership role in regional forums, and will serve as co-chair on the ASEAN Defence Ministers' Meeting Plus Experts Working Group on Cyber Security for the next three years. New Zealand has participated in a number of ASEAN Regional Forum workshops and supported the establishment of a dedicated ASEAN Regional Forum intersessional meeting on ICT security. It will also host the next Digital 5 Conference in 2018, joining with Estonia, Israel, South Korea and the UK to discuss cybersecurity issues. Further participation in multilateral discussions on cybersecurity would increase New Zealand's score for this indicator.

SCORE: 8

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

New Zealand effectively has two CERT teams. The NCSC continues to play a complementary and critical role, providing unclassified cyber threat reports and responding to significant cyber events. New Zealand officially launched CERT NZ in April 2017, well within schedule. CERT NZ is designed to be more public-facing than the NCSC. It has taken promising steps in its first months of operation, providing timely updates and threat reports, and its responses to cybersecurity incidents have been well received. CERT NZ's challenges will be to manage the increasing demand for its five foundational services (threat identification, vulnerability identification, incident reporting services, response coordination services, and readiness support services) and to develop those services further.

SCORE: 8

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

New Zealand is taking several steps to improve its ability to prevent, investigate and respond to cybercrime. The Department of Internal Affairs is implementing Phase 2 of the AML/CFT law, which enters into force in July 2018 and 2019, expanding the compliance umbrella to the private sector progressively from July 2018. The New Zealand Police is responsible for enforcing financial cybercrime laws, runs the Financial Intelligence Unit, which deals with elements of cybercrime, and is working towards regional guidelines and engaging with regional policing bodies. The unit manages financial intelligence from across New Zealand's reporting entities, refers cases for investigation, publishes advisories on emerging technologies, and is now improving information-sharing mechanisms with the banking sector to better detect and prevent economically motivated crime. Initiatives to increase the training of the police to address cybercrime have been mentioned in an annual update, but details remain scarce and the progress of the initiative is contingent on funding. Although New Zealand has taken some actions in combating financial cybercrime, its score remains the same as last year because evidence of a response capability and stronger international engagement is limited.

SCORE: 7

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

There's been little public movement by the New Zealand Defence Force (NZDF) to clarify its role in cyberspace. Its strategic documents from 2016 are now being acted on in 2017, but public-facing updates on those actions are scarce. The NZDF Capability Plan identifies defensive (not offensive) cyber operations as a 'capability', rather than a 'support' function. The NZDF sent a delegation to the US for cyber exercises, but there's little to suggest that there's a strategic consideration of cyber capabilities. Greater clarity on the NZDF's role in this space would be welcomed.

SCORE: 6

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

New Zealand has continued to engage the private sector effectively and has provided more opportunities for public–private dialogue, which is one of the four principles of the country's Cyber Security Strategy. New Zealand's Connect Smart partnership network now includes more than 150 private-sector partners, who have met in a series of workshops to consider next steps in the implementation of the cybersecurity strategy. Private-sector representatives provide continuing direction and guidance at an advisory level. CERT NZ is guided by the CERT Advisory Board, which comprises nine private-sector representatives. Similarly, New Zealand has established the Cyber Security Skills Task Force, with representatives from industry, academia and education, to address the national cyber skills shortage. Industry has stepped into public discussions, issuing a public manifesto on New Zealand's digital future and calling for the government to implement digital transformation policies. New Zealand released the *Investor's guide to the New Zealand technology sector*, providing valuable market research on the tech sector to potential investors. It has continued hosting conferences to increase government and industry interactions and held a Digital Transformation Summit in 2017. Although New Zealand's government–industry interactions on cyber issues have been reflected in an increased score, plans for a second Cyber Security Summit in 2017 have not yet materialised.

SCORE: 9

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

New Zealand has unveiled a series of initiatives to improve its digital economy. At the operational level, the Government Chief Information Officer reports strong progress in achieving tech adoption and cost savings across government systems. More broadly, the government has released *Building a digital nation*, a report that sets out policies to strengthen New Zealand's technological growth in several emerging technologies and to increase general digital economic participation. The report builds on the Digital Economy Work Plan. External studies have noted that New Zealand's policies in this area have been world-leading. New Zealand's score has increased for this year due to the number and quality of measures it has adopted to improve its digital economic participation.

SCORE: 10

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

There are continuing initiatives to increase awareness on cyber issues. Nethui, New Zealand's key public outreach conference, has entered its second year of operation and will be co-located with an additional forum. InternetNZ and Network4Learning, which are independent not-for-profit organisations, continue to provide informative research to the public and advocate to the government on cyber issues. New Zealand's organisations advocate strongly for awareness events and days, such as Safer Internet Day and Cyber Security Awareness Month. Connect Smart Week, an awareness event for New Zealand's nationwide public–private partnership, also advanced multiple awareness initiatives. Another awareness organisation, NetSafe, has been elevated to become a New Zealand Government 'approved agency' under law and is empowered to assist victims of harmful digital communications in several ways. It provides ongoing services, consultation and speaking services on cyber issues and administers grants for online safety initiatives and projects. An NGO, iSanz, provides awards recognising the achievements of information security organisations and government agencies. Overall, New Zealand has continued to use well-developed measures to increase public awareness and dialogue on cyber issues.

SCORE: 9

b) What percentage of individuals use the internet?

Some 89% of New Zealanders use the internet, and levels of mobile and fixed broadband penetration are high. Usage of mobile broadband has increased in recent years as its geographical coverage has improved.

SCORE: 9

NORTH KOREA

Rank 2017: 24th of 25

2016: 22nd of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	1
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	0
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	8
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	0
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	1
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	1
b) What percentage of individuals use the internet?	1

OVERALL ASSESSMENT

Despite a lack of transparency on cyber governance structure and policy, it's clear that North Korea's cyber operations are highly organised and that the leadership deems cyberspace to be of great strategic value. North Korea has strong top-down and military control of its cyber operations, and cyberspace is used as a tool of state power against conventionally superior international adversaries. North Korea is believed to have conducted a number of high-profile offensive cyber operations and financial cybercrimes. Centralised control means that the development of social networks and digital economic activity remains highly restricted to a small circle of elites. North Korea is absent from international debates on cybersecurity and doesn't engage in multilateral conflict-prevention measures.

WEIGHTED SCORE 17.3

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

North Korea continues to maintain its long-established centralised control over its cyberspace through a command structure centralised within the military. Bureau 121 within the Reconnaissance General Bureau continues to govern peacetime issues. North Korea's espionage and offensive cyber operations have stepped up noticeably in the past year, indicating the continuing significance accorded to the capability by the leadership. There doesn't appear to have been additional centralisation this year, and governance efforts remain limited to the military, although that governance structure has remained effective in the execution of cyber operations. North Korea has reportedly dedicated a significant amount of its national budget to online operations and maintains a wide range of operating posts and affiliate hacking groups throughout the world.

SCORE: 3

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

The government maintains effective nationwide internet access control, which implies a strong set of national cyber regulations. The internal intranet, Kwangmyong, continues to be well managed by the Central Scientific and Technological Information Agency. In addition, evidence suggests that certain members of the North Korean population regularly use wider internet services, including international news, social media and e-commerce websites, but these exceptions to access and content controls haven't resulted in an erosion of wider information controls in society. Regulation remains inaccessible, and the lack of accessible legislation articulating these control measures limits North Korea's score in this area.

SCORE: 1

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

North Korea has remained absent from multilateral discussions on international cyber issues but it has engaged bilaterally with selected international partners. It continues to receive significant technical support from China, including internet infrastructure and staff training, and China continues to host North Korean personnel conducting international cyber operations. Russia has increased its assistance, not only providing training to North Korean personnel but also providing a second internet connection for North Korea in addition to its current Chinese-provided connections. The second connection is predicted to undermine US efforts to limit North Korean cyber operations. North Korea had a diplomatic falling out with Malaysia after North Korean agents assassinated Kim Jong-un's elder brother, Kim Jong-nam, in Kuala Lumpur. This falling out came with the expulsion of a number of North Korean diplomats and expatriates, which adversely affected North Korea's cyber operations in Malaysia. The US has become more vocal in attributing cyberattacks to North Korea and has released technical details of malicious cyber activity that it calls 'Hidden Cobra'. However, despite increased evidence of North Korea's cyber personnel maintaining a sophisticated and multipronged international presence, there remains little substantive public participation from North Korea in international discussions on cyberspace.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

There's no evidence of a CERT in North Korea. North Korea is in a unique position, in that very low levels of internet penetration are coupled with very high interest from foreign intelligence services.

SCORE: 0

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

There's good evidence that Pyongyang has a cybercrime unit that *conducts*, rather than *counters*, financial cybercrime. The theft of US$81 million from the Bangladesh Central Bank via the international SWIFT network has been attributed to North Korea, as have a number of other attacks on banks in 18 countries. The global WannaCry ransomware attack has also been attributed to North Korea, although that attack was reportedly not very profitable. North Korea has also reportedly been conducting novel attacks against cryptocurrency exchanges, successfully compromising and extracting cryptocurrency from major South Korean exchange websites such as Bithumb and Yapizon. North Korea's brazen approach to cybercrime is expected to continue over the next year.

SCORE: 0

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

North Korea's military boasts sophisticated cyber capabilities and appears to favour cyberspace as an avenue for asymmetric confrontation with its enemies. While the Reconnaissance General Bureau conducts covert cyber operations during peacetime, the General Staff Department of the Korean People's Army is responsible for cyber operations in support of conventional military efforts during conflict. In this sense, North Korea conceives cyber operations both as an independent force projection and as a supporting element of military activity. The country's investment in cyber capability remains sizeable, and it was recently able to access a secure South Korean military network and extract a large volume of highly sensitive documents and data, including several particularly sensitive operational planning documents relating to South Korean contingency plans and a possible decapitation strike against the North Korean wartime leadership. The full impact and nature of the breach of South Korean military data aren't yet clear, but the breach suggests sophisticated capability and significantly complicates the response planning of South Korea and US military officials for cyber, conventional or nuclear conflict. However, there is no published strategy or accessible doctrine espousing North Korea's approach to cyberspace. This shortcoming, and the absence of international military engagements on cyber issues, have limited North Korea's score for this indicator.

SCORE: 8

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

There's no evidence of dialogue within North Korea, where most companies are owned by the state. There have been few cases of foreign investment in the past year, although Russian state-owned TransTeleCom has opened a new internet connection for North Korea that now provides most internet connections within the country. The level of public–private interaction that took place to achieve this connection isn't clear. The level of involvement of North Korea's emerging business community and merchants on cyber issues is also unclear. Sanctions and North Korea's poor track record of relations between government and industry is likely to continue to discourage foreign investment in the digital economy and leave North Korea's government–business dialogue at a low level and quality of interaction.

SCORE: 0

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The digital economy doesn't form a significant part of North Korea's economy in the traditional sense, but efforts in financial cybercrime are reportedly now a significant and increasing part of the government's operating budget. North Koreans based overseas reportedly play a large part in these cyber operations. Within the country, a relatively small circle of elites is reportedly internet connected and regularly takes part in the global digital economy through international e-commerce websites, social media and other digital platforms. Beyond this elite access, however, internet infrastructure is restricted and of poor quality, and North Korea's digital economic activity remains very low.

SCORE: 1

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Because of the widespread lack of connectivity, there's little awareness of cyber issues outside government-mandated operations. Any public dialogue that does take place is likely to be stifled by strong government regulation and censorship. Cyber skill recruitment campaigns continue to be run through the tertiary education system, providing a steady flow of talent for North Korea's expanding and sophisticated cyber operations network. A study of internet traffic from North Korea indicates that a small subset of the country's population is actively engaged in the wider internet and well aware of international news and developments, but that awareness is limited to a small circle of elites. Debate remains limited or non-existent.

SCORE: 1

b) What percentage of individuals use the internet?

There is no data available for North Korea, but it's likely that less than 10% of the population is connected to the internet.

SCORE: 1

PAKISTAN

Rank 2017: equal 19th of 25

2016: 18th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	2
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	1
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	4
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	4
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	3
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of individuals use the internet?	2

OVERALL ASSESSMENT

Pakistan has consistently struggled to enact cybercrime legislation and policy, but in 2016 the Prevention of Electronic Crime Bill made its way through parliament. It's hard to see effective implementation, however, although there are signs that Pakistan is beginning to seize opportunities presented by the digital economy. Cyber maturity is very patchy: the country has an underdeveloped CERT and very poor internet connectivity. Military capabilities exist, but they are opaque and not being harnessed for the good of the broader economy.

WEIGHTED SCORE 30.3

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Pakistan's Ministry of Information Technology is the lead agency for the planning, coordination and implementation of policies and programs relating to IT. The Pakistan Government has made several attempts to implement cyber policies or legislation, but those efforts have tended to be either short-lived or unsuccessful. For example, a 2007 executive ordinance for the prevention of electronic crimes expired in 2009, and only in 2017 has a new Prevention of Electronic Crimes Act been passed. Neither a National Cyber Strategy nor a National Cyber Security Council Act has materialised, although both were announced in 2014.

SCORE: 3

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

In August 2016, the Prevention of Electronic Crimes Act was passed. The Act includes provisions related to both information security and, controversially, information control. The bill was criticised as being too harsh and too vague and an attempt to curtail freedom of speech. It was also criticised for the lack of effective enforcement against genuine threats such as extremist content and cybercrimes, although there have been a number of prosecutions for cyber-stalking and harassment.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Pakistan engages in a limited range of international cyber-oriented discussions. Much of its current international outreach is tied to work with the ITU, hosting workshops and receiving aid for training programs. Pakistan also probably leans on traditional allies such as China for assistance with cyber issues. In 2017, the government was accepted into the Shanghai Cooperation Organisation, which could boost Pakistan's international engagement on cyber issues.

SCORE: 2

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

PakCERT is Pakistan's national CERT, and PISA-CERT is its first public CERT. PISA-CERT represented Pakistan at a 2016 OIC-CERT cyber drill. Last year, PakCERT seemed to be dormant, but this year it's organising regular training courses.

SCORE: 1

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Federal Investigation Agency's National Response Centre for Cyber Crimes (NR3C) is the national body responsible for policing cybercrime in Pakistan. It has the ability to carry out digital forensics, IT system security audits and penetration testing. The NR3C works with and trains other law-enforcement and judicial bodies to investigate online crime and raise awareness, capability and resilience. It also performs this awareness-raising role in the broader community and has established the Cyber Scouts program to train students in IT skills. The NR3C also maintains an online cyber complaint service and 24/7 hotline for the public to report cybercrimes.

SCORE: 4

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Pakistan's Inter-Services Intelligence agency is said to possess both defensive and offensive cyber capabilities, although the extent of those capabilities is largely unknown. Under the Prevention of Electronic Crime Act, the agency has been given authority to act against those breaching national security, but further explanation of its authorities, capabilities and oversight of cyber operations would be welcome.

SCORE: 4

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

The Pakistan Government has established Ignite, which is a national ICT R&D fund that aims to 'transform Pakistan's economy into a knowledge based economy by promoting efficient, sustainable and effective ICT initiatives through synergic development of industrial and academic resources'. Cybersecurity is one of Ignite's thematic areas for R&D, and many other themes contain a cyber component. In 2017, the government established national incubation centres in Karachi, Lahore and Peshawar. In additional, Ignite plans to train 1 million students in IT freelancing over the next five years. The Ministry of Information Technology's draft Digital Pakistan Policy also recognises the importance of cross-sector collaboration.

SCORE: 5

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Despite relatively poor internet access (only 15% of the population uses the internet), Pakistan performs strongly in the freelance programming market, ranking third behind the US and India, and the country's IT exports have grown 20-fold over the past decade. The draft Digital Pakistan Policy strongly emphasises growing Pakistan's digital economy, and policies to encourage that growth include tax concessions, subsidised technology parks, subsidised bandwidth, marketing and more. The policy also outlines a comprehensive suite of key components, including legislation, education, infrastructure and entrepreneurship. This is a promising sign, but Pakistan has a long history of stalled cyber initiatives, so implementation will be closely watched.

