CYBER MATURITY IN THE ASIA–PACIFIC REGION 2015

CREATING A REGIONAL CYBER MATURITY METRIC

ACKNOWLEDGEMENTS

The authors would like to thank several colleagues who generously contributed their time and comments to this report. Mr Peter Jennings was integral to the initial design of this project in 2013 and his on-going input, insights and guidance have been invaluable. Special thanks this year again go to Dr Andrew Davies for his assistance devising the quantitative elements of the country weightings and ranking system. We also thank Klée Aiken, Simon Hansen, Roy Birch, Hayley Channer, Stephanie Huang and Zoe Hawkins for their invaluable research assistance.

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 (ICPC) brings together the various Australian Government departments with responsibilities for cyber issues, along with a range of private-sector partners and creative thinkers to assist Australia in creating constructive cyber policies both at home and abroad. The centre aims to facilitate conversations between government, the private sector and academia across the Asia–Pacific region to increase constructive dialogue on cyber issues and do its part to create a common understanding of the issues and possible solutions in cyberspace.

The ICPC has four key aims:

- Lift the level of Australian and Asia–Pacific public understanding and debate on cybersecurity.
- Provide a focus for developing innovative and high-quality public policy on cyber issues.
- Provide a means to hold Track 1.5 and Track 2 dialogue on cyber issues in the Asia–Pacific region.
- Link different levels of government, business and the public in a sustained dialogue on cybersecurity.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various funders, but special mention should go to the Commonwealth Bank, which has been a strong advocate and supporter of our work since the centre's inception.

First published September 2015

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
cyberpolicy.aspi.org.au
www.aspistrategist.org.au
Facebook/ASPI.org
@ASPI_ICPC

CONTENTS

A companion interactive infographic is available at http://cyberpolicy.aspi.org.au.

INTERPOL

FOREWORD:
INNOVATIVE POLICING IN THE DIGITAL WORLD

The internet has created a borderless society, providing unprecedented opportunities to generate wealth and stimulate economies.

An increasing reliance upon the internet has also created unexpected vulnerabilities, with organised crime groups operating across the world able to coordinate complex attacks in a matter of minutes. Cybercrime and cyber-enabled crime are no longer an emerging threat, but the reality of modern crime, and one to which police forces must now adapt.

When it comes to cybercrime, the list of challenges facing communities and governments is daunting. Traditional methods are no longer adequate for the transnational nature of cyberspace, which now requires stronger international collaboration. There are very few crimes which do not rely in some way on the use of the internet to move money, for communication between criminals or for access to victims.

In order to effectively address issues related to multi-jurisdictional cooperation in cybercrime investigations, there is a need for countries to have bilateral, regional and international agreements specifically tailored to meet the requirements of the cyber domain.

Although a global problem, there remains significant differences between countries in both their ability and capacity to address cybercrime. Cybercrime in the Asia–Pacific region accounts for a significant proportion of global cybercrime yet the diversity between countries can be significant. Across the Asia–Pacific region, there are a number of prosperous economies with well-developed cyber ecosystems, and others with developing economies and only rudimentary cyber capabilities at best—often heavily reliant on the support of foreign aid programmes and capacity-building measures. This, and the growing number of people connected to the internet, mean that cybercrime in the Asia–Pacific is likely to continue to increase.

These differences are also reflected in the diverse levels of cybersecurity maturity and also perhaps in terms of prioritising cyber issues. Interdependence is a defining characteristic of the digital world, meaning we are only as strong as our weakest link.

Finally, on the ground, the broad disparities between countries' capabilities and systems make for difficulties in effective law enforcement cooperation on investigations, which can be compounded by language issues amongst parties. Differences in cultural views of what is the acceptable use of the internet can also create tensions.

It was under INTERPOL's vision of connecting police for a safer world that the INTERPOL Global Complex for Innovation (IGCI) in Singapore was created to address the unprecedented challenges facing law enforcement in a digital age.

The IGCI aims to provide a centre of excellence for combating cybercrime, to identify trends, build capacity in cybercrime units and facilitate international cooperation. It will provide a platform for collaboration both on operational matters and policy issues which have implications for the law enforcement community, as well as on the wider cybersecurity debate.

The continued evolution of technology and other developments in the cyber arena, underlines the need to constantly scan and assess the environment and make any necessary adjustments to our strategy for combating cybercrime. IGCI aims to provide this strategic support to its membership.

The underlying driver of all INTERPOL cybercrime initiatives is the recognition of the importance of global harmonisation of skill levels through training; of legal and technical frameworks; and the centralisation of information and expertise.

To help national law enforcement identify and address any shortfalls in their cyber capabilities, the IGCI has launched National Cyber Reviews (NCRs). This initiative gives member countries the possibility to request a review of its legal and technical frameworks in order to better understand strengths and weaknesses, and be able to target efforts of improvement. In this context, reports such as the ASPI Cyber Maturity Metric are invaluable tools for policymakers when assessing broad cyber issues.

Keeping up with technological advancements, and their possible criminal use, is essential to fight cybercrime. Recognising the importance of a multi-stakeholder alliance to address emerging threats, the IGCI brings together specialists from law enforcement, public institutions, the private sector, and academia to leverage their respective expertise and resources for the benefit of law enforcement fighting cybercrime.

Information sharing across sectors is critical and the Cyber Fusion Centre was created in the IGCI to address this need. Using a range of sources, including the private sector, the centre provides real-time monitoring and analysis of threats and malicious internet activity in order to produce intelligence reports and assistance to INTERPOL's member countries. The Digital Forensics Laboratory will be a central contact point for law enforcement in all 190 member countries requiring specialist support.