SCORE: 3

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Public awareness of cyber issues in Pakistan is rising off a low base. Coverage of cyber topics in the media is generally related to prosecutions for blasphemy or harassment. The Pakistan Information Security Association, an information security professional association, conducts events, prepares publications to boost the skills and awareness of its members, and runs cybersecurity awareness-raising seminars. Other groups tackling cyber issues are often concerned with state surveillance.

SCORE: 2

b) What percentage of individuals use the internet?

Pakistan has low fixed and mobile broadband penetration (0.9 fixed and 20 mobile broadband subscribers per 100 inhabitants), and only 15% of the population uses the internet. Further growth in internet access will depend on widespread and cost-effective mobile broadband.

SCORE: 2

PAPUA NEW GUINEA

Rank 2017: 23rd of 25

2016: 21st of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	4
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	1
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	1
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	1
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of individuals use the internet?	1

OVERALL ASSESSMENT

Papua New Guinea (PNG) continues to take a limited approach to cyber governance, despite recent efforts at legislative reform, including the Cybercrime Policy and the Sim Card Registration initiative. Policy implementation remains patchy, while PNG's international cyber engagement is centred on financial and technical support. PNG recognises potential cyber threats but lacks the military capability to defend against them. The government seeks to pursue private-sector partnerships to develop the country's ICT industry, which is impeded by limited infrastructure. While a large rural population has little internet access, public awareness of cyber issues is evident. A more comprehensive cyber strategy and effective policy implementation would improve PNG's score.

WEIGHTED SCORE 23.6

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

PNG's organisational structure remains largely focused on the development of ICT infrastructure. The Department of Communication and Information and the National Information and Communications Technology Authority are responsible for cyber matters. The authority drafted the 2016 National Cybercrime Policy, which is the first significant new cyber policy in PNG since 2013. Cybercrime response remains the key organisational theme for PNG's cyber governance structures, although some organisations are coalescing to coordinate and manage undersea telecommunication cable projects that route through PNG. A new national cybersecurity policy and strategy, for which public submissions recently closed, is being developed. The new strategy was slated for a 2017 release, in partnership with the ITU, but details of a publication timeline haven't been made public. The release of the strategy would boost PNG's score for this category.

SCORE: 4

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

PNG's parliament passed the Cybercrime Act 2016, building on pre-existing policy to better respond to cybercrime and improve information governance. Criticism of its heavy penalties and potential to suppress online freedom of expression continues. It also lacks an effective enforcement capacity to reduce crime where that's needed. A novel Integrated Government Information System was announced and is being developed by PNG Data and the Department of Communication and Information for better e-government, although details are scarce.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

PNG participates in a number of multilateral forums through APEC, the Pacific Islands Telecommunications Association, the ITU, the Asia–Pacific Telecommunity, and the Pacific ICT Regulatory Resource Centre, which it chairs. It has played a leading role among the Pacific island states, hosting several meetings and conferences in multilateral forums. It has identified cyber threats as a key security issue at a bilateral ministerial forum with Australia. Most importantly, in cooperation with the ITU, PNG is currently developing a national cybersecurity policy and strategy, which is expected to be released this year. Broader international engagement and a wider range of bilateral engagements would improve PNG's score for this category.

SCORE: 4

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

PNG has no national CERT, and has not had access to a CERT since the closure of PacCERT. It's discussing the creation of a CERT with the ITU, and has broached the topic in other regional discussions and a capacity-building workshop.

SCORE: 1

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Intelligence Unit of the Royal Papua New Guinea Police Intelligence Unit is responsible for enforcing cybercrime law in PNG. In 2014, the police established a cybercrime taskforce, with plans to provide training for officers and increase the force's response capability; however, effective implementation of this initiative remains to be seen. An additional national cybercrime unit is reportedly being established within the force. Some evidence of enforcement capability and coordination has been demonstrated; for example, PNG Customs has cooperated with the National Information and Communications Technology Authority to stop illegal ICT imports. More evidence of implementation of the country's cybercrime taskforce and the expected establishment of the national cybercrime unit would increase PNG's score for this category.

SCORE: 1

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

PNG's military doesn't appear to have a cyber strategy. While PNG's 2013 Defence White Paper illustrated an awareness of cyber threats, it did not indicate any capability to defend against them.

SCORE: 1

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Dialogue between government and industry on cyber issues is limited, and no officially recognised national or sector-specific initiatives are apparent. Some dialogue with the ITU on a cybersecurity strategy, the national cybercrime unit and e-agriculture may improve the quality of public–private interaction. A new gateway submarine cable from Sydney to Port Moresby, funded by the World Bank and the Australian Government, may also improve the quality of interaction. However, evidence of an improvement in dialogue and in the range of dialogue partners remains limited.

SCORE: 2

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

PNG's digital economic development is constrained by a lack of ICT and other infrastructure and its largely rural population. Most of the people lack electricity and don't use banking services, and internet access costs are prohibitively high for small business. A series of promising initiatives in PNG universities, and one notable program from ExxonMobil, are improving cybersecurity skills in PNG. Agricultural workers have reportedly improved their marketing and selling with the use of 2G-based mobile phones. While the proposed submarine cable may resolve some of these constraints, overall awareness of the digital economy is low and policy supporting its development is lacking.

SCORE: 1

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Despite internet access constraints, public awareness and debate on cyber issues have been comparatively vibrant. The recent passage of the Cybercrime Act sparked considerable discussion in the blogging community, and PNG's traditional media was able to comment freely on the topic. More debate from a wider range of actors would improve PNG's score on this indicator.

SCORE: 5

b) What percentage of individuals use the internet?

Just under 10% of Papua New Guineans use the internet. Fixed-line and mobile broadband penetration are low, and PNG's mountainous geography makes it difficult to provide even mobile broadband for broad swathes of the population.

SCORE: 1

PHILIPPINES

Rank 2017: 15th of 25

2016: 14th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	6
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	6
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	3
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	6
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	3
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	4
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	5
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of individuals use the internet?	5

OVERALL ASSESSMENT

The Philippines has had a positive year of cybersecurity engagement. The three main entities responsible for cybersecurity are the Department of Information and Communications Technology (DICT), the Department of Justice Office of Cybercrime and the Philippines National Police Anti Cybercrime Group. All three are pursuing a more secure internet. DICT released the National Cybersecurity Plan 2022 in May 2017, focusing on critical infrastructure, cyber resilience and law enforcement coordination. DICT has also announced the National Broadband Plan to support broadband demand. The Office of Cybercrime has collaborated internationally to prevent and prosecute cybercrime. The Philippines re-established a CERT in late 2016 and has signed a trilateral agreement with Malaysia and Indonesia to stop the spread of online terrorist propaganda. While there have been announcements from the military about future cybersecurity projects, there's no evidence of follow-up action. The Philippines has made efforts to increase its education programs on cybersecurity and has a promising digital economy.

WEIGHTED SCORE 49.9

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

DICT, which was created at the start of 2016, houses the Cybercrime Investigation and Coordinating Center. Other agencies working within DICT include the National Telecommunications Commission and the National Privacy Commission. The Department of Justice manages the Office of Cybercrime, which coordinates international cybersecurity efforts. The Philippines National Police Anti Cybercrime Group plays an important role in educating the public about cyber issues.

SCORE: 6

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

DICT was established by an Act of the Philippine Congress in 2016. In May 2017, DICT announced the new National Cybersecurity Plan 2022. The plan has several key objectives: to improve the security of critical information infrastructure, to protect government and to increase cybersecurity knowledge in private industry and among individual citizens. In 2017, DICT also established the National Broadband Plan, which aims to increase government investment in broadband infrastructure and to support higher demand.

SCORE: 6

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

The Philippines continues to engage with other ASEAN nations on cyber issues. In August 2017, it hosted the 2nd ASEAN Telecommunications and Information Technology Senior Officials Meeting ASEAN Telecommunications Regulators' Council Leaders' Retreat, attended by telecommunications representatives from the 10 ASEAN member states. The Department of Justice's Office of Cybercrime assisted with 20 international cyber requests in 2016. The department also coordinated with the Council of Europe to run the Regional Conference on Cybercrime 2017, which focused on enhancing regional and international cooperation on cyber matters. The Philippines signed a trilateral agreement with Malaysia and Indonesia in June 2017, aiming to prevent terrorist propaganda from proliferating online.

SCORE: 6

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

The Philippines registered a new CERT, known as CSP CERT, in August 2016, and soft-launched the CERT in December 2016. CSP CERT has taken over from PHCERT, which was disbanded in June 2016. CSP CERT provides digital forensics and incident response; a CERT response centre; research and development; and a cybersecurity enablement team. The US State Department, FBI, and CMU CERT partnered with CSP CERT to get the program established.

SCORE: 3

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Cybercrime Investigation and Coordinating Center, an agency of DICT, was formed as a result of the Cybercrime Prevention Act of 2012. The centre is tasked with forming cybersecurity policies, suppressing and monitoring cybercrime, and cooperating with international agencies on cyber matters. The Department of Justice's Office of Cybercrime produces yearly reports, enforces the Cybercrime Law and has a particular focus on online gambling and child abuse. The National Bureau of Investigation and Philippine National Police Anti Cybercrime Group are both actively enforcing cyber laws.

SCORE: 6

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

In July 2017, the Armed Forces of Philippines (AFP) Public Affairs Chief stated that the AFP will build a cyber workforce. The announcement came soon after the AFP conducted a cybersecurity summit, which was attended by representatives from DICT, the Philippines National Police Anti Cybercrime Group and other partners. The military has announced that it's developing a Cyberspace Strategic Plan, which will be available later in 2017. The US military collaborated with the AFP for a two-day cybersecurity dialogue in Quezon City in May 2017, exchanging ideas about risk management and how to create policy. While there have been some promising announcements from the military in 2017 about its willingness to prioritise cybersecurity, at the time of writing no policy from the AFP is available and the workforce is yet to be established. Effective implementation of these proposed changes over the next year would raise the Philippines' score in this category.

SCORE: 3

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

DICT is currently working on iGovPhil, which is a national portal that will allow fast, easy access to public and private services. The Department of Science and Technology's Information and Communications Technology Office runs the annual Information Technology Business Process Management Summit. The department is working on the Technology for Economic Development program, which aims to alleviate poverty through teaching digital literacy and skills training. The Philippines also has a focus on increasing entrepreneurship through tech start-ups. In August 2017, the Expanded Anti-Red Tape Act was approved by the Philippines Senate in an attempt to make doing digital business in the Philippines easier. In July, the Philippines also introduced a new cloud-based system for administering business licences. DICT continues to engage competently with industry, and in 2017 organised the CyberSecurity Summit 2017 with Kaspersky Lab, a Russian cybersecurity and anti-virus provider.

SCORE: 4

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The Philippines continues to be at the forefront of internet usage not only in Asia but globally. It has the 5th highest social media penetration in Asia. According to Freedom House, internet speeds in the Philippines continue to be slow, but a free Wi-Fi program being rolled out by the government should help to combat this problem. The Philippines was labelled as a breakout country in the 2017 Digital Evolution Index, which means that, although it has a relatively modest digital economy, it has great potential. The potential stems from the fact that Filipinos are generally keen internet users who are competent English speakers, which creates opportunities for outsourcing. Filipino ISP PLDT runs an outreach program aimed at increasing digital literacy among youth to boost the digital economy in the Philippines. DICT's National Broadband Plan will help grow the digital economy further, but it would be advisable for the government to create its own plan specifically for the digital economy.

SCORE: 5

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

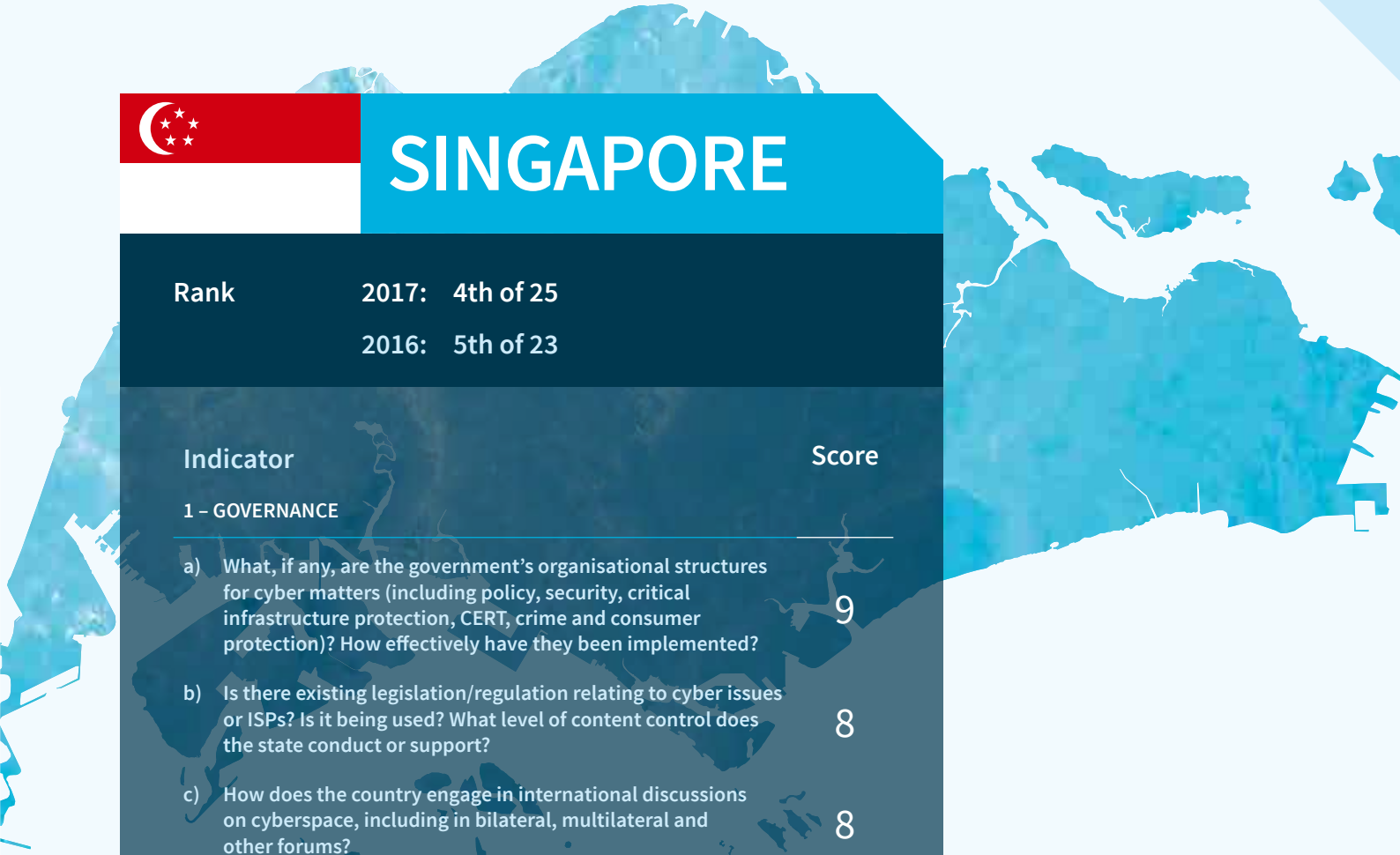
The Philippines continues to display evidence of public awareness of cyber issues. The Office of Cybercrime's annual public report contains valuable information about cyber trends, cooperation and programs. In April 2017, DICT began a 'cybersecurity caravan' campaign, in which cyber experts are sent into the community to teach high-school and college students about cybersafety. DICT is also encouraging cybersecurity education in schools and hopes to increase the number of people trained for top cybersecurity jobs to address the current deficit in this area. The Foreign Service Institute of the Philippines produced a report as a part of a February volume for the Center for International Relations and Strategic Studies about cyberspace vulnerability, and cyber issues have continued to receive a moderate amount of coverage in the press. AlamBau, a Filipino website, provides advice for children, teenagers, parents and teachers on cybersafety. The Philippines also hosted the ComputerWorld Security Summit 2017. Cyber awareness in the Philippines is tied up with issues relating to freedom of expression, fake news, data speeds and e-literacy.