Whilst dialogue in relation to certain issues relating to cybersecurity may not be progressing as fast as some would like, there are already significant strides being made in international collaborative efforts among law enforcement.

INTERPOL stands ready to support its membership, paving the way for police to address 21st century crime threats.

Noboru Nakatani
Executive Director
INTERPOL Global Complex for Innovation

INTRODUCTION

Online, 2015 has been a significant year for the Asia–Pacific: the internet has played a pivotal and ongoing role in many of the region's political disputes, economic growth spurts and social movements.

Leadership and organisational changes across the region have led to an increased focus on cyber issues and how they are addressed. New organisational bodies have been established, and cyber issues have been lent new ministerial prominence in several countries. Governments are also taking a progressively more active role in trying to bridge the internet connectivity divide between urban and rural areas by expanding internet infrastructure, often with the support of foreign-owned private enterprise. Fixed-line and, perhaps more dramatically, mobile internet networks have expanded access to online services and markets, allowing the region's digital economies to continue to grow.

The potential for social, economic and political change continues to expand as online technology advances and access to the internet grows. This is invigorating and enabling the next generation of technologists and entrepreneurs, but also creates avenues for new forms of crime. To reflect the increasing prominence of financial cybercrime and the need for adequate responses to it, this year's cyber maturity metric includes a standalone assessment criterion on financial cybercrime.

Beyond domestic cyber issues such as cybercrime, governance structures and connectivity is a continually evolving international strategic landscape. While cyber quarrels frequently break out between various state and non-state actors, for the most part traditional geopolitical flashpoints replicated online account for the most significant cyber incidents. This has led militaries to deepen their thinking on cyberspace, prompting to an uptick in recruiting, training and strategic planning.

The Asia–Pacific region continues to be a major source of interest for major and middle powers. Many countries are increasing their region-based capacity-building efforts. While critical to developing cyber maturity, these efforts also underpin a larger observable trend in targeted ideological persuasion and manoeuvring.

As connectivity grows, so does the need for cyber-focused policies, legislation and regulatory frameworks. Governments in increasing numbers are addressing gaps in their domestic arrangements, but all countries still have improvements to make in the adequate formation or implementation of cyber centric mechanisms, frameworks and policies.

GAUGING NATIONAL CYBER MATURITY

To make considered, evidence-based cyber policy assessments in the Asia–Pacific context, robust data and an effective analytical framework are required. The methodology used in this report uses a 'cyber maturity metric' to assess the various facets of states' cyber capabilities.

'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 crime, military organisation, business and digital economic strength, and levels of cyber social awareness. The research base underpinning each of these indicator groups has been collated exclusively from information in the public domain; as such, this report's conclusions are based solely on open-source material.

This report is the second edition of an annual report examining cyber maturity trends across the Asia–Pacific. It analyses the cyber maturity of 20 countries, which make up a wide geographical and economic cross-section of the region.

To gain a more holistic picture of regional developments, this year's maturity metric has expanded to incorporate five additional countries: Vietnam, Laos and Brunei in Southeast Asia, plus New Zealand and Fiji in the South Pacific. With these new additions, this study now assesses the entire Association of Southeast Asian Nations (ASEAN) grouping and seven of the 10 ASEAN dialogue partners.

Using the data from the metric, we have also developed a standalone '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.

2014–15 MATURITY TRENDS

REGIONAL CYBER MATURITY: A GOVERNMENT PERSPECTIVE

In 2015, regional government awareness of cyber threats and opportunities remains uneven. Governments that prioritise the development of coherent cyber policy frameworks understand that those frameworks are necessary for their countries to advance digitally. Others, specifically South Korea and the US, have also been subject to incidents in cyberspace that have critically affected their economic and national security. Those left behind are usually struggling to develop the required infrastructure to open up cyberspace to more of their population, challenging their capacity to develop adequate policy frameworks. However, it's critical that these frameworks are established as cyber infrastructure is developed and not bolted on retrospectively.

GOVERNANCE GROWTH

The trend of growing cyber policy and governance frameworks described in 2014 has continued in 2015, although somewhat slower for most of the region except for some standout countries. South Korea, Singapore and Japan are noteworthy for the breadth of their cyber policy governance frameworks and the effectiveness of their implementation. Those countries and others such as Australia, New Zealand and the US are increasingly centralising the administration of their cyber policy and security under leading departments of government.

In contrast, other states are still working to develop the necessary telecommunications infrastructure to increase digital access for their citizens. These states, including Laos, Cambodia, Papua New Guinea and Fiji, tend to place responsibility for cyber policy and security in the hands of their telecommunications-related agencies. The narrowness of that approach is likely to cause problems down the track when increased exposure to cyber risk without adequate policy frameworks increases their vulnerability to malicious cyber actors and cybercriminals. These states need support from more developed regional partners, but the sensitivity of states' technical cybersecurity capability means that this help is often not forthcoming, or welcomed by those who need it most.

MILITARY USE OF CYBERSPACE

The growing comprehension of cyber threats within regional militaries continues to prompt developments in both the organisation and the cyber capability of those forces. However, specific details of cyber capability, organisation and doctrine remain hidden from public view, making research on this indicator particularly difficult.

North Korea's use of cyber capability against South Korea and the US demonstrates its belief that cyber operations are a useful and low-risk way to project power against its more technologically dependent opponents. In the past year, defectors have reported the significant size of North Korea's offensive cyber forces. The Chinese People's Liberation Army was more forthcoming in 2015 on its perspective on cyberspace as both a threat and

an opportunity, stating its intent to integrate cyber operations into conventional military operations to achieve a competitive edge. The US has also released more information on how it will develop its armed forces to conduct cyber operations.