SCORE: 6

b) What percentage of individuals use the internet?

As in many countries in the region, broadband internet access is increasingly provided by mobile connections, and significant increases in mobile connectivity are observable from year to year. There are 5.5 fixed-line broadband subscriptions and 46 mobile broadband subscribers per 100 inhabitants, and 47.8% of Filipinos use the internet.

SCORE: 5



SINGAPORE

Rank 2017: 4th of 25

2016: 5th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	9
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	8
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	7
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	8
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	9
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	10
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	10
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	10
b) What percentage of individuals use the internet?	9

OVERALL ASSESSMENT

Singapore has one of the most highly developed cybersecurity environments in the region. The Cyber Security Agency of Singapore functions as a central hub for cybersecurity governance and will be granted increased powers to protect critical information infrastructure in a draft bill currently under consideration. Singapore's international engagement is extended through ASEAN and bilaterally, and industry–government dialogue is a cornerstone of policy development.

WEIGHTED SCORE 87.7

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

The centre of Singapore's organisational structure for cyber matters is the Cyber Security Agency of Singapore (CSA), which is within the Ministry of Communications and Information. The CSA is an oversight body that promotes the holistic development of Singapore's cybersecurity and functions as a central hub. Singapore's regulatory capacity in cybersecurity is under the purview of the Infocomm Media Development Authority, which, with its Personal Data Protection Commission, is a statutory board in the Singaporean Government that advises on ICT regulation. In addition to the current structures, a draft cybersecurity bill, currently under consideration, will create the position of Commissioner of Cyber Security as a central figure in Singaporean cybersecurity. The roles of the position include informing the government on cyber threats, creating codes of practice and designating critical information infrastructure.

SCORE: 9

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Singapore has comprehensive legislation relating to cyber issues. The key piece of legislation is the Computer Misuse and Cybersecurity Act, which was enacted in 1993 and revised in 2007. In 2017, the Act was amended to expand the activities that it prohibits. Singapore's action on cybersecurity is guided by the Cybersecurity Strategy and its four pillars: strengthen the resilience of critical information infrastructure, empower business and society, develop a vibrant cybersecurity ecosystem and strengthen international partnerships. To combat cybercrime specifically, Singapore developed the National Cybercrime Action Plan. The Singaporean Government has also released a draft Cybersecurity Bill for public comment. The bill is designed to regulate critical information infrastructure designated as such by the Commissioner of Cyber Security, increase CSA powers to manage and respond to threats, establish an information-sharing framework on cybersecurity, and introduce licensing regulation for cybersecurity providers.

SCORE: 8

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

One of the priorities of Singapore's Cybersecurity Strategy is building 'strong international partnerships', and in the past year Singapore has been very active in this area. Bilaterally, it has signed a raft of MoUs and joint declarations of interest. The Minister for Communications and Information has also travelled broadly to engage on cybersecurity, meeting with regional governments and governments further abroad. Singapore is an active member of ASEAN's cyber initiatives and in September held the second Singapore International Cyber Week.

SCORE: 8

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Singapore's national CERT, SingCERT, is highly developed and capable. The CERT was established in 1997 and has since been moved to the CSA. Singapore's telecommunication companies, Singtel and Starhub, have also set up helplines to provide the public with better access to cybersecurity assistance.

SCORE: 7

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

In 2017, Singapore released the National Cybercrime Action Plan and accompanying legislation to address cybercrime. The Technology Crime Unit, which is within the Financial and Technology Crime Division under the purview of the Attorney-General, specialises in cyber- and technology-related crime and develops and reviews cybercrime policies. The Financial Technology and Innovation Group also contributes to the Singaporean cybersecurity ecosystem by providing financial support and 'regulatory sandboxes'. Singapore hosts Interpol's cybercrime unit and engages internationally on cybercrime bilaterally and through ASEAN.

SCORE: 8

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

The role of the Singaporean military in cyberspace is highly developed. The Defence Science and Technology Agency is responsible for advising the Ministry of Defence on defence science and technology matters and developing infrastructure and systems for cyber defence. Singapore also has the C4 Operations Group, which consists of 700 regular and national service personnel who monitor and protect the Singapore Armed Forces' cyber ecosystem. Singapore has announced that a new body, the Defence Cyber Organisation, will be created to function as a central cyber hub within the Ministry of Defence and oversee the ministry's cyber policies. A new central command for cyber operations will also be created. C4 Cyber Defence Operations will consist of 1,300 service personnel. Singapore's military is also active in promoting cybersecurity awareness and skills and runs several programs to encourage budding cyber defenders.

SCORE: 9

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

There's significant and high-quality dialogue between the Singaporean Government and industry on cyber issues. Singapore's cybersecurity legislation and guidelines take industry into account and are crafted through consultation. The National Cyber Security Masterplan 2018, which guides the country's cyber policy, was written after extensive consultation with industry to ensure a holistic approach. Similarly, the National Cybercrime Action Plan highlights the role that industry plays in national cybersecurity, recognising the engagement between industry and police and prescribing further engagement between government and industry to raise both awareness and capability. Singapore's National Security Conference, organised by the Singapore Business Federation and supported by the CSA, is a key forum through which this dialogue is facilitated.

SCORE: 10

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The digital economy is an integral part of Singapore's economic activity. The government has implemented various policies over the years to ensure Singapore's place as a world leader in the digital economy. Singapore also intends to prioritise e-commerce and the digital economy in the region when it takes over as the chair of ASEAN in 2018. The Future Economy Council brings together government and industry and has identified seven strategies to ensure that Singapore remains at the forefront of the international digital economy.

SCORE: 10

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

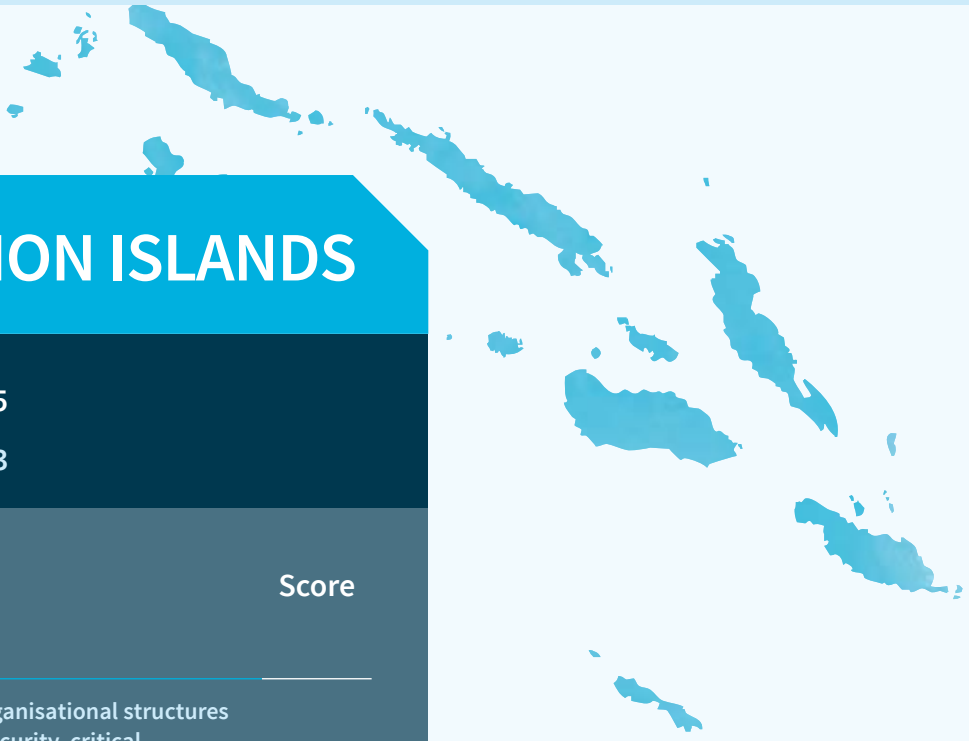
Singapore has taken significant steps to heighten public awareness of cyber issues. This year, it launched *Live Savvy with Cybersecurity*, its first cybersecurity public awareness campaign. There are also products aimed at fostering awareness among young Singaporeans, such as the *Cyber safety activity book*. Singapore conducted its first cybersecurity public awareness survey, which showed that 70% of Singaporeans agreed that everyone had a role to play in cybersecurity and that 67% were interested in learning more about cybersecurity.

SCORE: 10

b) What percentage of individuals use the internet?

Some 85% of Singaporeans use the internet, and Singapore has very high levels of fixed-line and mobile broadband usage.

SCORE: 9



SOLOMON ISLANDS

Rank 2017: 25th of 25

2016: 23rd of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	0
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	1
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	0
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	1
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of individuals use the internet?	2

OVERALL ASSESSMENT

Solomon Islands' cyber maturity is nascent. It has low connectivity and there's little awareness of cyber issues. The basic cyber governance structures of Solomon Islands are geared towards improving infrastructure and connectivity. Those goals have been dealt a blow by problems in the installation of a submarine fibre-optic cable. However, statements from the Royal Solomon Islands Police Force (RSIPF) show a developing awareness of potential cyber threats.

WEIGHTED SCORE 13.8

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Cyber matters in Solomon Islands are the responsibility of the Ministry of Communication and Aviation, which develops and coordinates the country's cyber policies. Solomon Islands' cyber structures focus on two main areas: infrastructure and ICT industry liberalisation. ICT infrastructure development is addressed by the National Development Strategy (2016–2035) and the National Infrastructure Investment Plan. Industry liberalisation is the remit of the Telecommunications Commission of Solomon Islands. The integrity of the country's cyber governance has been called into question by a recent political donations scandal involving proposals to install a submarine fibre-optic cable.

SCORE: 3

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Solomon Islands has no specific legislation on cybercrime, electronic transactions, or data security and privacy. The Telecommunications Act of 2009 opened the ICT market to competition and established the Telecommunications Commission as its regulator. There's some intent to develop cybercrime legislation, and the RSIPF has announced that cybercrime will be a focus of its efforts.

SCORE: 0

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Solomon Islands engages with several multilateral regional forums and initiatives on cyber issues, including Cyber Safety Pasifika, APNIC, Pacific ICT ministerial meetings and the Melanesian Spearhead Group. Bilaterally, it engages with Australia and has recently signed an MoU with Indonesia that includes cybercrime cooperation. Solomon Islands' international engagement has been significantly damaged by the fallout from the submarine cable deal. The Asian Development Bank, which was funding the deal, and Australia, the country to which the cable would connect, have expressed concerns about corruption in the bidding and the potential negative cybersecurity impacts of the cable.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Solomon Islands was a member of the Pacific islands' PacCERT, which has ceased operation due to lack of funding.

SCORE: 0

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The RSIPF doesn't have a dedicated cybercrime unit. However, it has shown increasing awareness of the threat of cybercrime, and 22 RSIPF members have participated in a five-week training course on cybersecurity. The RSIPF's participation in initiatives such as Cyber Safety Pasifika and statements at the Pacific Chiefs of Police Conference also attest to the force's push to engage internationally on these issues.

SCORE: 1

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Solomon Islands does not have an official military force.

SCORE: 0

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

There's evidence of dialogue between government and industry on cyber issues in Solomon Islands; however, given the nascent state of the nation's ICT industry, the dialogue is very limited and appears to be focused mainly on improving ICT infrastructure and connectivity. The government's National Infrastructure Investment Plan, which was developed in consultation with industry, stresses the need for open competition and industry cooperation in expanding ICT connectivity.

SCORE: 2

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The digital economy isn't a significant part of economic activity in Solomon Islands, where the economy is based on agriculture, fishing and forestry. However, in the past year, the Solomon Islands Central Bank has taken steps to digitise financial services. As part of the National Financial Inclusion Strategy 2016–2020, the Solomon Islands Government joined the Better Than Cash Alliance and has committed to digitising 80% of its payments by 2020.

SCORE: 1

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Media coverage of Solomon Islands cyber issues has increased significantly with the scandal concerning the new cable. The coverage is mainly external, but there's also some local media reporting. Despite this, public awareness of and debate about cyber issues is still extremely limited and centred almost entirely on increasing connectivity and improving infrastructure.

SCORE: 2

b) What percentage of individuals use the internet?

Only 11% of Solomon Islanders use the internet. Mobile and fixed-line broadband penetration is very low, despite reasonable mobile phone penetration.

SCORE: 2

SOUTH KOREA

Rank 2017: 5th of 25

2016: 2nd of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	8
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	9
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	8
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	8
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	8
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	9
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	9
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	9
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of individuals use the internet?	10

OVERALL ASSESSMENT

South Korea's governance approach to cyberspace continues to be highly organised and heavily regulated. The military remains focused on cybersecurity in the light of continuing tensions with North Korea and has doubled down on efforts to boost its cyber capability through youth recruitment. However, South Korea is also very aware of the benefits of connectivity and runs strong government initiatives to support the digital economy and seek private-sector consultation. In addition to krCERT's ongoing public awareness efforts, there's been a rise in public discussion of cyber issues in relation to the controversial surveillance powers of the new Anti-Terrorism Act. South Korea has also taken a greater leadership role on international issues, establishing new regional bodies for multilateral cooperation.

WEIGHTED SCORE 86.8

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

South Korea has maintained strong governance structures and a centralised approach to cyber issues. The National Security Office continues to oversee the country's cybersecurity governance as a control tower, while incident management and response are conducted by the National Cyber Security Center within the National Intelligence Service. The Ministry of Science, ICT and Future Planning's Korea Internet and Security Agency (KISA) provides public-facing warnings and alerts, as well as promoting cyber-centred innovation. The Ministry of Foreign Affairs and the National Police Agency also host their own cyber work areas, and South Korea has several commissions dedicated to regulating internet media and content. Government policy remains informed by the 2011 National Cyber Security Masterplan, and an update to that plan could increase South Korea's score for this indicator. A discussed further centralisation under the National Cyber Security Center could also prove beneficial.

SCORE: 8

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

South Korea has taken steps this year to update an already impressive cyber legislative framework. Regulations to protect personal data have been published in the form of *Guidelines for de-identification of personal data* (2016) and *Amended guidelines on financial sector personal information protection* (2017), and there's ongoing enforcement of the Personal Information Protection Act 2011 and the Act on the Promotion of Information and Communications Network Utilisation and Information Protection 2016 after their entrance into force last year. These substantive additions to South Korea's already well-regulated cyber landscape have provided important protections for personal data at a critical time. The sustained focus on cyber issues, the expansion of legislation and strong implementation mean South Korea's score for this indicator remains consistently high.

SCORE: 9

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

South Korea has continued to engage in a diverse array of international cyber forums. Its international cyber diplomacy efforts are well organised under its Coordinator for Counter Terrorism and Cyber Security and its Ambassador for International Security Affairs. South Korea has concluded agreements or continued mature bilateral dialogue with the US, China, India, Indonesia, Japan, Kenya, Malaysia, Gabon, Kazakhstan, Senegal and Tanzania. It has begun engaging bilaterally and multilaterally outside the Asia–Pacific region, particularly in Central Asia. South Korea's Ministry of Defense stated that it would establish a complementary multilateral defence mechanism to assist in building cyber partnerships, and the Ministry of Foreign Affairs is exploring ways to cooperate with the North Atlantic Treaty Organization in exercises and other cyber affairs. Trilaterals between South Korea, China and Japan remain prominent, as does engagement with APEC and ASEAN. South Korea's score remains steady this year, although its increasing regional and extra-regional engagement and leadership could result in an improved score next year.

SCORE: 8

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

South Korea maintained its sophisticated CERT capability during the year. KNCERT continues to oversee the security of government networks. KrCERT, under KISA, provides incident response for the private sector and is a member of APCERT. KrCERT noticeably up-scaled its threat monitoring activities this year and actively crawled and monitored more than 3.4 million domestic websites. KrCERT also engaged 24 other CERTs in a mutual exchange and training program and hosted the 28th FIRST Annual Conference in June. KrCERT continued to engage actively as a member of APCERT and in even more global CERT activities, such as the CERT Romania Annual Conference. Further development in international cooperation and leadership by South Korean CERTs would improve South Korea's score.