As awareness of cybersecurity threats grows, more military cybersecurity centres and units are being stood up, including in Indonesia and Japan. However, it isn't clear how well those units have been integrated into the order of battle at the strategic, operational and tactical levels. For some militaries, such as those of Laos and Fiji, that don't rely on digitally enabled capability, cybersecurity is likely to remain a low priority for investment in the near term.

INTERNATIONAL ENGAGEMENT

While online battles between major powers in the region often earn the most headlines, practical, useful engagement on cyber policy and security issues continues for most states below that political level. The effects of the Snowden leaks on international engagement linger in some pockets, but the region is gradually moving on. The ASEAN Regional Forum (ARF) is one example: ARF workshops are providing ongoing opportunities for regional states to pursue a meaningful conflict-prevention agenda.

These types of multilateral gatherings are steered mainly by those states with a high level of cyber maturity. They also often have an agenda to push with those states that haven't yet conclusively taken sides in debates, such as those about privacy protection and multi-stakeholder or state-led models of internet governance. The Asia–Pacific was strongly represented in the 2015 meeting of UNGGE (the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), in which China, Japan, Malaysia and the US participated. The final report of the 2015 UNGGE meeting provides welcome agreement on a selection of voluntary norms, including setting standards against attacks on critical infrastructure and computer emergency response teams (CERTs).

However, the debate over state or multi-stakeholder management of the internet is likely to continue unabated in the Asia–Pacific.

CERT engagement remains a key pathway for regional international engagement, particularly through the Asia-Pacific Computer Emergency Response Team (APCERT), and often between those states that might otherwise typically have strained relationships. CERT engagement is also an opportunity to build the cybersecurity awareness and skills of less developed regional states. This trend can also be seen in cybercrime enforcement cooperation, in which states such as Australia are notably active in supporting the development of regional cybercrime enforcement capacity. As overall regional cyber maturity grows and more states become increasingly capable, it's likely that more states will begin to see the benefits of development assistance to regional partner CERTs and cybercrime centres.

A BUSINESS PERSPECTIVE

The region's economic growth is easing, in large part due to the recent slowdown of the Chinese economy. However, it's expected that during 2015 the Asia–Pacific economy will still grow by 6.7% and the region will still account for one-third of global growth (twice the combined contribution of all other developing regions). This means that investors and businesses will continue to turn to the Asia–Pacific region as a driving force for growth. As home to some of the world's largest and most dynamic economies as well as some of the least developed, the region offers a diverse range of opportunities and challenges in the digital realm. Businesses region-wide are looking to use the digital economy to enhance productivity and diversify their business practices.

China's policy decisions are worthy of note for future market shaping over 2015–16. Beijing is increasing the nationalisation of its ICT base and creating an environment that pushes China to the forefront of technological advancements and advantages its companies over foreign enterprises. This will have significant economic impacts on international companies and investors seeking to capitalise on China's growth in this area.

THE SAFE BETS

On the whole, there's been little shift over the past year in those economies that are capitalising most on the digital economy. Advanced markets in Australia, Singapore, Japan, the US and South Korea, where infrastructure, legislation and regulatory frameworks are mature and allow for confidence in those markets, all offer solid if unspectacular investment opportunities. In Australia, the digital economy accounts for 5% of GDP, making it a bigger contributor to the overall economy than both agriculture and the retail industry. This is in large part due to the surge in mobile phone markets and the take-up of cloud services.

Japan's e-commerce revenue grew by 7.1% in 2014–15, to US$114 billion. With strong support for further expansion in this sector from recent government ICT growth strategies, this means the future is looking bright for further capital investment.

In the recent World Economic Forum *Global Information Technology Report 2015*, Singapore rated number one for its ability to harness ICT. That ranking is further supported by Singapore's ambitious Smart Nation Programme, which seeks to harness the potential of the 'internet of things' into the heart of all it does.

THE UP AND COMERS

Some Asia–Pacific states are seeking to expand aggressively into the new business models that the digital economy makes possible. ICT firms account for 16% of Malaysia's GDP, and Kuala Lumpur has put in place plans and policies, such as its Digital Malaysia Programme, to support and expand this part of the economy out to 2020, making this an attractive market for potential large gains.

Other countries are also 'on the up'. Vietnam is seeing a rapid uptick in tech start-up firms, growth in online shopping and an e-commerce market that's thought to be worth US$4 billion through 2015. This is supported by its National E-Commerce Development Program 2014–2020 and tighter laws that facilitate secure e-transactions.

PLENTY OF ROOM FOR GROWTH

Despite lower oil prices in 2014–15 benefiting the poorest states in the region, such as Cambodia, Laos and the Pacific island countries, there are question marks over the ability of those states to invest and develop adequate infrastructure to harness the potential of the digital economy. These countries are struggling to develop a mature connected platform for their digital economies to take off. However, all is not lost: they could find that not being tied to legacy physical infrastructure and technologies allows them to more easily adopt disruptive business models, in a way that more established economies can't.

This is especially true for internet access via mobile platforms. Mobile phones have provided online access to a new generation in the region, and it's been taken up with gusto. In 2005, only 23 of every 100 inhabitants in the Asia–Pacific had mobile internet access; in 2014, the number had risen 387% to 89 in every 100. Disruptive business models and the technologies that enable them, such as big data analytics, mobile internet, the internet of things and the cloud, are estimated by McKinsey[1] to be worth US$220–625 billion by 2030, which is 4–12% of the region's total projected GDP.