SCORE: 8

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

South Korea continues to address cybercrime through the Cyber Bureau of the National Police Agency, which hosts a number of response capabilities in safety, cybercrime response and digital forensics. The Supreme Prosecutor's Office hosts its own Cyber Crime Investigation Division, which has a capacity to conduct technical analysis for its cybercrime prosecutions. South Korea secured an agreement with Microsoft to receive and assess source code for Microsoft's major products to better evaluate existing computer systems and to improve overall security. However, the country remains vulnerable to financial cybercrime. South Korean banks continue to be targeted, and South Korean cryptocurrency companies were actively targeted by cybercriminals in the past year, resulting in record losses of cryptocurrency. South Korea has also engaged internationally on financial cybercrime laws. Its pursuit of novel arrangements in cybercrime and ongoing response to novel financial cybercrime threats have increased its score for this year.

SCORE: 8

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

South Korea's military has continued to be active on cybersecurity issues in response to the high-profile threat of North Korean cyber operations. South Korea has reportedly increased cyberwarfare staffing by an additional 1,000 personnel as part of a wider bolstering in the capability of rear-area operation units, adding to an already 6,000-strong complement of dedicated cyberwarfare personnel. A revised mid-term defence plan reserves US$218 million specifically for countering North Korean cyber threats as part of a wider funding plan to counter growing nuclear, ballistic missile, cyber and long-range artillery threats. South Korea's Ministry of Defense Cyber Command is the key point of coordination for military actions on cyber issues. The command has noted a noticeable uptick in the number of attacks from North Korea over the past year and was compromised in late 2016 (the compromise was later attributed to North Korea). The military continues to play a significant and clearly defined role in cyberspace, but the focus remains narrowly defined as defence against the North Korean threat.

SCORE: 9

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

There's strong two-way dialogue between the government and the private sector in South Korea. The Future Wealth Business Plan 2016 continues to provide guidance for public–private dialogue and interaction. K-Startup continues to host Grand Challenges in South Korea, with participation from a global pool of start-up teams. The Ministry of Science, ICT and Future Planning partnered with Facebook to deliver the Korea Business Hub Center. South Korea's regional government organisations have been cultivating start-ups in regional areas, and its innovation-dedicated NGOs sent representations to innovation hubs in the US. A major inaugural Ministerial Meeting on the Economy in 2017 set ambitious targets for government support to start-ups and start-up growth. A novel Asia–Pacific Internet Governance Academy was set up in August 2016 to improve participants' understanding of internet governance and the multistakeholder processes involved.

SCORE: 9

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

South Korea continues to be one of the region's and the world's most flourishing digital economies. KISA has established a service to support start-ups domestically and globally to improve private-sector inputs into national cybersecurity. The agency also promotes better security practice through the National Biometric Test Center. A partnership with Facebook for a business hub, annual Grand Challenges and other recruitment, incubation and accelerator programs for start-ups provide further evidence of commitment to this initiative. A number of skills-building initiatives on the more government-focused side of cybersecurity, including a reserve force, an enhanced cyber defence curriculum, explicit ethical hacking training courses and governance training, are likely to provide a useful skills base for further digital economic development.

SCORE: 9

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

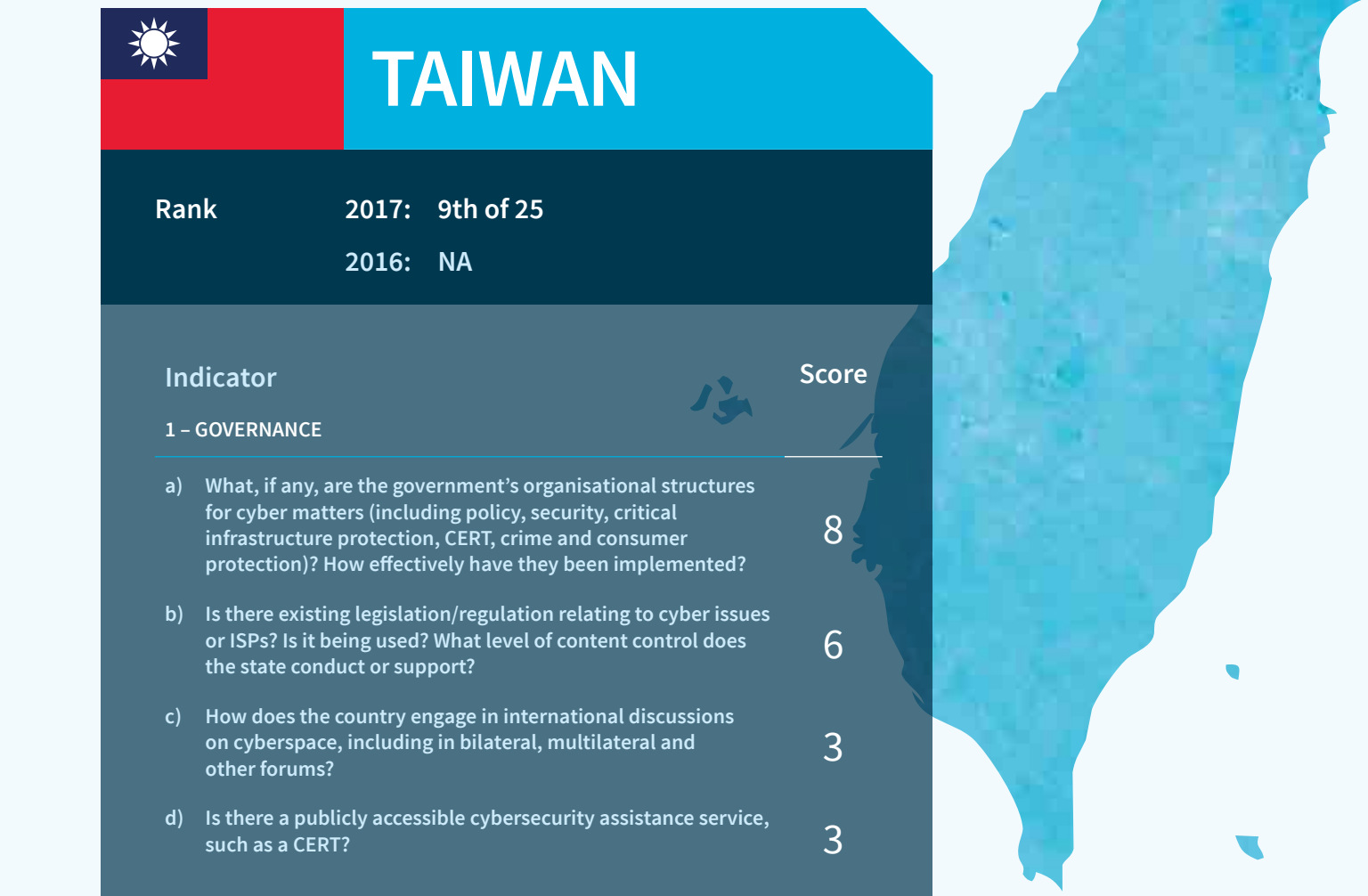
KISA is responsible for public awareness on cyber issues. Its work is complemented by KrCERT's active contribution to public awareness on specific cybersecurity threats. The National Information Society Agency issues e-newsletters and a yearbook of statistics to assess the level of cybersecurity awareness among the general public. Cybersecurity issues are the subject of extensive media coverage. Legislation on cyber issues is a lightning rod for public commentary, as government and, in particular, national intelligence agencies in South Korea are the subject of notable distrust when it comes to surveillance and censorship, which could prove to be an obstruction to effective public–private cooperation on cybersecurity. Public exposure to technology remains high, particularly among South Korean youth.

SCORE: 9

b) What percentage of individuals use the internet?

South Korea has one of the world's most active telecommunications markets, and 93% of the population uses the internet. Fixed-line and mobile broadband penetration are very high.

SCORE: 10



TAIWAN

Rank 2017: 9th of 25

2016: NA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	8
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	3
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	5
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	5
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	6
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	6
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of individuals use the internet?	9

OVERALL ASSESSMENT

The self-governed democracy of Taiwan is viewed by China as a renegade province; as such, it's long been an important testing ground for Chinese cyber capabilities. The country frequently tops the global list of nations most often attacked in cybersecurity incidents. Since coming to office in May 2016, President Tsai Ing-wen has elevated cybersecurity as a priority for Taiwan, saying on numerous occasions that 'cybersecurity is national security'. Taiwan plans to create a 'Cyber Army' as the fourth branch of its armed forces in what looks likely to be a world first. In 2016, the Executive Yuan—the executive branch of the central government—established the Department of Cybersecurity in conjunction with the Ministry of Science and Technology.

WEIGHTED SCORE 56.9

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Taiwan has strong organisational structures within government for dealing with cyber matters. Its National Information and Communication Security Taskforce was established as early as 2001. In 2016, the Executive Yuan established the Department of Cyber Security in conjunction with the Ministry of Science and Technology. There are now eight major working groups for cybersecurity-related task execution and coordination among agencies. The country's National Center for Cyber Security Technology plays the role of its national CSIRT. In June, Taiwan established the Information and Electronic Warfare Command. President Tsai Ing-wen has reiterated on many occasions that 'cybersecurity is national security'. The Information Security Office, started in August 2016, is tasked with coordinating with other government departments on cybersecurity issues.

SCORE: 8

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Since assuming office in May 2016, President Tsai Ing-wen has elevated cybersecurity as a priority for Taiwan. In August 2016, the Department of Cyber Security and the Information Security Office were established to improve the country's cyber defence capabilities. A national information security improvement project is slated to run from 2017 to 2020 to further bolster Taiwan's ability to deal with attacks on national communications networks. A Cybersecurity Bill, aimed at guarding key infrastructure, protecting sensitive information and countering network attacks, was approved by the Executive Yuan and submitted to the Legislative Yuan for approval in April.

SCORE: 6

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Taiwan's ability to engage in international discussions on cyberspace is constrained by its diplomatic isolation. It has found it difficult to gain membership in any international CERT alliances due to pressure from Beijing. Despite these constraints, Taiwan and the US signed a statement of intent agreeing to strengthen cybersecurity cooperation between the two countries in May 2016. Taiwan held the 7th Asia–Pacific Regional Internet Governance Forum in 2016.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

The country has the Taiwan National CERT, TWNCERT, which has a coordination centre. TWNCERT aims to create a government response centre that can help optimise the capability to monitor, coordinate, respond to and handle security incidents. TWNCERT has been a steering committee member of APCERT and played host to its Training Working Group from 2014 to 2017.

SCORE: 3

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The Cybercrime Investigative System is one of two major parts of the National Information and Communication Security Taskforce (the other being the Cyberspace Protection System). In December 2016, the Taipei Police Department opened its High Technology Crime Investigation Unit in response to a rise in crimes involving the use of advanced technology. Following a series of cyberattacks on a number of Taiwan's brokerages in early 2017, the Financial Supervisory Commission announced that it would establish a financial information sharing and analysis centre to provide timely threat bulletins and 'counterattack resources'. Taiwan's ability to deal with its own nationals who have been caught for cybercrime offences overseas has been hampered by interference from mainland China.

SCORE: 5

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

In June 2017, President Tsai Ing-wen officially inaugurated the country's new Information and Electronic Warfare Command. The new command is meant to integrate and coordinate information and electronic warfare units that already exist throughout the armed forces. It reports directly to the Ministry of National Defense's General Staff Headquarters, is commanded by a major general and has around 2,400 staff. The Defence Ministry plans to use financial bonuses as an incentive to attract cybersecurity experts from the private sector in 2018. The ruling Democratic Progressive Party is pushing for the establishment of a cyberwarfare branch in the armed forces.

SCORE: 5

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

The Department of Cyber Security has drafted the Cyber Security Management Act, which will compel not just government agencies but also certain private companies to comply with cybersecurity baselines. Certain companies in critical infrastructure areas (including energy; water; information and telecommunications; transportation; banking and finance; emergency services and public healthcare; central government; and hi-tech industrial parks) will be held responsible for cyber breaches.

SCORE: 6

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Taiwan launched its Digital Nation and Innovative Economic Development Plan, known as 'DIGI+', in November 2016. The main goal of the DIGI+ plan is to grow the country's digital economy to NT$6.5 trillion (US$216 billion) by 2025. The government also hopes that the plans will help increase internet bandwidth, expand broadband internet accessibility and make the country more competitive in the global information sector. The plan will focus on kickstarting an 'Asian Silicon Valley' by establishing 100 start-ups over the course of seven years in Taoyuan.

SCORE: 6

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

This year, the WannaCry global ransomware events affected Taiwanese schools, power companies and other segments of civil society, garnering broad mainstream media coverage. Progress on broad-based education and training is increasing, with a particular focus on combating 'fake news'. Faced with an onslaught of disinformation, Taiwan is also rolling out a new school curriculum to teach children how to identify and combat false news. A 35-year-old computer prodigy, Audrey Tang, was appointed Minister Without Portfolio by the Taiwanese Government to directly involve the public in policymaking and to counter disinformation. Public dialogue on cyber issues continues to focus on the risk of cyberattacks from mainland China.

SCORE: 6

b) What percentage of individuals use the internet?

Taiwan has a dynamic and well-developed telecommunications market. Some 73.4% of the population uses smartphones. Taiwan's internet penetration reached 83% in 2016.[2]

SCORE: 9

2 As ITU data is not available for Taiwan, this data was from 'Asia—fixed broadband market: statistics and analysis, *Budde.Comm*, January 2017, online.

THAILAND

Rank 2017: 13th of 25

2016: 9th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	7
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	5
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	5
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	5
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	5
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	4
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	6
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of individuals use the internet?	5

OVERALL ASSESSMENT

Thailand produced consistent cyber maturity results in 2016–17. The biggest change has been the introduction of the Ministry of Digital Economy and Society (MDES) to replace the Ministry of Information and Communication Technology. This year, there have also been discussions on establishing a National Cybersecurity Committee, which would operate under the Prime Minister, separately from the MDES. Once again, Thailand has primarily focused its cybersecurity efforts on enforcing censorship and *lèse majesté* laws, as evidenced by changes to the Computer Crime Act. While Thailand has made some improvements to its domestic structures, its international engagement has remained static. The digital economy is a major focus for Thailand, and the government has unveiled a 20-year four-part digital economy plan.

WEIGHTED SCORE 54.0

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Thailand's organisational structures for cyber matters have changed significantly in the past 18 months. The MDES replaced the Ministry of Information and Communication Technology in September 2016. The departments and organisations that now report to the MDES include the Meteorological Department, the National Statistical Office, the Telephone Organization of Thailand, the Communications Authority of Thailand, the Electronic Government Agency, the Electronic Transactions Development Agency and the Digital Economy Promotion Agency. A proposal to introduce a National Cybersecurity Committee was made in May 2017, and the establishment of the committee was officially published in October. Amendments to the 2017 draft Cybersecurity Bill will mean that the proposed committee reports directly to the Prime Minister and not the MDES.

SCORE: 7

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

The Thai government has finalised the National Cybersecurity Strategy (2017–2021), which will soon be submitted to the Cabinet for approval. In late 2016, the 2007 Computer Crime Act was amended, and many claim that the changes increase censorship and are too restrictive of free speech. Thailand has very strict *lèse majesté* laws, and has arrested and prosecuted citizens who post content online that shames the King or other leaders. A new draft Cybersecurity Bill was opened to public consultation between 24 May and 7 June 2017. Once any changes have been made, the bill will become another one of many digital economy bills that are currently awaiting approval from the National Legislative Assembly. Thailand's cybersecurity laws are often focused on censorship. This is evidenced by the fact that the cybercrime division within the police force lists its number one mission as protecting the King, Queen and royal family.

SCORE: 6

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Thailand has continued to engage in ASEAN- and APCERT-related cyber dialogues. However, much of the focus on cybersecurity in the past 12 months has been domestic, and the transition from the Ministry of Information and Communication Technology to the MDES has taken considerable time and resources. The Thai government hosted a Regional Workshop on Cybersecurity with ASEAN and non-ASEAN members. Thailand also hosted an ASEAN cybersecurity workshop in June 2017, but more international dialogue with non-ASEAN members is needed to improve its score in this category.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

ThaiCERT is Thailand's national CERT, operating under the MDES. There was a decrease in the number of incidents handled by ThaiCERT between 2015 and 2016, and fraud, intrusions, intrusion attempts and malicious code were the most common types of incidents recorded. ThaiCERT engages with other Asian CERTs for training and produces publications and alerts to help citizens safeguard themselves against cyberattacks. To improve in this category, ThaiCERT needs to increase its international cooperation and engagement.

SCORE: 5

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Thailand's cybercrime unit is the Technology Crime Suppression Division of the Royal Thai Police. The division enforces the computer crime law and has a hotline that can be called to report inappropriate online content. The division reportedly spent 28 million baht (US$860,000) on a computer system that helps enforce *lèse majesté* laws. In order to improve in this category, the Technology Crime Suppression Division needs to broaden its cybersecurity objectives and increase its international engagement. There's no recently published information that suggests the division is enforcing financial cybercrime laws.

SCORE: 5

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

In 2015, it was announced that the Royal Thai Armed Forces would establish a cybersecurity unit. While some have since criticised the unit for focusing too much on *lèse majesté* laws, Thailand's army commander has insisted that it's also equipped to tackle national security and hacking. Since the 2014 coup, which saw the current Thai military government gain control, multiple people have been arrested and charged for breaking the *lèse majesté* laws by posting offensive material online, including one man who received a 35-year jail sentence for defaming the King on Facebook. To improve in this category, the Thai military needs to show greater international involvement on cybersecurity and a broader focus.

SCORE: 5

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

In October 2016, Microsoft announced a Government Security Program agreement with Thailand's Electronic Transactions Development Agency. The program has been running since 2003, aiming to help government and organisations better protect citizens against cyberattacks. In early 2017, Dr Pichet Durongkaveroj from the MDES announced that the government was planning to build a digital park to unite government, industry and academia. The Asia Internet Coalition, an industry body, provided regular feedback to the Thai Government and has been particularly vocal regarding the Computer Crime Act.

SCORE: 4

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The digital economy is a significant focus for the government of Thailand. The MDES has appointed a committee to focus on a 20-year digital economy plan and has initiated a Smart City program in Phuket. The department has a clear vision and strategy for how it will implement its digital economy goals, which include improving the telecommunications network, increasing knowledge about digital technology and regulating digital laws. Despite these steps, Thailand still faces significant challenges and was labelled as a 'watch out' country in the 2017 Digital Evolution Index. If Thailand can continue to create policy that supports and prioritises the digital economy, it will improve in this category.

SCORE: 6

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

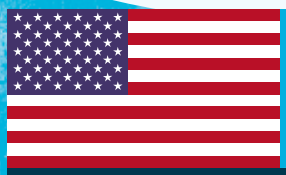
In September 2017, the MDES held Digital Thailand Big Bang, a tech exhibition that featured a variety of different stakeholders, with the goal of driving digital advancement. Much of the cyber debate is still centred on censorship and the challenges associated with it. Thai think tanks have provided little information about cybersecurity in the past year, leaving most of the work to the MDES. There was some public debate about the effectiveness of the Cybersecurity Bill. The Executive Director of the IMC Institute, Dr Thanachart Numnonda, stated in May 2017 that Thailand doesn't have enough workers with cybersecurity skills, and that the population as a whole has a general lack of cybersecurity awareness.

SCORE: 6

b) What percentage of individuals use the internet?

Thailand has a saturated mobile broadband market. Mobile broadband has grown strongly to 95 subscriptions per 100 inhabitants. Fixed-line broadband has also grown over recent years to 11 subscriptions per 100 people. Despite this, just under half (47.5%) of Thai citizens use the internet.

SCORE: 5



UNITED STATES OF AMERICA

Rank 2017: 1st of 25

2016: 1st of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	10
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	8
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	10
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	10
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	9
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	9
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	10
b) What percentage of individuals use the internet?	8

OVERALL ASSESSMENT

The US has retained its leading cyber maturity position in the Asia–Pacific and globally in 2017. However, a significant Russian hacking and information operation campaign to influence the 2016 presidential election remains an ongoing source of division within the government and among the US public. The surprise election victory of President Donald Trump resulted in a review of cyber policy development and a pause in implementation early in the year, but since then there have been no major shifts in direction and only modest changes in priorities. However, the proposed 2018 federal budget comes with little new money for cyber expenditures, and there have been few significant moves in cyber legislation in Congress. In addition, most recommendations from the Obama administration's Commission on Enhancing National Cybersecurity haven't been adopted. The military continued to invest significantly in cyberspace capabilities and announced that it will elevate US Cyber Command to a unified combatant command and give it increased independence on training and capability acquisition. US financial cybercrime units have continued to lead the world and are slated to add new capabilities to tackle new kinds of cybercrime.

WEIGHTED SCORE 90.8

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

The US Government's governance of cyber issues has remained largely consistent between the former Obama administration and current Trump administration. The Obama administration published a major report from the Commission on Enhancing National Cybersecurity. However, most of the report's recommendations weren't adopted by the succeeding administration. More importantly, the Obama administration's organisational framework and response reportedly failed to respond effectively to Russian cyberattacks and information operations during the 2016 presidential election. Problems with interagency collaboration and consensus-building, a fear of escalation and difficulties in the decision-making process have been identified as shortcomings in the Obama administration's response to the hacks. The new Trump administration hasn't addressed those obstacles, or the extent of the role of Russia, although investigations and inquiries are ongoing. After some delay, the Trump administration issued the 'Strengthening US Cyber Security and Capabilities' executive order, which remained largely consistent with initiatives from the previous administration. For example, the order calls for similar 60-day and 100-day assessments of the state of US cybersecurity. The order also continues Obama-era practices of encouraging streamlined IT procurement by directing agencies to procure shared IT solutions where possible. The order has been criticised for failing to consult or coordinate with the affected federal departments and agencies. Reporting has suggested that there are ongoing problems with personnel shortages throughout the US cybersecurity policymaking structure. Lastly, a slated federal budget for 2018, while not finalised at the time of writing, does not include a top-line figure for cybersecurity expenditures comparable to the $19 billion figure from the 2017 federal budget, and current submissions indicate that cybersecurity spending will remain at parity with 2016 or be cut.

SCORE: 10

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Significant legislative activity in the US on cyber-related issues has continued. This year's legislation is largely focused on administrative matters, such as providing for law enforcement and security agencies' cyber capabilities, rather than legislating on the more divisive issues of encryption and privacy that dominated last year. Most legislative activity has taken the form of provisions or amendments attached to the National Defense Authorization Act for Fiscal Year 2018 and the 2018 federal budget. A notable exception, the Active Defense Certainty Act, which would allow cybercrime victims to 'hack back' their attackers to determine attribution or delete stolen data, was introduced to Congress in October. Bills to regulate the cybersecurity of the IoT, internet-connected children's toys and other areas have also been introduced, but they have yet to be passed into law. Given that most bills don't become law, the full impact of this year's legislative developments isn't yet clear. Concerns have been raised that national security decisions by the new administration damage the privacy of EU citizens. A recent review of the EU–US Privacy Shield agreement was satisfied with the arrangement, but sought improvements. The debate about cyber-related issues in legislation indicates a good awareness of cyber matters among US legislators.

SCORE: 8

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

The US has continued to promote an open, interoperable, secure and reliable internet with a collaborative multistakeholder governance model. However, the United Nations Group of Governmental Experts on Information Security (UNGGE) failed to deliver a report codifying international norms on cyberspace after some participating states objected to the application of humanitarian law and the use of force in cyberspace. The Department of State's Office of the Coordinator for Cyber Issues will be consolidated into the Bureau of Economic and Business Affairs in a move that is seen as downgrading the importance and influence of cyber issues within the State Department. US relations with Russia have become hotly contested, and an intelligence community assessment has stated that Russia played an active role in influence operations to sway the 2016 presidential election. This assessment has been rejected by the current administration, although separate and independent investigations are ongoing. The US has signed a landmark MoU with India on cyber cooperation, the first US–Ukraine Cybersecurity Dialogue was held in September, and a US–China Law Enforcement and Cybersecurity Dialogue was held in October. Cyber affairs have continued to permeate strategic dialogues with Thailand, South Korea, Japan and Australia. In his cybersecurity executive order, President Trump asked for an international cybersecurity engagement strategy, but the September deadline date has since passed with no strategy in sight. While US leadership on international cyber policy issues is strong, a defined strategy that recognises the importance of cyber issues across the sweep of policy areas, from national security and the economy to human rights and counterterrorism, would be welcome, as would a greater presence and visibility of US capacity-building efforts in the Asia–Pacific.

SCORE: 9

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

The Department of Homeland Security's National Cybersecurity and Communications Integration Center continues to house both US CERT and the Industrial Control System CERT (ICS-CERT). US CERT provides a range of information to public- and private-sector organisations to manage cyber threats via vulnerability bulletins, alerts and tips as part of a wider National Cyber Awareness System. ICS-CERT has been active in more hands-on threat assessments and reporting on 130 organisational cybersecurity assessments in critical infrastructure sectors, 290 incident responses, and in-depth technical analysis of 100 malware samples. US CERT collaborates extensively with the CIO Forum, the Government Forum of Incident Response and Security Teams, the National Council of Information Sharing Analysis Centers (a coordinating body to share information between government and private-sector critical infrastructure bodies), and the Software Assurance Community Resources and Information Clearinghouse. The two CERTs are complemented by a third and separate element, Cyber Force Management, which handles human resources and other support functions for them. The US has a well-developed CERT community with strong response capabilities, but could improve its score for this category with further evidence of international engagement and capacity building in the CERT sector.

SCORE: 8

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The US remains an international leader in the pursuit and prosecution of financial cybercriminals. According to preliminary budget submissions, the FBI will be spending less on cyber capabilities: it will request US$41.5 million in 2018, down from US$85.1 million in 2017. The general program enhancement budget has undergone steep cuts, falling from US$873.8 million to US$117.6 million. The cuts affect a wide variety of operational capabilities, from counterintelligence, operational technology and combating organised crime to other taskforces that could prove cyber-relevant. General cyber R&D funding has undergone cuts, and a US Secret Service digital forensics training centre for state and local police has been slashed entirely. The FBI Internet Crime Complaint Center has reported that losses from internet crimes increased to US$1.33 billion in 2016, most of which was lost in confidence frauds. The US Treasury Department's Financial Crimes Enforcement Network has stepped up its role in securing against financial cybercrime, issuing advisories on how to respond to and report cyber events. The Securities and Exchange Commission has also launched a Cyber Police unit, which will target cybercrime violations relating to blockchain and initial coin offerings, market manipulation, and dark-web-related financial misconduct. US-led rendition and prosecution of cybercriminals from around the globe continues, indicating that the US's international law enforcement ties and response capabilities remain strong.

SCORE: 10

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Significant decisions that enhance the role of cyber capabilities within the overall US military have been made. US Cyber Command (CYBERCOM) has started on its journey towards becoming a full unified combatant command, which will be an elevation from being subordinate to US Strategic Command. The elevation comes alongside the provision of authorities to develop strategy, doctrine and tactics and to have a greater degree of administrative, training and budgetary independence than all other unified combatant commands (other than Special Operations Command). Concern has arisen that CYBERCOM's new responsibilities are too large and that it isn't adequately staffed to meet its wide variety of responsibilities. It's also not yet clear how the potentially conflicting roles of cyber offence at CYBERCOM and intelligence gathering at the National Security Agency will be reconciled. This balancing act currently occurs at the agency head level, as Admiral Michael Rogers heads both organisations, but it hasn't yet been decided whether or for how long this dual-hatted management structure will continue. However, this move for CYBERCOM recognises the growing centrality of cyberspace to US national security and demonstrates a long-term commitment to investment in cyberspace operations to defend the country from cyber threats and to engage adversaries in cyberspace.

SCORE: 10

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

The US Government has a clear focus on improving the quality of its engagement with the private sector on cyber issues. The Commission on Enhancing National Cybersecurity, assembled under the Obama administration from key private-sector leaders, concluded its report and issued recommendations. However, most of the recommendations haven't been adopted by the new administration. Moreover, several members of the National Infrastructure Advisory Council, which is a gathering of private-sector executives from major tech companies and other similarly senior executive positions, have resigned. The resignations came after a number of high-profile events, such as the US withdrawal from the Paris climate accord, the government's controversial bans on migrants from certain countries and a failure to respond adequately to white nationalism in Charlottesville, Virginia. The US congressional system has adopted a much more active stance in engaging the private sector on cybersecurity, and a number of committees and investigations have increasingly scrutinised tech companies' roles in the divisive and misinformation-ridden discourse that surrounded the 2016 presidential election. There's increasing sentiment favouring the regulation of big tech companies when it comes to encryption, extremist messaging, content moderation, privacy, inequality and anti-trust matters. The tech companies in question have begun more actively engaging with the public and with government by broadcasting their actions in those areas. However, while there's increased public- and private-sector engagement on cybersecurity, the interaction between government, industry and the wider public has become more fractured.

SCORE: 9

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The US digital economy continues to stand out globally for the breadth and influence of its digital products and services. Major US technology firms lead the way in the development of new products that have a significant influence on the global digital economy, although that influence is now increasingly being seen in an ambivalent light. The US remains a favourable environment for business and innovation, according to studies from the World Economic Forum and Tufts University. Digital economic transformation in government is clearly valued by the current administration, which has continued to use the expertise of private-sector workers through digital transformation programs such as 18F, the US Digital Service and the Defense Innovation Unit experimental (DIUx). Despite the US's strength in the digital economy, US Government efforts have been hampered by a government-wide hiring freeze, and their remit has been made less clear with the establishment of the new Office of American Innovation under Special Advisor Jared Kushner. In addition, a Trump administration decision to block special 'start-up visas' is projected to negatively affect job creation, as are cuts to the federal budget, which are also predicted to negatively affect innovation throughout the country. Administration decisions that led to many resignations from the Digital Economy Advisory Board (a high-level board that advised about the digital economy) will undoubtedly affect US Government and private-sector policy interactions for the worse. Overall, while the US remains a leading country with one of the most well-developed digital economies, the Trump administration hasn't been able to provide consistent leadership to make the best use of the country's digital advantages.

SCORE: 9

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

Awareness of and debate about cyber matters in the US continues to cover a broad range of issues in international and domestic cyber policy and cybersecurity. A strong academic and think tank community is highly active in researching and providing public comment on cyber issues. Cybersecurity proved to be a defining issue in the 2016 presidential election, and statements from the intelligence community have indicated that Russia played a role in hacking and conducting influence operations during the election. Investigations into the extent and the role of Russian hacking and information operations are ongoing. The issue has yet to be resolved and has proved to be highly divisive, contributing to an at times highly adversarial relationship between the US Government and the mainstream media, and between Republicans and Democrats. There's also been an uptick in conversations about regulating big technology companies on security, information integrity, privacy and anti-trust issues. Encryption remains an issue, although it hasn't proved to be as mainstream a topic as it was last year. The Federal Communications Commission's decision to overturn an Obama-era net neutrality provision has uncorked a wellspring of public comment, drawing more than 22 million public comments, 98.5% of which oppose the plan to repeal the rules. While public awareness of cyber issues has become even more heightened, the debate and media coverage can be highly polarised by divisive and adversarial discussions across the political spectrum and between the government and the public.

SCORE: 10

b) What percentage of individuals use the internet?

The US has a large and well-developed telecommunications market and has high rates of both fixed-line and mobile broadband penetration (32 and 120 subscribers per 100 inhabitants, respectively). Smartphone ownership is high, mobile data usage continues to increase, and 76% of inhabitants use the internet.