CYBERCRIME

How effectively a country combats financial cybercrime will directly affect business confidence in that jurisdiction. Without reliable and safe online environments in which to do business, companies are unlikely to invest.

Substantial numbers of first-time users are coming online in the Asia–Pacific, but cyber-hygiene awareness and practice are very low, so there are easy pickings for criminals. The rapid take-up of mobile online access creates new opportunities for data and identity theft. Online crime and a lack of harmonised legal structures and capacity are shared challenges in the region.

Severe vulnerabilities result from some countries' high use of unlicensed software, for example, 84% of all software in Indonesia and 81% in Vietnam is pirated, creating opportunities for criminals to exploit. Vietnam is currently the ninth largest global botnet command and control centre (the US ranks first in this category).

The regional situation is compounded by legal frameworks in the region—in many countries, there are very few prosecutions for cybercrime. The Asia–Pacific needs to urgently address shortfalls in combating financial cybercrime if it's to fulfil its undoubted potential.

METHODOLOGY

CHANGES TO THE 2014 METHODOLOGY

Since the publication of the 2014 cyber maturity report, the ICPC has assessed the methodology based on feedback from across the region and made some amendments to the questions and scoring breakdown used to assess states' cyber maturity. The major changes are as follows:

- A question on financial cybercrime enforcement was added to ensure that this critical issue is better reflected in the assessment. States define cybercrime differently, but financial cybercrime is a common issue across the region. Therefore, the question was intentionally limited to financial cybercrime overcome inconsistent definitions.
- States' views on content control and internet freedom weren't considered when scoring Question 1b, which concerns cyber legislation and regulation: *Is there legislation/regulation relating to cyber issues and ISPs? Is it being used?* States were scored only on the scope of cyber-related or specific legislation and the effectiveness of its implementation. Consideration of content control was removed to ensure a consistent approach to scoring this indicator, but shouldn't be interpreted as support for state efforts to impose restrictions on content and access to cyberspace.
- The scoring breakdown (in Appendix 1) was broken down further to provide better definition of the differences between scores.
- 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 UK, included in 2014 as an extra-regional comparator, has been omitted from this year's analysis.

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 with those issues; the state's legislative intent and ability; and 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 regional 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 and ability to engage on cyber issues.

b) Is there legislation/regulation relating to cyber issues and 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 region.

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 region on those issues.

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

The existence of a service to help business 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 question 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 regional states, so this area requires careful consideration before other states seek or agree to engagement.

a) What is the military's role in cyber policy and security?

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 a 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 among 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 or trade development and private-sector investment.

5 Social engagement

a) Is 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 the population has internet connectivity?

The proportion of the state's population with internet connectivity indicates the type of business and personal engagement in cyberspace, the quality of ICT infrastructure and the citizens' trust in digital commerce. This can guide development agencies seeking to build regional economies and businesses wanting to develop trade in the region. This question can also indicate the penetration of fixed-line and wireless networks.

COMPONENTS OF THE METHODOLOGY

This 2015 report builds on the method used in 2014 to assess a country's cyber maturity. It considers five key areas that together encompass whole-of-nation approaches to cyber policy and cybersecurity. These questions were developed in 2014 through a three-stage process:

- Stage 1: Drawing on a range of sources, the ICPC developed an initial draft set of questions.
- Stage 2: The questions 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 rated them on a scale of 1 to 10: 1 was 'not important at all' and 10 was 'extremely important'.

The importance ratings for each question provided by the experts and stakeholder groups 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, again 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 applicable, a comparison with the 2014 research and results.

The overall score for each country was the sum of the scores against each factor weighted by the average 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.

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: WEIGHTINGS ASSIGNED TO EACH CATEGORY

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 penetration

TABLE 2: WEIGHTED SCORES

	Country	Weighted score
1	United States	90.7
2	Japan	85.1
3	South Korea	82.8
4	Singapore	81.8
5	Australia	79.9
6	New Zealand	72.8
7	Malaysia	68.3
8	China	64.0
9	Vietnam	53.6
10	Brunei	51.6
11	India	50.0
12	Thailand	49.1
13	Philippines	46.8
14	Indonesia	46.4
15	Fiji	30.7
16	Myanmar	26.9
17	Laos	23.3
18	Cambodia	20.7
19	Papua New Guinea	20.3
20	North Korea	16.4

TABLE 3: COUNTRY SCORES, BY CATEGORY

	1a	1b	1c	1d	2	3	4a	4b	5a	5b	Total
Australia	7	8	9	8	9	7	7	8	8	9	**79.9**
Brunei	6	6	4	6	5	4	5	5	3	7	**51.6**
Cambodia	3	3	3	2	1	1	2	1	4	1	**20.7**
China	8	7	9	6	5	8	5	6	5	5	**64.0**
Fiji	2	4	4	0	4	2	3	4	3	5	**30.7**
India	7	5	7	4	4	4	5	6	6	2	**50.0**
Indonesia	6	5	5	6	4	5	4	5	4	2	**46.4**
Japan	8	8	9	10	8	7	8	9	8	10	**85.1**
Laos	4	3	3	3	1	1	2	2	2	2	**23.3**
Malaysia	7	7	8	8	6	5	7	7	6	7	**68.3**
Myanmar	3	4	4	3	2	5	1	2	2	1	**26.9**
New Zealand	8	8	6	7	7	5	6	8	9	9	**72.8**
North Korea	3	1	2	0	0	8	0	1	1	1	**16.4**
Papua New Guinea	3	3	3	0	1	2	2	1	5	1	**20.3**
Philippines	5	5	5	3	5	3	4	6	6	5	**46.8**
Singapore	9	8	7	7	7	8	9	9	9	9	**81.8**
South Korea	8	8	7	8	7	9	9	9	9	9	**82.8**
Thailand	6	6	5	5	4	5	3	6	5	4	**49.1**
United States	9	8	9	8	10	10	9	9	10	9	**90.7**
Vietnam	6	7	5	6	6	4	4	6	4	5	**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 are 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, 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) illustrates 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 & 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 & 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, capability, or wider political factors. Major investments and effort will most likely be needed to produce results.