SCORE: 8

VANUATU

Rank 2017: 17th of 25

2016: NA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	5
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	5
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	1
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	2
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	0
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	7
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	4
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of individuals use the internet?	3

OVERALL ASSESSMENT

Vanuatu has clearly defined government structures for cyber matters, which generally focus narrowly on infrastructure development and connectivity. The installation of a submarine cable has increased internet access markedly, and Vanuatu has received international awards for its efforts in telecommunications infrastructure development. This increased connectivity, however, will come with an increased threat of cybercrime, and Vanuatu's cybersecurity structures remain underdeveloped and underprepared for such increased risk.

WEIGHTED SCORE 35.2

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

In Vanuatu, the Prime Minister is also the minister responsible for ICT and telecommunications. The multistakeholder National ICT Committee, which advises the government on cyber matters, works with the Prime Minister. The Office of the Government Chief Information Officer is tasked with encouraging the spread of ICT in Vanuatu. The Telecommunications and Radiocommunications Regulator, set up in 2009, is tasked with ICT market liberalisation and regulation. Vanuatu has had a National Cybersecurity Policy, National ICT Policy and Universal Access Policy since 2013. Significant steps have been taken to improve connectivity and infrastructure in recent years, including the installation of a submarine fibre-optic cable in 2014. Vanuatu also won an ITU award in 2015 for ICTs in Sustainable Development.

SCORE: 5

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

Vanuatu doesn't yet have specific cybercrime legislation but has some cyber-related legislation. Notable pieces are the Electronic Transactions Act of 2000, the E-Business Act of 2000, and the Telecommunications and Radiocommunications Regulation Act of 2009. A specific Cybercrime Bill has been drafted but there are concerns that the draft bill falls short in key areas of combating cybercrime. It's hoped that it will be brought before parliament by the end of this year.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Vanuatu actively engages in international discussions on cyberspace, mainly in multilateral forums on technical matters. According to the National ICT Policy, Vanuatu has many international ICT partners, especially in Melanesia, and has engaged with the ITU on many areas. In 2014, the ITU IMPACT body conducted a CIRT/CERT readiness assessment for Vanuatu as the first step in setting up a national CERT. Vanuatu is a member of AusCERT and the now dormant PacCERT and has begun collaboration and partnership with CERT Australia. It also hosts Pacific ICT Day, which is an annual international ICT event in Port Vila that attracts several high-level attendees from the Pacific region and elsewhere.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

Vanuatu doesn't currently have a CERT. It was a member of PacCERT before PacCERT closed due to lack of funding. The Office of the Government Chief Information Officer maintains Vanuatu's membership with AusCERT. Vanuatu is now working with the ITU to lay the groundwork for a national CERT.

SCORE: 1

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Vanuatu doesn't have a cybercrime centre or unit, but its Financial Intelligence Unit, which investigates money laundering and terrorism financing, also investigates financial cybercrime. The unit's latest annual report, released in 2012, specifically mentioned cybercrime as an area of concern but showed little action in combating it. Non-financial cybercrimes are the domain of the Vanuatu Police Force through its Trans-National Crime unit, which was established to investigate crimes committed across borders and online. The Vanuatu Police Force is an important stakeholder for the current National Cyber Security Policy and recently for the draft Cybercrime Bill. Vanuatu engages passively in international discussions on the issue of cybercrime. It's a member of Cyber Safety Pasifika, which is run by the Australian Federal Police and dedicated to promoting community awareness about cybersafety issues, and the Pacific Islands Law Officer Network, which recognises cybercrime as a 'priority legal issue' in the Pacific islands.

SCORE: 2

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Vanuatu does not have a formal military.

SCORE: 0

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Vanuatu's government recognises the importance of industry players, as well as other stakeholders, in cyber discussions and has structures in place to facilitate their participation. The National Cybersecurity Policy and National ICT Policy were the result of consultation between government ministries and agencies, the private sector, NGOs and civil society. These policies identify building a platform for multistakeholder and multisector coordination and collaboration as a priority. In the country's ICT governance structure, the permanent multistakeholder National ICT Development Committee advises the Prime Minister on cyber issues. Vanuatu businesses have also engaged with the regional private sector. For example, the Vanuatu Chamber of Commerce and Industry attended the Pacific Business Forum, the second iteration of which met in August and was focused on the digital economy.

SCORE: 7

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

The economy relies mainly on agriculture, fishing, tourism and offshore financial services. The government clearly recognises the potential benefits of a digital economy and is working to build infrastructure to realise those opportunities. The submarine cable connecting Vanuatu to broadband networks has been a major boost for internet connectivity, and there are signs of digital development (for example, all local banks now offer internet banking).

SCORE: 4

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

More widespread internet access has also resulted in increased public awareness of cyber issues. In an indicator of public engagement, the Vanuatu Government is amending its draft Cybercrime Bill based on feedback from public consultations. In addition, international programs such as Cyber Safety Pasifika are attempting to improve public awareness, and many civil society organisations are conducting cyber awareness campaigns, especially using social media.

SCORE: 4

b) What percentage of individuals use the internet?

About 28% of the population uses the internet. Mobile coverage reaches over 90% of the population, and mobile broadband penetration is growing.

SCORE: 3

VIETNAM

Rank 2017: 14th of 25

2016: 11th of 23

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (including policy, security, critical infrastructure protection, CERT, crime and consumer protection)? How effectively have they been implemented?	6
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	7
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	5
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	6
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	5
3 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	3
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	6
5 – SOCIAL	
a) Are there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of individuals use the internet?	6

OVERALL ASSESSMENT

Vietnam has been relatively consistent in its cyber maturity efforts for 2016–17. The Ministry of Information and Communications continues to take the lead on cyber matters and has several departments operating beneath it. Increased collaboration between government and industry has been notable, particularly between the Department of Cyber Security and Vietnam Airlines after the noteworthy attack on the latter's systems in 2016. The Ministry of Public Security released a draft Law on Cyber Security that attracted some criticism, but with some adjustments the law could help reduce cybercrime. Vietnam needs to seek opportunities to engage with countries outside of ASEAN on cyber issues, and improvements need to be made to increase the effectiveness of its High-Tech Crime Prevention group.

WEIGHTED SCORE 53.6

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Vietnam's Ministry of Information and Communications (MIC) is the primary department in charge of cyber matters. The Authority of Information Security, the Department of Information Technology, Vietnam CERT (VNCERT), and the National Electronic Authentication Centre all come under the MIC. The Vietnam Information Security Association is a non-profit cybersecurity-focused group that plays an active role in increasing cybersecurity in Vietnam. The Ministry of Public Security also has a Department of Cyber Security. In March 2017, it was announced that Vietnam intends to establish a national steering committee for cyberattacks as a response to the 2016 attack on Vietnam Airlines. If the proposed cyberattack committee is able to work effectively between the existing structures and the Police Department for High-Tech Crime Prevention, then Vietnam has the potential to progress in this category.

SCORE: 6

b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?

In June 2017, the Ministry of Public Security released a draft Law on Cyber Security, which was open to public consultation for two months. The Asia Internet Coalition published several notable criticisms, including that the draft law is too broad, lacks clarity, restricts civil liberties and will have a negative effect on business in Vietnam. However, once some changes are made, implementation of the Law on Cyber Security could enable greater cooperation between private businesses and government agencies. The Law on Cyber Information Security came into effect in July 2016 and seeks to consolidate the proliferation of existing IT-security-related laws into a single law. The law includes provisions for the protection of the safety of personal information. Vietnam also has the 2001 Management and Use of Internet Services Decree, the 2005 Law on E-Transactions, the 2006 Law on Information Technology, the 2009 Telecommunication Law and the 2010 Law on Protection of Consumers' Rights.

SCORE: 7

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

Vietnam, along with other ASEAN nations, has recently received training from Japan on incident response and countermeasures to cyberattacks. This training is scheduled to continue for a total of three years. In late 2016, Vietnam engaged with Australia in an annual strategic dialogue in which cybersecurity was discussed. Vietnam hosted a training day at which representatives from CNCERT, JPCERT and KrCERT presented on a range of cybersecurity topics. It also hosts Security World, which is an annual conference that focuses on IT security projects in government and industry. It remains a member of both ITU-IMPACT and Interpol. Vietnam needs to be more deliberate in engaging with international partners on cybersecurity to improve in this category.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

VNCERT, established in 2005, is Vietnam's national CERT and works under the MIC. In March 2017, Vietnam participated in the annual APCERT Cyber Drill, focusing on emerging distributed denial of service threats. VNCERT processed more than 134,000 security incidents in 2016, most of which were defacement, malware and phishing incidents. The number of incidents has increased exponentially, from just 19,156 in 2015. VNCERT continues to engage strongly with LaoCERT and also organised a workshop regarding 'kill chain and IOC analysis' for government agencies and CSIRT teams. In order to improve in this category, VNCERT needs to increase its international engagement, particularly outside of ASEAN.

SCORE: 6

2 CYBERCRIME

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

Vietnam's Police Department for High-Tech Crime Prevention has struggled to keep up with the onerous task of protecting the country against cyberattacks. Vietnam was ranked 101 out of 195 countries in the Global Security Index 2017—the poorest ranking in Southeast Asia. The unit has mainly focused its energy on tackling gambling rings but has failed to reduce cybercrime. Microsoft revealed early in 2017 that Vietnam has experienced double the volume of malware compared to the world average.

SCORE: 5

3 MILITARY

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

Vietnam's military hasn't taken an active role in cybersecurity. In 2017, FireEYE released information about a hacking group from Vietnam called APT32, but it isn't known whether that group has any connection to the military. The MIC seems to take on most cybersecurity work, and little is known about the involvement of the military in cybersecurity matters.

SCORE: 3

4 BUSINESS

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

Vietnamese Prime Minister Nguyen Xuan Phuc has highlighted the importance for Vietnam of capitalising on the next industrial revolution (or 'Industry 4.0'), which will include advanced technologies such as artificial intelligence, the IoT and automated vehicles. In June 2017, the Department of Cyber Security signed an agreement with Vietnam Airlines to help evaluate the airline's security measures and prevent attacks on critical infrastructure. This followed a cyberattack in July 2016 in which computer systems were compromised and flight information was stolen. An industry body, the Asia Internet Coalition, regularly responds to laws and decrees produced by the Ministry of Public Security. The Vietnam Information Security Association, an industry-led organisation that undertakes R&D on cyber issues, worked with the MIC to coordinate Vietnam Information Security Day.

SCORE: 5

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

Experts who attended the Vietnam Private Sector Forum noted that the digital economy has huge growth potential in Vietnam but currently makes up only a small part of the national economy. The head of the forum, Nguyen Trung Chinh, estimated Vietnam's digital economy to be worth just US$900 million in 2016. According to a June 2017 KPMG report, Vietnam is considering implementing taxation rules for digital companies profiting in Vietnam. The Vietnamese Government is said to be studying a base erosion and profit shifting plan similar to that of the Organisation for Economic Co-operation and Development. In August 2017, the Asia Internet Coalition claimed that Vietnam's new draft Law on Cyber Security could hinder the digital economy because of the difficult responsibilities it places on ISPs. Despite Vietnam being labelled as a 'break out' country in the 2017 Digital Evolution Index, there's evidence to suggest that only a small proportion of businesses contribute to the digital economy in Vietnam, indicating slow implementation of policies. With this in mind, Vietnam's focus on taxation issues seems misplaced; it would be more beneficial to focus on policies that promote the digital economy first.

SCORE: 6

5 SOCIAL

a) Are there public awareness, debate and media coverage of cyber issues?

More than half of Vietnam's population are internet users. The Vietnam Information Security Association is the premier source of cybersecurity information for the public. In August 2017, Vietnamese President Tran Dai Quang published an article on a government website calling for improved cybersecurity. Minister for Information and Communications Truong Minh Tuan made a speech in April 2017 saying he wanted Vietnam to produce its own platforms to replace Facebook and Google, because the country can't control those sites or their content.

SCORE: 4

b) What percentage of individuals use the internet?

Vietnam has a relatively high fixed-line broadband penetration of 10 subscribers per 100 inhabitants, and a moderate mobile broadband penetration of 46 subscribers per 100 inhabitants. Mobile broadband is growing rapidly, fixed-line broadband is growing moderately, and 57% of individuals use the internet.

SCORE: 6

APPENDIXES

APPENDIX 1:
SCORING BREAKDOWN

Key indicators	Scoring breakdown
1a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?	0 = No organisational structure, policy frameworks, or protections. 1 = Some intent to develop cyber policy frameworks and organisational structure but little or no action to implement them. 2 = Clear intent to develop a cyber policy framework but no clear plan for organisational structure or implementation. 3 = Basic organisational structures (mainly technical) exist; some plans for policy and organisational development. 4 = Basic organisational structures (mainly technical) exist; policy and organisational development underway. 5 = Nascent policy frameworks and organisational structures exist, but are narrowly focused and/or not yet implemented. 6 = Policy frameworks and organisational structures exist; implementation is apparent. 7 = Policy frameworks and organisational structures exist; implementation is obvious but not yet comprehensive or complete. 8 = Strong policy frameworks and organisational structures exist, but are not yet fully implemented. 9 = Extensive, but not comprehensive, policy frameworks and organisational structures exist and are fully implemented. 10 = Comprehensive, strong policy frameworks and organisational structures exist and are fully implemented.
1b) Is there existing legislation/regulation relating to cyber issues and ISPs? Is it being used?	0 = No cybersecurity laws or regulations exist. 1 = Insufficient legislation exists, or government regulation is excessive. 2 = Insufficient legislation exists, but there is some intent to begin development of suitable legal frameworks. 3 = A few laws exist, but without adequate implementation measures. 4 = A few laws exist; some implementation measures undertaken. 5 = A legal framework exists, with moderate implementation; some regulation in specific areas. 6 = A legal framework exists, with moderate implementation; some regulation in critical areas. 7 = A strong legal framework exists; implementation is incomplete or stalled. 8 = A strong legal framework exists and is partially implemented. 9 = A strong legal framework exists and is effectively implemented. 10 = A comprehensive legal framework is strongly implemented.
1c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	0 = No international engagement. 1 = Some intent to engage internationally, as yet unrealised. 2 = Some passive international engagement. 3 = Minimal international engagement; technically focused. 4 = Minimal international engagement; aid-based or basic technical/policing. 5 = Some bilateral and multilateral engagement in technical/policing. 6 = Strong bilateral engagement and some multilateral engagement in technical, policing and policy. 7 = Strong bilateral and multilateral engagement in technical/policing and policy engagement. 8 = Very strong bilateral and multilateral engagement in technical/policing and policy engagement. 9 = Multilayered international engagement; bilateral and multilateral engagement, technical/policing and policy engagement, with leadership roles. 10 = A prominent leader in multilayered international engagement; bilateral and multilateral engagement, technical/policing and policy engagement.

Key indicators	Scoring breakdown
1d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0 = No. 1 = No; plans exist for establishment. 2 = Yes, but response capability is developing. 3 = Limited response capability; emerging international engagement. 4 = Uneven response capability; some international engagement. 5 = Structured and planned response capability; minimal international engagement. 6 = Structured and planned response capability; limited international engagement. 7 = Well-structured and planned response capability; some international engagement. 8 = Well-structured and planned response capability; strong international engagement. 9 = Strong response capability; strong international leadership. 10 = Very strong response capability; key international leader.
2a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	0 = No. 1 = No; plans exist for establishment or some personnel are in training. 2 = Yes, but response capability is developing. 3 = Limited response capability; emerging international engagement. 4 = Uneven response capability; some international engagement. 5 = Structured and planned response capability; minimal international engagement. 6 = Structured and planned response capability; limited international engagement. 7 = Well-structured and planned response capability; some international engagement. 8 = Well-structured and planned response capability; strong international engagement. 9 = Strong response capability; strong international leadership. 10 = Very strong response capability; key international leader.
3a) What is the military's role in cyberspace, cyber policy and cybersecurity?	0 = No awareness of cybersecurity threats. 1 = Limited awareness of cybersecurity threats. 2 = Limited awareness of cybersecurity threats; some plans for defensive capability. 3 = No policy development apparent; limited defensive capabilities apparent. 4 = Minimal defensive capabilities; nascent policy framework exists. 5 = Good defensive capability; some policy frameworks exist. 6 = Very good defensive capability, defined military role in cyber policy and capability; some international engagement. 7 = Defined civilian and military roles in cyber policy and capability development; good international engagement; very strong defensive capability. 8 = Well-defined civilian and military cyber roles; very good international engagement; very strong defensive capability. 9 = Well-defined civilian and military cyber roles, with clear cyber policy direction and strong international engagement; excellent defensive capability. 10 = Clear definition of the separation of responsibility for military and civil agencies in cybersecurity; clear military cyber strategy and/or doctrine; a leader in international engagement; excellent defensive capability.