TABLE 4: REGIONAL CYBER ENGAGEMENT OPPORTUNITIES

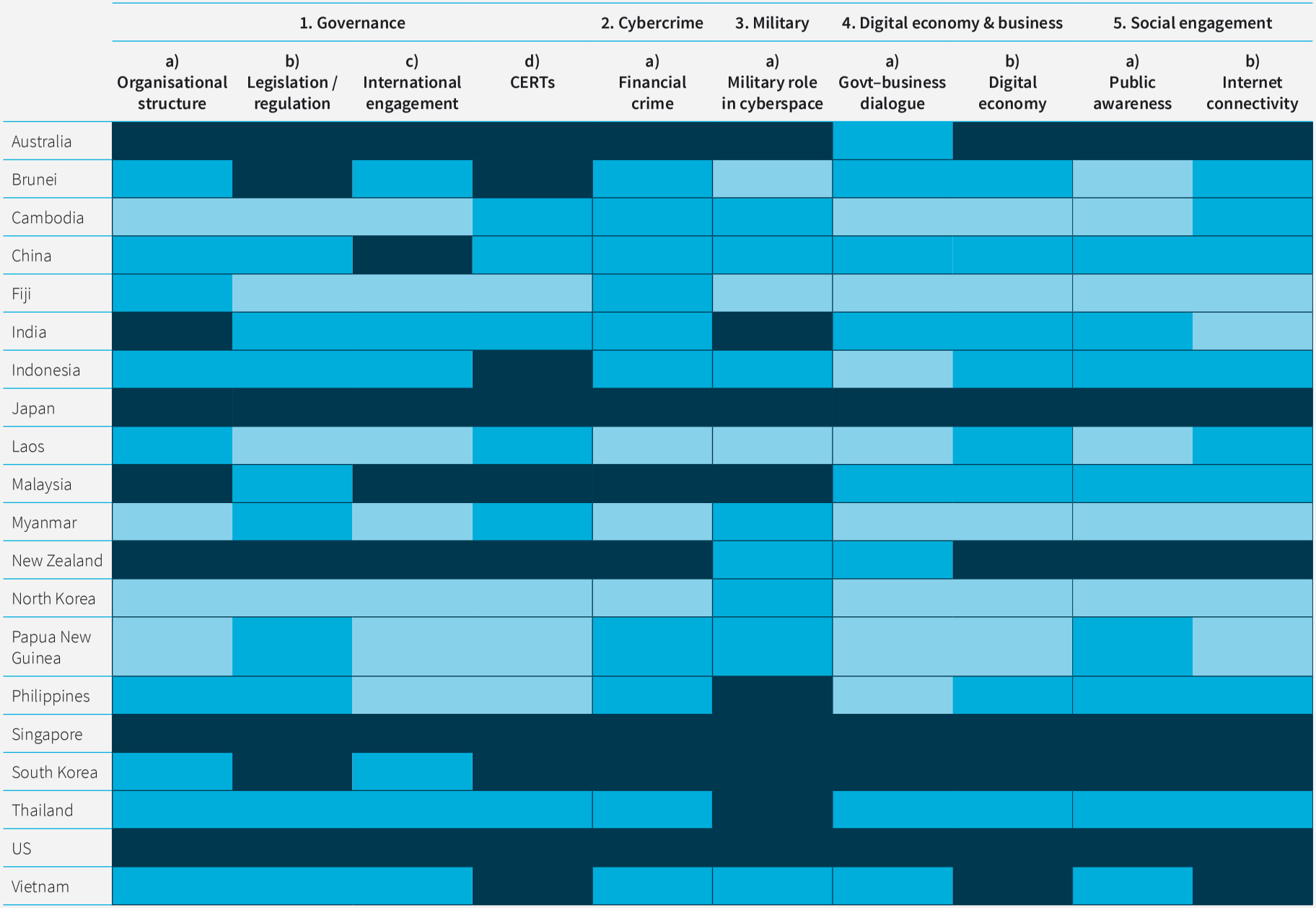


FIGURE 2: ENGAGEMENT OPPORTUNITIES INDICATORS

Indicator	Mature engagement	Engagement & development	Development
1 – GOVERNANCE			
a) What, if any, is the government's organisational structure for cyber matters (including policy, security, critical infrastructure protection, CERTs, crime and consumer protection)? How effectively have they been implemented?	• Country has a transparent organisational structure with a delineated leadership framework. • 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, 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 legislation/regulation relating to cyber issues and ISPs? Is it being used?	• 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 and/or enforcement. • Opportunity to assist in further development of legislation and/ or enforcement capacity-building.	• Lacks proficient legislation, regulation or critical national infrastructure (CNI) 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/ private sector.
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	• Established, internationally engaged CERT. • 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 and/ or anti-financial crime capabilities. • Opportunity to help train officers and build cybercrime enforcement program.