Key indicators	Scoring breakdown
4a) Is there dialogue between government and industry on cyber issues? What is the level/ quality of interaction?	0 = No dialogue; no plans to begin or facilitate dialogue. 1 = No dialogue; some plans to begin or facilitate dialogue. 2 = Some dialogue beginning. 3 = Very limited dialogue. 4 = Limited dialogue. 5 = Dialogue exists, but is one-way or with only a few sectors. 6 = Two-way dialogue exists with a narrow range of critical sectors. 7 = Two-way dialogue exists with a broad range of sectors. 8 = Very good two-way dialogue exists with a broad range of sectors. 9 = Strong two-way dialogue exists, with some capacity for the private sector to play an advisory role in policy and operational issues. 10 = Strong two-way dialogue exists, with capacity for the private sector to play an active role in policy and operational issues.
4b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	0 = No evidence of a digital economy. 1 = Little evidence of a digital economy; some evidence of awareness of its benefits. 2 = Little evidence of a digital economy; nascent awareness of its benefits, or organic emergence of e-commerce. 3 = There is an awareness of the benefits of the digital economy, which is a small portion of economic activity. 4 = Digital economy is a small part of economic activity; growing awareness of its potential. 5 = Digital economy is a growing part of economic activity, but no government policy to assist it exists. 6 = Digital economy is a growing part of economic activity; government policy to assist it under development. 7 = Digital economy is a strong and expanding part of economic activity; some government policy to assist it exists. 8 = Digital economy is a very strong and expanding part of economic activity; significant government policy to assist it exists. 9 = Digital economy is a fully integrated element of the state's economic activity; strong government policy to assist digital economic growth. 10 = Digital economy is a fully integrated element of the state's economic activity; strongly implemented mature government policy to assist digital economic growth exists.
5a) Are there public awareness, debate and media coverage of cyber issues?	0 = No dialogue on cybersecurity issues. 1 = Very little coverage of cyber issues. 2 = Some coverage, mainly external. 3 = Insubstantial domestic media interest in cyber issues. 4 = Limited awareness, mainly media- and NGO-led. 5 = Good awareness, but mainly media- and NGO-led. 6 = Good awareness among public and media. 7 = Strong public, media and private-sector debate on cyber issues. 8 = Very strong public, media and private-sector debate on cyber issues. 9 = Strong public, media, academic and private-sector debate on cyber issues. 10 = Very strong public, media, academic and private-sector debate on cyber issues.

Key indicators	Scoring breakdown
5b) What percentage of individuals use the internet?	1 = 0–9% 2 = 10–19% 3 = 20–29% 4 = 30–39% 5 = 40–49% 6 = 50–59% 7 = 60–69% 8 = 70–79% 9 = 80–89% 10 = 90–100%

APPENDIX 2:
2017 OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

		1a	1b	1c	1d	2	3	4a	4b	5a	5b	Total	Weighted score
Weighting		**8.0**	**7.8**	**7.0**	**8.0**	**7.8**	**6.8**	**7.8**	**7.7**	**6.0**	**7.0**		
Australia	Scores	8	9	9	9	9	8	9	9	9	9	88	
	Weighted scores	6.4	7.1	6.3	7.2	7.1	5.5	7.1	6.9	5.4	6.3	65.1	**88.0**
Bangladesh	Scores	4	3	3	3	4	1	4	4	5	2	33	
	Weighted scores	3.2	2.4	2.1	2.4	3.1	0.7	3.1	3.1	3.0	1.4	24.5	**33.1**
Brunei	Scores	6	6	4	6	5	4	6	6	3	8	54	
	Weighted scores	4.8	4.7	2.8	4.8	3.9	2.7	4.7	4.6	1.8	5.6	40.5	**54.7**
Cambodia	Scores	4	4	4	3	4	1	3	6	4	3	36	
	Weighted scores	3.2	3.1	2.8	2.4	3.1	0.7	2.4	4.6	2.4	2.1	26.8	**36.2**
China	Scores	9	8	9	6	6	8	5	8	5	6	70	
	Weighted scores	7.2	6.3	6.3	4.8	4.7	5.5	3.9	6.1	3.0	4.2	52.0	**70.2**
Fiji	Scores	2	4	4	0	4	1	2	3	4	5	29	
	Weighted scores	1.6	3.1	2.8	0.0	3.1	0.7	1.6	2.3	2.4	3.5	21.1	**28.5**
India	Scores	7	5	8	5	4	3	6	7	8	3	56	
	Weighted scores	5.6	3.9	5.6	4.0	3.1	2.1	4.7	5.4	4.8	2.1	41.3	**55.8**
Indonesia	Scores	6	6	5	5	6	6	5	7	5	3	54	
	Weighted scores	4.8	4.7	3.5	4.0	4.7	4.1	3.9	5.4	3.0	2.1	40.2	**54.3**
Japan	Scores	9	8	10	10	8	7	8	9	9	10	88	
	Weighted scores	7.2	6.3	7.0	8.0	6.3	4.8	6.3	6.9	5.4	7.0	65.1	**88.0**
Laos	Scores	4	4	3	4	1	1	4	3	3	3	30	
	Weighted scores	3.2	3.1	2.1	3.2	0.8	0.7	3.1	2.3	1.8	2.1	22.4	**30.3**
Malaysia	Scores	7	8	8	8	6	7	7	8	6	8	73	
	Weighted scores	5.6	6.3	5.6	6.4	4.7	4.8	5.5	6.1	3.6	5.6	54.2	**73.2**
Myanmar	Scores	3	4	4	3	2	5	1	3	2	3	30	
	Weighted scores	2.4	3.1	2.8	2.4	1.6	3.4	0.8	2.3	1.2	2.1	22.1	**29.9**
New Zealand	Scores	8	8	8	8	7	6	9	10	9	9	80	
	Weighted scores	6.4	6.3	6.4	6.4	5.5	4.1	7.1	7.7	5.4	6.3	59.3	**82.0**

		1a	1b	1c	1d	2	3	4a	4b	5a	5b	Total	Weighted score
Weighting		**8.0**	**7.8**	**7.0**	**8.0**	**7.8**	**6.8**	**7.8**	**7.7**	**6.0**	**7.0**		
North Korea	Scores	3	1	3	0	0	8	0	1	1	1	18	
	Weighted scores	2.4	0.8	2.1	0.0	0.0	5.5	0.0	0.8	0.6	0.7	12.8	**17.3**
Pakistan	Scores	3	4	2	1	4	4	5	3	2	2	30	
	Weighted scores	2.4	3.1	1.4	0.8	3.1	2.7	3.9	2.3	1.2	1.4	22.4	**30.3**
Papua New Guinea	Scores	4	4	4	1	1	1	2	1	5	1	24	
	Weighted scores	3.2	3.1	2.8	0.8	0.8	0.7	1.6	0.8	3.0	0.7	17.4	**23.6**
Philippines	Scores	6	6	6	3	6	3	4	5	6	5	50	
	Weighted scores	4.8	4.7	4.2	2.4	4.7	2.1	3.1	3.8	3.6	3.5	36.9	**49.9**
Singapore	Scores	9	8	8	7	8	9	10	10	10	9	88	
	Weighted scores	7.2	6.3	5.6	5.6	6.3	6.2	7.8	7.7	6.0	6.3	64.9	**87.7**
Solomon Islands	Scores	3	0	3	0	1	0	2	1	2	2	14	
	Weighted scores	2.4	0.0	2.1	0.0	0.8	0.0	1.6	0.8	1.2	1.4	10.2	**13.8**
South Korea	Scores	8	9	8	8	8	9	9	9	9	10	87	
	Weighted scores	6.4	7.1	5.6	6.4	6.3	6.2	7.1	6.9	5.4	7.0	64.2	**86.8**
Taiwan	Scores	8	6	3	3	5	5	6	6	6	9	57	
	Weighted scores	6.4	4.7	2.1	2.4	3.9	3.4	4.7	4.6	3.6	6.3	42.1	**56.9**
Thailand	Scores	7	6	5	5	5	5	4	6	6	5	54	
	Weighted scores	5.6	4.7	3.5	4.0	3.9	3.4	3.1	4.6	3.6	3.5	40.0	**54.0**
United States of America	Scores	10	8	9	8	10	10	9	9	10	8	91	
	Weighted scores	8.0	6.3	6.3	6.4	7.8	6.8	7.1	6.9	6.0	5.6	67.2	**90.8**
Vanuatu	Scores	5	4	5	1	2	0	7	4	4	3	35	
	Weighted scores	4.0	3.1	3.5	0.8	1.6	0.0	5.5	3.1	2.4	2.1	26.1	**35.2**
Vietnam	Scores	6	7	5	6	5	3	5	6	4	6	53	
	Weighted scores	4.8	5.5	3.5	4.8	3.9	2.1	3.9	4.6	2.4	4.2	39.7	**53.6**

APPENDIX 3:
2016 OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

		1a	1b	1c	1d	2	3	4a	4b	5a	5b	5c	Total	Weighted score
Weighting		**8.0**	**7.8**	**7.0**	**8.0**	**7.8**	**6.8**	**7.8**	**7.7**	**6.0**	**7.0**	**7.0**		
Australia	Scores	8	8	9	8	9	8	8	9	9	3	10	89	
	Weighted scores	6.4	6.3	6.3	6.4	7.1	5.5	6.3	6.9	5.4	2.1	7.0	65.6	**80.9**
Bangladesh	Scores	4	3	2	2	3	1	4	4	5	1	2	31	
	Weighted scores	3.2	2.4	1.4	1.6	2.4	0.7	3.1	3.1	3.0	0.7	1.4	22.9	**28.3**
Brunei	Scores	6	6	4	6	5	4	5	5	3	1	1	46	
	Weighted scores	4.8	4.7	2.8	4.8	3.9	2.7	3.9	3.8	1.8	0.7	0.7	34.7	**42.8**
Cambodia	Scores	4	4	3	3	2	1	3	3	4	1	5	33	
	Weighted scores	3.2	3.1	2.1	2.4	1.6	0.7	2.4	2.3	2.4	0.7	3.5	24.3	**30.0**
China	Scores	9	7	9	6	6	8	5	6	5	2	6	69	
	Weighted scores	7.2	5.5	6.3	4.8	4.7	5.5	3.9	4.6	3.0	1.4	4.2	51.1	**63.0**
Fiji	Scores	2	4	3	0	4	1	2	3	3	1	5	28	
	Weighted scores	1.6	3.1	2.1	0.0	3.1	0.7	1.6	2.3	1.8	0.7	3.5	20.5	**25.3**
India	Scores	7	5	7	5	4	3	5	7	7	1	2	53	
	Weighted scores	5.6	3.9	4.9	4.0	3.1	2.1	3.9	5.4	4.2	0.7	1.4	39.2	**48.4**
Indonesia	Scores	5	5	5	6	4	6	5	5	5	1	5	52	
	Weighted scores	4.0	3.9	3.5	4.8	3.1	4.1	3.1	4.6	3.0	0.7	3.5	38.4	**47.4**
Japan	Scores	9	8	9	10	8	7	8	9	9	4	10	91	
	Weighted scores	7.2	6.3	6.3	8.0	6.3	4.8	6.3	6.9	5.4	2.8	7.0	67.2	**82.9**
Laos	Scores	4	3	2	3	1	1	2	2	2	1	2	23	
	Weighted scores	3.2	2.4	1.4	2.4	0.8	0.7	1.6	1.5	1.2	0.7	1.4	17.2	**21.3**
Malaysia	Scores	7	7	8	8	6	6	7	8	6	1	10	74	
	Weighted scores	5.6	5.5	5.6	6.4	4.7	4.1	5.5	6.1	3.6	0.7	7.0	54.8	**67.7**

		1a	1b	1c	1d	2	3	4a	4b	5a	5b	5c	Total	Weighted score
Weighting		**8.0**	**7.8**	**7.0**	**8.0**	**7.8**	**6.8**	**7.8**	**7.7**	**6.0**	**7.0**	**7.0**		
Myanmar	Scores	3	4	4	3	2	5	1	2	2	1	4	31	
	Weighted scores	2.4	3.1	2.8	2.4	1.6	3.4	0.8	1.5	1.2	0.7	2.8	22.7	**28.1**
New Zealand	Scores	8	8	6	7	7	6	8	9	9	4	10	82	
	Weighted scores	6.4	6.3	4.2	5.6	5.5	4.1	6.3	6.9	5.4	2.8	7.0	60.4	**74.6**
North Korea	Scores	3	1	3	0	0	8	0	1	1	1	1	19	
	Weighted scores	2.4	0.8	2.1	0.0	0.0	5.5	0.0	0.8	0.6	0.7	0.7	13.5	**16.7**
Pakistan	Scores	3	3	2	1	4	4	4	3	2	1	2	29	
	Weighted scores	2.4	2.4	1.4	0.8	3.1	2.7	3.1	2.3	1.2	0.7	1.4	21.6	**26.6**
Papua New Guinea	Scores	4	3	2	0	1	1	2	1	5	1	1	21	
	Weighted scores	3.2	2.4	1.4	0.0	0.8	0.7	1.6	0.8	3.0	0.7	0.7	15.2	**18.7**
Philippines	Scores	5	6	5	0	6	3	4	5	6	1	5	46	
	Weighted scores	4.0	4.7	3.5	0.0	4.7	2.1	3.1	3.8	3.6	0.7	3.5	33.7	**41.6**
Singapore	Scores	9	8	7	7	8	8	10	9	9	3	10	88	
	Weighted scores	7.2	6.3	4.9	5.6	6.3	5.5	7.8	6.9	5.4	2.1	7.0	64.9	**80.2**
Solomon Islands	Scores	3	0	2	0	1	0	2	1	1	1	2	13	
	Weighted scores	2.4	0.0	1.4	0.0	0.8	0.0	1.6	0.8	0.6	0.7	1.4	9.6	**11.9**
South Korea	Scores	8	9	8	8	8	9	9	9	9	5	10	92	
	Weighted scores	6.4	7.1	5.6	6.4	6.3	6.2	7.1	6.9	5.4	3.5	7.0	67.7	**83.6**
Thailand	Scores	6	6	5	5	5	5	4	6	6	2	8	58	
	Weighted scores	4.8	4.7	3.5	4.0	3.9	3.4	3.1	4.6	3.6	1.4	5.6	42.7	**52.7**
United States of America	Scores	10	8	9	8	10	10	9	9	10	4	10	97	
	Weighted scores	8.0	6.3	6.3	6.4	7.8	6.8	7.1	6.9	6.0	2.8	7.0	71.4	**88.1**
Vietnam	Scores	6	7	5	6	6	3	4	6	4	1	4	52	
	Weighted scores	4.8	5.5	3.5	4.8	4.7	2.1	3.1	4.6	2.4	0.7	2.8	39.0	**48.1**