Indicator	Mature engagement	Engagement & development	Development
3 – MILITARY			
a) What is the military's role in cyberspace, policy and security?	• Clear military engagement with cyber issues. • Opportunity for dialogue, joint cyber exercises and information sharing.	• Clear military involvement with cyber issues. • Opportunities to develop and/or further cyber confidence-building measures.	• Little or no opportunity for constructive military-to-military engagement on cyber issues.
4 – BUSINESS			
a) Is there dialogue between government and industry on cyber issues? What is the level/ quality of interaction?	• Strong government–business dialogue/ interaction. • Government responsive to business cyber concerns. • Healthy business environment for ICT investment.	• 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			
a) Is 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 the population has internet connectivity?	• 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.

RESULTS BY COUNTRY

AUSTRALIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	7
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	9
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	8
b) What percentage of the population has internet connectivity?	9

OVERALL ASSESSMENT

Australia continues to improve the political, business and social elements of its cyber maturity, as evidenced by the opening of the Australian Cyber Security Centre in 2014. Australia has a well-established legal framework that continues to be adjusted and augmented in response to contemporary cyber issues, which is actively enforced. The country has sustained its role as a regional leader in multilateral forums on cybersecurity, while deepening interactions with Australian businesses through the expansion of a reciprocal cyber-dialogue. There remains a paucity of coherent national cyber policy with which to guide these developments; however, this will improve if the Australian Government delivers and effectively implements its promised Cyber Strategy.

WEIGHTED SCORE: 79.9

1 GOVERNANCE

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

Australian Government agencies remained highly engaged on cybersecurity issues throughout 2014–15. The long-awaited opening of the Australian Cyber Security Centre occurred in November 2014. At the official opening of the centre, Prime Minister Tony Abbott announced that the government will review Australia's cybersecurity strategy. While the government is engaging with the private sector during the review process, it's yet to be seen what the review will deliver and what changes will be implemented as a result. Australia's score could improve with the release of a new cyber strategy and a more streamlined cyber policy structure to complement the country's operational cyber improvements.

SCORE: 7

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

Australia possesses a very well-developed legal structure relating to cybercrimes, including the *Criminal Code Act 1995*. It has also acceded to the Council of Europe Convention on Cybercrime. In the past 12 months, the government passed the *Enhancing Online Safety for Children Act 2015*, which establishes the role of the Children's eSafety Commissioner and grants new social media takedown powers to the position. The government is also considering the implementation of mandatory data breach notification laws, which would require changes to the *Privacy Act 1988*.

SCORE: 8

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

Australia has a vigorous international engagement program that includes strong multilateral and bilateral engagement on policy, international security, internet governance, CERTs and policing, and plays leadership roles in those areas. In the past year, Australia has held bilateral cyber dialogues with China, Japan and Korea, and co-chaired an ASEAN Regional Forum (ARF) Workshop on Cyber Confidence Building Measures (CBMs) with Malaysia. With Malaysia and Russia, Australia also led the development of the ASEAN Regional Forum Work Plan on Security of and in the Use of ICTs, which underpins the ARF's continued and successful cyber CBM agenda. Australia was a founding member of the Global Forum on Cyber Expertise launched at the 2015 Global Conference on Cyber Space in The Hague. Australia's score for this indicator would improve with the release of an international cyber strategy that publicly and coherently states Australia's standing on key cyber issues.

SCORE: 9

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

CERT Australia is Australia's national CERT, acting as a point of contact between Australian businesses and the Australian Government for cybersecurity threats targeted against critical national infrastructure (CNI) operators and additional systems of national importance. In 2014–15, CERT Australia produced the Cybercrime and Security Survey, which is designed to show how cyber incidents are affecting Australian businesses. CERT Australia remains highly engaged in the region at bilateral and multilateral levels and is an active member of APCERT. CERT Australia also assisted in the delivery of the ARF workshop on cyber CBMs in Kuala Lumpur. Questions remain about how CERT Australia's interaction with private-sector partners will be affected by its co-location in the Australian Cyber Security Centre within an Australian intelligence agency building.

SCORE: 8

2 CYBERCRIME

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

The Australian High Tech Crime Centre, located within the Australian Federal Police (AFP), has responsibility for coordinating approaches to hi-tech crime and supporting efforts to protect Australia's national information infrastructure. The AFP coordinates with many regional partners on cybercrime issues and helps to build capacity in the region, particularly in Southeast Asia and the Pacific islands, where it has helped to establish several hi-tech and cybercrime centres. The AFP prosecutes financial crimes and works in close collaboration with international partners in doing so.

SCORE: 9

3 MILITARY

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

Australia's score remains unchanged from 2014. Australia also still lacks a publicly available strategy or policy document that guides the department's and the ADF's approach to cyber threats. The Defence Minister has indicated publicly that the upcoming Defence White Paper will look to address Defence's future cyber capability and the role it has to play in contributing to the protection of Australia and its critical systems. It also struggles to engage beyond traditional intelligence partners on cybersecurity issues. Australia's score could improve with further clarification of the ADF's roles and responsibilities.

SCORE: 7

4 BUSINESS

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

As a component of its cybersecurity review, the Government has engaged strongly with the business community, including a meeting between the Prime Minister and the chief executives of high-profile Australian companies. Beyond the review, there's sustained two-way dialogue between government and key sectors such as banking, telecommunications and CNI. This effort could be both deepened and widened to incorporate more sectors. The increase in Australia's score also reflects the introduction of the Australian Cybercrime Online Reporting Network and the streamlined cybercrime reporting process now available via the Australian Cyber Security Centre website.