APPENDIX 4:
2015 OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

		1a	1b	1c	1d	2a	3a	4a	4b	5a	5b	Total weighted scores
Weighting		**8**	**7.8**	**7**	**8**	**7.8**	**6.8**	**7.8**	**7.7**	**6**	**7**	
Australia	Scores	7	8	9	8	9	7	7	8	8	9	
	Weighted scores	5.6	6.3	6.3	6.4	7.1	4.8	5.5	6.1	4.8	6.3	**79.9**
Brunei	Scores	6	6	4	6	5	4	5	5	3	7	
	Weighted scores	4.8	4.7	2.8	4.8	3.9	2.7	3.9	3.8	1.8	4.9	**51.6**
Cambodia	Scores	3	3	3	2	1	1	2	1	4	1	
	Weighted scores	2.4	2.4	2.1	1.6	0.8	0.7	1.6	0.8	2.4	0.7	**20.7**
China	Scores	8	7	9	6	5	8	5	6	5	5	
	Weighted scores	6.4	5.5	6.3	4.8	3.9	5.5	3.9	4.6	3	3.5	**64**
Fiji	Scores	2	4	4	0	4	2	3	4	3	5	
	Weighted scores	1.6	3.1	2.8	0	3.1	1.4	2.4	3.1	1.8	3.5	**30.7**
India	Scores	7	5	7	4	4	4	5	6	6	2	
	Weighted scores	5.6	3.9	4.9	3.2	3.1	2.7	3.9	4.6	3.6	1.4	**50**
Indonesia	Scores	6	5	5	6	4	5	4	5	4	2	
	Weighted scores	4.8	3.9	3.5	4.8	3.1	3.4	3.1	3.8	2.4	1.4	**46.4**
Japan	Scores	8	8	9	10	8	7	8	9	8	10	
	Weighted scores	6.4	6.3	6.3	8	6.3	4.8	6.3	6.9	4.8	7	**85.1**
Laos	Scores	4	3	3	3	1	1	2	2	2	2	
	Weighted scores	3.2	2.4	2.1	2.4	0.8	0.7	1.6	1.5	1.2	1.4	**23.3**
Malaysia	Scores	7	7	8	8	6	5	7	7	6	7	
	Weighted scores	5.6	5.5	5.6	6.4	4.7	3.4	5.5	5.4	3.6	4.9	**68.3**

		1a	1b	1c	1d	2a	3a	4a	4b	5a	5b	Total weighted scores
Weighting		**8**	**7.8**	**7**	**8**	**7.8**	**6.8**	**7.8**	**7.7**	**6**	**7**	
Myanmar	Scores	3	4	4	3	2	5	1	2	2	1	
	Weighted scores	2.4	3.1	2.8	2.4	1.6	3.4	0.8	1.5	1.2	0.7	**26.9**
New Zealand	Scores	8	8	6	7	7	5	6	8	9	9	
	Weighted scores	6.4	6.3	4.2	5.6	5.5	3.4	4.7	6.1	5.4	6.3	**72.8**
North Korea	Scores	3	1	2	0	0	8	0	1	1	1	
	Weighted scores	2.4	0.8	1.4	0	0	5.5	0	0.8	0.6	0.7	**16.4**
PNG	Scores	3	3	3	0	1	2	2	1	5	1	
	Weighted scores	2.4	2.4	2.1	0	0.8	1.4	1.6	0.8	3	0.7	**20.3**
Philippines	Scores	5	5	5	3	5	3	4	6	6	5	
	Weighted scores	4	3.9	3.5	2.4	3.9	2.1	3.1	4.6	3.6	3.5	**46.8**
Singapore	Scores	9	8	7	7	7	8	9	9	9	9	
	Weighted scores	7.2	6.3	4.9	5.6	5.5	5.5	7.1	6.9	5.4	6.3	**81.8**
South Korea	Scores	8	8	7	8	7	9	9	9	9	9	
	Weighted scores	6.4	6.3	4.9	6.4	5.5	6.2	7.1	6.9	5.4	6.3	**82.8**
Thailand	Scores	6	6	5	5	4	5	3	6	5	4	
	Weighted scores	4.8	4.7	3.5	4	3.1	3.4	2.4	4.6	3	2.8	**49.1**
United States of America	Scores	9	8	9	8	10	10	9	9	10	9	
	Weighted scores	7.2	6.3	6.3	6.4	7.8	6.8	7.1	6.9	6	6.3	**90.7**
Vietnam	Scores	6	7	5	6	6	4	4	6	4	5	
	Weighted scores	4.8	5.5	3.5	4.8	4.7	2.7	3.1	4.6	2.4	3.5	**53.6**

APPENDIX 5:
2014 OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

		Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores
	Weighting	Australia	Australia	Cambodia	Cambodia	China	China	India	India	Indonesia	Indonesia	Japan	Japan	Malaysia	Malaysia	Myanmar	Myanmar
1a	8.4	7	5.9	2	1.7	6	5.1	7	5.9	5	4.2	7	5.9	7	5.9	4	3.4
1b	8.3	9	7.5	3	2.5	5	4.1	5	4.1	4	3.3	7	5.8	5	4.1	4	3.3
1c	6.9	8	5.5	3	2.1	9	6.2	5	3.4	6	4.1	8	5.5	7	4.8	4	2.7
1d	6.3	8	5.0	3	1.9	6	3.8	5	3.1	6	3.8	9	5.7	7	4.4	3	1.9
2a	7.0	7	4.9	2	1.4	8	5.6	4	2.8	4	2.8	6	4.2	4	2.8	5	3.5
3a	7.3	6	4.4	1	0.7	3	2.2	3	2.2	3	2.2	8	5.8	5	3.6	2	1.5
3b	7.4	8	5.9	1	0.7	7	5.2	4	3.0	4	3.0	8	5.9	6	4.5	1	0.7
4a	4.9	7	3.4	2	1.0	4	1.9	6	2.9	4	1.9	7	3.4	5	2.4	2	1.0
4b	6.1	8	4.9	1	0.6	4	2.5	2	1.2	2	1.2	8	4.9	6	3.7	1	0.6
Total weighted scores			**75.8**		**20.1**		**58.4**		**45.9**		**42.4**		**75.3**		**57.9**		**29.7**

	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores	Scores	Weighted scores
	North Korea	North Korea	PNG	PNG	Philippines	Philippines	Singapore	Singapore	South Korea	South Korea	Thailand	Thailand	United Kingdom	United Kingdom	United States	United States
1a	3	2.5	3	2.5	5	4.2	8	6.7	7	5.9	5	4.2	9	7.6	9	7.6
1b	1	0.8	3	2.5	4	3.3	6	5.0	6	5.0	5	4.1	8	6.6	7	5.8
1c	2	1.4	3	2.1	5	3.4	7	4.8	7	4.8	4	2.7	9	6.2	10	6.9
1d	0	0.0	2	1.3	4	2.5	8	5.0	8	5.0	5	3.1	6	3.8	9	5.7
2a	7	4.9	2	1.4	5	3.5	7	4.9	7	4.9	4	2.8	8	5.6	9	6.3
3a	1	0.7	1	0.7	2	1.5	8	5.8	8	5.8	2	1.5	8	5.8	8	5.8
3b	2	1.5	1	0.7	6	4.5	7	5.2	8	5.9	5	3.7	8	5.9	9	6.7
4a	1	0.5	4	1.9	5	2.4	9	4.4	9	4.4	4	1.9	9	4.4	9	4.4
4b	1	0.6	2	1.2	3	1.8	8	4.9	9	5.5	3	1.8	8	4.9	8	4.9
Total weighted scores		**20.7**		**23.0**		**43.4**		**74.7**		**75.5**		**41.6**		**81.2**		**86.3**

APPENDIX 6:
KEY INDICATORS

Country	*Freedom on the net* report[a]	ITU statistics 2017[b]			FIRST membership[c]	World Economic Forum *2016 Global information technology report*: Knowledge-intensive jobs, % workforce (rank)[d]	APCERT operational member teams[e]
		Fixed broadband subscriptions/100 inhabitants	Active mobile-broadband subscriptions/100 inhabitants	Percentage of individuals using the internet			
Australia	Free	30.4	130.2	88.2	6	44.9 (13)	CERT Australia, AusCERT,
Bangladesh	Partly free	3.8	17.8	18.2	1	20.0 (71)	bdCERT, BGD e-GOV CIRT
Brunei	n.a.	8.3	116.6	75.0	1	n.a.	BruCERT
Cambodia	Partly free	0.6	50.2	25.6	0	4.1 (104)	n.a.
China	Not free	22.9	66.8	53.2	6	n.a.	CCERT, CNCERT/CC
Fiji	n.a.	1.4	54.3	46.5	0	n.a.	n.a.
India	Partly free	1.4	16.8	29.6	1	n.a.	CERT-In
Indonesia	Partly free	1.9	67.3	25.4	1	8.9 (98)	ID-CERT, ID-SIRTII/CC
Japan	Free	31.5	131.9	92.0	30	24.4 (58)	JPCERT/CC
Laos	n.a.	0.3	34.7	24.8	0	n.a.	LaoCERT
Malaysia	Partly free	8.7	91.7	78.8	2	25.2 (53)	MyCERT
Myanmar	Not free	0.1	47.6	24.4	0	n.a.	mmCERT
New Zealand	n.a.	34.2	101.3	88.5	3	42.9 (18)	CERT NZ
North Korea	n.a.	n.a.	14.3.	n.a.	0	n.a.	n.a.
Pakistan	Not free	0.9	20.1	15.5	0	19.5 (73)	n.a.
Papua New Guinea	n.a.	0.2	9.2	9.6	0	n.a.	n.a.
Philippines	Free	5.5	46.3	47.8	0	23.5 (61)	n.a.
Singapore	Partly free	25.4	144.6	85.2	11	52.7 (2)	SingCERT
Solomon Islands	n.a.	0.2	12.9	11.0	0	n.a.	n.a.
South Korea	Partly free	41.1	111.5	92.7	8	21.6 (65)	KrCERT/CC
Taiwan	n.a.	31.9	66.9	83.0	4	33.3 (39)	EC-CERT, TWCERT/CC, TWNCERT
Thailand	Not free	10.7	94.7	47.5	1	13.8 (90)	ThaiCERT
United States of America	Free	32.4	120.0	76.2	77	38.0 (26)	n.a.
Vanuatu	n.a.	1.6	22.3	27.5	0	n.a.	n.a.
Vietnam	Not free	9.9	46.6	57.1	0	10.3 (95)	VNCERT

n.a. = not available.

a https://freedomhouse.org/report/freedom-net/freedom-net-2016

b www.itu.int/pub/D-IND-WTID.OL-2017

c www.first.org/members/map

d www.weforum.org/reports/the-global-information-technology-report-2016/

e www.apcert.org/about/structure/members.html

ACRONYMS AND ABBREVIATIONS

AFP	Australian Federal Police; Armed Forces of the Philippines
AML/CTF	anti-money-laundering and counterterrorism financing
APCERT	Asia–Pacific Computer Emergency Response Team
APEC	Asia–Pacific Economic Cooperation
APNIC	Asia–Pacific Network Information Centre
ASEAN	Association of Southeast Asian Nations
AusCERT	Australia CERT
AUSTRAC	Australian Transactions and Analysis Centre
bdCERT	Bangladesh CERT
BGD e-GOV CIRT	Bangladesh e-Government CIRT
BruCERT	Brunei CERT
BSSN	Badan Siber dan Sandi Negara (Indonesia)
CAC	Cyberspace Administration of China
CamCERT	Cambodia CERT
CCERT	China Education and Research Network Emergency Response Team
CERT	computer emergency response team
CERT-In	CERT India
CERT NZ	New Zealand CERT
CIRT	computer incident response team
CNCERT	China CERT
CSA	Cyber Security Agency (Singapore)
CSIRT	computer security incident response team
CSM	Cyber Security Malaysia
CSP CERT	Philippines CERT
CTO	Commonwealth Telecommunications Organisation
CYBERCOM	US Cyber Command
DICT	Department of Information Communication Technology (Philippines)
FBI	Federal Bureau of Investigation (US)
FIRST	Forum of Incident Response and Security Teams
GCSIRT	Government Computer Security Incident Response Team (Philippines)
GDP	gross domestic product
ICPC	International Cyber Policy Centre (ASPI)
ICS-CERT	Industrial Control System CERT (US)
ICT	information and communications technology
ID-CERT	Indonesia CERT
ID-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center
IMPACT	International Multilateral Partnership Against Cyber Threats
IoT	internet of things
ISP	internet service provider
IT	information technology
ITU	International Telecommunication Union
JPCERT/CC	Japan CERT / Coordination Center
KISA	Korea Internet and Security Agency
KNCERT/CC	South Korea National Intelligence Service CERT for critical infrastructure in government/public sector
KrCERT/CC	Korea Internet Security Center (South Korea)
mmCERT	Myanmar CERT
MDES	Ministry of Digital Economy and Society (Thailand)
MIC	Ministry of Information and Communications (Vietnam)
MoU	memorandum of understanding
MyCERT	Malaysia CERT
NCSC	National Cyber Security Centre (New Zealand, Singapore); National Cyber Security Center (South Korea)
NGO	non-government organisation
NR3C	National Response Centre for Cyber Crimes (Pakistan)
NZDF	New Zealand Defence Force
OIC-CERT	Organisation of Islamic Cooperation CERT
PacCERT	Pacific CERT
PakCERT	Pakistan CERT
PH-CERT	Philippines CERT
PISA-CERT	Pakistan Information Security Association CERT
PNG	Papua New Guinea
R&D	research and development
RSIPF	Royal Solomon Islands Police Force
SingCERT	Singapore CERT
ThaiCERT	Thailand CERT
TSUBAME	Internet Traffic Monitoring Data Visualisation Project
TWNCERT	Taiwan National CERT
UN	United Nations
UNGGE	United Nations Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security
US-CERT	United States CERT
VNCERT	Vietnam CERT

AUTHORS

TOM UREN

Tom Uren is a Visiting Fellow in the International Cyber Policy Centre. He has worked in various analytical and operational areas in Defence and has diverse expertise across internet and cyber issues. Tom researches and writes on international and domestic cyber issues. He has a BSc(Hons) in Molecular Biology and previously worked for CSIRO in research on forest tree molecular genetics.

FERGUS HANSON

Fergus Hanson is Head of the International Cyber Policy Centre at ASPI. He is the author of *Internet Wars* and has published widely on a range of cyber and foreign policy topics. He was a Visiting Fellow at the Brookings Institution and a Professional Fulbright Scholar based at Georgetown University working on the take-up of new technologies by the US Government. Fergus has worked for the UN and as a Program Director at the Lowy Institute and served as a diplomat at the Australian Embassy in The Hague. He has been a Fellow at Cambridge University's Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies, Pacific Forum.

FERGUS RYAN

Fergus Ryan is an analyst at the International Cyber Policy Centre. He has worked in media, communications and marketing roles in China and Australia for close to a decade and has published widely on Chinese tech, entertainment and media industries. Most recently, Fergus was a journalist for the News Corp. publications *China Spectator* and *The Australian*. He has also been published in *The Guardian* and *Foreign Policy*. Prior to that, Fergus worked on business development for the Chinese actress Li Bingbing. He holds a Masters in International Studies from the University of Technology Sydney.

MICHAEL CHI

Michael Chi is a research assistant in the International Cyber Policy Centre. His research interests include the policy implications of emerging technology, East Asian security, and Australia's Asia–Pacific policy. Prior to joining ASPI, he worked as a research assistant at the public policy initiative China Matters. Michael holds a Bachelor of International Studies.

JACK VIOLA

Jack Viola is a research intern at ASPI and the International Cyber Policy Centre. He is currently undertaking research into the power dynamics of the Asia–Pacific region and the roles of emerging regional powers. His research interests include East and Southeast Asian security, with a focus on territorial disputes and historical influences. Prior to joining ASPI, Jack studied a Masters in International Relations at the University of Melbourne. He also holds a Bachelor of Arts with a major in the Classics.

ELIZA CHAPMAN

Eliza Chapman is a research intern at ASPI and the International Cyber Policy Centre. She is currently researching the internet of things, with a focus on industrial control system security. Eliza has a Bachelor of Science degree in Biology from Emmanuel College, Georgia, USA. While spending time abroad, she became particularly interested in Australia–US relations and the implications for current and future security arrangements. Eliza will finish her Masters in International Relations at ANU next year.