SCORE: 7

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

In 2015, Deloitte Access Economics valued the Australian digital economy at $79 billion, or around 5% of total GDP. The sector now surpasses traditional sectors such as agriculture and the retail industries. Growth in this area is being supported by growing mobile markets and cloud computing. Following on from the launch of the myGov website in 2013, the government launched the Digital Transformation Office in 2015 to drive online service delivery. Australia's score could improve with faster and more readily available internet services and a pronounced effort to foster and support domestic digital innovation, which is often lost to offshore economies.

SCORE: 8

5 SOCIAL

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

There's very strong public awareness of cybersecurity issues in Australia, driven by solid media coverage of cyber threats and cybersafety. An active civil society discussion on cyber issues is driven by universities and think tanks. Private-sector companies are also becoming increasingly involved in awareness raising and end-user education; for example, the AFP is pairing with the Commonwealth Bank to deliver the ThinkUKnow cybersafety campaign. The Australian Government has also established the new position of Children's eSafety Commissioner.

SCORE: 8

b) What percentage of the population has internet connectivity?

84.6% of Australia's population have access to the internet.

SCORE: 9

BRUNEI

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	6
b) Is there legislation/regulation relating to cyber issues or internet service providers (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 on 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?	5
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	3
b) What percentage of the population has internet connectivity?	7

OVERALL ASSESSMENT

Brunei exhibits modest cyber development, but its achievements are undermined by government control, inefficiency and inaction. There are distinct cyber agencies and legislation; however these focus more on controlling opposition to government than policing cybercrime. Brunei does engage with some domestic cybercrime threats but doesn't contribute to the effort at the regional level or take action on the issue of military cyber capabilities. High levels of regulation and government ownership of ISPs limit public awareness of cyber issues in Brunei.

WEIGHTED SCORE: 51.6

1 GOVERNANCE

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

The Government of Brunei has established agencies, centred on the Prime Minister's office, to develop its cyber infrastructure and digital economy, regulate and develop the local ICT industry, enhance the digital delivery of government services and deliver cybersecurity services. This is part of an overarching objective to diversify the Bruneian economy and make government more efficient. Brunei has released several strategies for ICT development, including the 2014 National Broadband Policy and the 2015 Digital Government Strategy. For a small country, Brunei's organisational structure is complex, and its drive to become a regional 'cyber hub' may be impeded by unnecessary bureaucracy.

SCORE: 6

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

Brunei has enacted legislation to regulate cybercrime, copyright infringement, electronic transactions and digital content. It regulates internet content through the *Broadcasting Act*, the *Internet Code of Practice Notification of 2001* and the *Broadcasting Code of Practice Notification 1998*. Content must not be subversive and must align with Brunei's religious values.

SCORE: 6

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

Brunei is relatively active in ASEAN cybersecurity discussions and in various CERT organisations, including APCERT, the Forum of Incident Response and Security Teams (FIRST) and the Organisation of Islamic Cooperation CERT (OIC-CERT), and it has hosted several IMPACT conferences. It's not as active in broader bilateral or multilateral cybersecurity discussions, reducing its score for this category.

SCORE: 4

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

BruCERT was established in May 2004 and currently has 66 staff. It's a member of FIRST, APCERT and OIC-CERT. Brunei's score for this category is reduced because BruCERT doesn't provide significant assistance to other international CERTs.

SCORE: 6

2 CYBERCRIME

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

The Royal Brunei Police Force maintains officers trained in digital forensics in the Commercial Crime Division. While the force is active domestically, Brunei's small contribution to global efforts to counter cybercrime reduces its score.

SCORE: 5

3 MILITARY

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

Brunei's 2011 Defence White Paper listed cyberwarfare as a potential threat to Brunei's national security, particularly to national decision-making and commercial and economic activity. The Defence White Paper noted that, while the Ministry of Defence is not responsible for protecting government or commercial networks, it must protect its own networks from physical attack and cyberattack. However, it's not apparent that the military has taken any steps to implement this guidance.

SCORE: 4

4 BUSINESS

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

Brunei's government has sought to engage the country's private sector in the development of the country's digital economy, primarily through the Brunei Information Technology (BIT) Council. The council, which has representatives from the government and the private sector, is responsible for leading the development of Brunei's ICT infrastructure and digital economy. However, this engagement appears to be mainly government-led and directed. A greater contribution from business to the development of government policy in this area would raise Brunei's score for this category.

SCORE: 5

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

Brunei views cyberspace as a potential source of diversity in an economy dominated by oil and gas production. The 2014 National Broadband Policy seeks to support the growth of Brunei's digital economy, particularly in those areas dependent on high bandwidth. The policy addresses key issues such as accessibility, affordability, quality and usage. While it's promising that the Brunei Government has put in place policy for the development of digital business, there's still a lack of critical mass in the digital economy necessary for Brunei to score higher for this category.

SCORE: 5

5 SOCIAL

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

There's little evidence of significant discussion or debate about cybersecurity and cyber policy in Brunei and criticism of the Brunei Government is highly regulated. The link between the government and the country's two ISPs, which are both publicly owned, may inhibit the development of the national discussion of cyber issues.

SCORE: 3

b) What percentage of the population has internet connectivity?

69% of Bruneians have access to the internet.

SCORE: 7

CAMBODIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	3
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	2
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has internet connectivity?	1

OVERALL ASSESSMENT

Cambodia lacks adequate cybercrime legislation and appears to have neglected the vulnerabilities of cyber technology. Instead, progress and international engagement focus on the development of national ICT infrastructure. There's been a fivefold rise in internet access, but levels of connectivity are still so low as to hamper the establishment of a digital economy. Although steps have been taken to facilitate dialogue between the government and the private sector, the effectiveness of that interaction is yet to be seen. There's an increasing social awareness of cyber issues, although the discussion mostly highlights concerns about the abuse of legislative power.

WEIGHTED SCORE: 20.7

1 GOVERNANCE

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

Cambodia's cyber governance structures reflect the low levels of internet penetration in the country. The National ICT Development Authority and the Ministry of Posts and Telecommunications are responsible for the development of the necessary infrastructure and the regulation of the telecommunications industry through the Telecommunications Regulator of Cambodia. The narrow focus of governance structures means that Cambodia's score for this indicator remains low.

SCORE: 3

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

Cambodia doesn't have consistent legal frameworks for cybersecurity, cyber policy and cybercrime. As noted in 2014, there's some awareness of the need for cybercrime legislation, but Cambodia's lack of action on this front reduces its score significantly.

SCORE: 3

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

Cambodia's international engagement on cyber issues is generally limited to development assistance for its ICT sector and CERT capability. Without broader engagement on regional and global cyber policy and security issues, Cambodia's score for this indicator will not improve.

SCORE: 3

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

CamCERT's effectiveness is difficult to ascertain from available sources, especially as it isn't an operational member of APCERT. Further evidence of the capacity of CamCERT to respond to cyber incidents would be needed for Cambodia to score higher.

SCORE: 2

2 CYBERCRIME

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

It's believed that the National Police maintains some cybercrime investigative capacity, but the lack of a cybercrime law is likely to inhibit the force's effectiveness.

SCORE: 1

3 MILITARY

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

It isn't apparent that the Cambodian military has significant awareness of cyber threats or the capacity to defend against them. The military's limited reliance on networked capabilities means that cyber threats are not a priority for mitigation.

SCORE: 1

4 BUSINESS

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

The establishment of the Information and Communications Technology Federation is a positive step for greater private–public dialogue on cyber issues, but there remains a lack of evidence of consistent dialogue or influence from the private sector on public cyber policy.

SCORE: 2

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

The lack of connectivity in Cambodia significantly hampers the development of a digital economy in the country. Government efforts to develop ICT infrastructure and cybercrime legislation may provide the basis for growth in the future, but the slow pace of these developments makes this is a long-term prospect.

SCORE: 1

5 SOCIAL

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

There appears to be increasing awareness of some cybersecurity issues in local media, which report on cyber incidents affecting government websites and opposition to the draft cybercrime legislation based on fears that it will be misused to control content and suppress online dissent. Cambodian opposition parties are also increasingly using online media to build support for their policies before elections, undermining the ruling Cambodian People's Party's privileged access to traditional media.

SCORE: 4

b) What percentage of the population has internet connectivity?

The Telecommunications Regulator of Cambodia has reported that 3.8 million Cambodians, about 25% of the population, has access to the internet through fixed-line or mobile subscriptions. However, the World Bank estimates that only 9% of the population have access to the internet.

SCORE: 1

CHINA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	8
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	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?	5
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has internet connectivity?	5

OVERALL ASSESSMENT

China has improved its cyber maturity by clarifying and centralising the coordination of government cyber agencies and continuing to produce relevant cyber legislation. Cybercrime is actively but inconsistently addressed, and there's a notable focus on content control. China has articulated a deepened understanding of the cyber military threat but has failed to translate this into a tangible policy or program. There's been greater interaction between the public and private sectors, but the overall development of a Chinese digital economy is held back by poor rural infrastructure and a lack of coherent strategy. Censorship continues to be a fundamental barrier to public debate and to overall cyber maturity in China.

WEIGHTED SCORE: 64.0

1 GOVERNANCE

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

China has begun to implement action that supports the principle of safeguarding cyberspace sovereignty and security in all cyber issues, including legislation and international relations. Its move to centralise cyber policymaking appears to have significantly improved its coordination of cyber governance, policy and implementation. China established the Central Group for Cyberspace Affairs, chaired by President Xi Jinping, in early 2014. The group's director, Lu Wei, is also head of the Cyberspace Administration of China, which replaced the State Internet Information Office. The Cyberspace Administration leads the development and implementation of cyber policy, including the new Cyber Security Law, across the Chinese Government and coordinates with other government agencies with cyber responsibilities and telecommunications providers. This high-level centralisation of policy authority indicates the importance of cybersecurity policy to the Chinese Government. The new National Security Law and Cyber Security Law reflect a coordinated approach to cyber policy issues, improving China's score significantly.

SCORE: 8

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

China's cyber legislation has been further extended in 2015, notably through the National Security Law, which includes references to national internet sovereignty and a requirement to achieve security and control in ICT. Under the Cyber Security Law, the government will establish national security standards for information networks, more strictly enforce real name registration, provide for greater investment in Chinese cybersecurity firms and mandate a Cyberspace Administration of China review of key telecommunication companies. However, this legislation may reduce the ability of foreign ICT firms to invest in China.

SCORE: 7

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

China remains at the forefront of international cybersecurity discussions, providing the counterpoint to US-led efforts in this area. China's efforts are in pursuit of the principle that all states should have sovereign control over cyberspace within their borders, including control of physical infrastructure and content. In January 2015, China, Russia, Kazakhstan, Tajikistan, Uzbekistan and Kyrgyzstan submitted a revised version of their International Code of Conduct for Information Security to the UN, with a request that it be circulated to the 69th session of the General Assembly. The draft was little altered from a 2011 draft, and failed to mention developments such as the 2013 UNGGE report's agreement that international law applies to cyberspace. China is also a member of the 2015 UNGGE, which has reached a consensus on a selection of voluntary norms of behaviour for cyberspace. China is working consistently to achieve its vision for state control of cyberspace through the UN, the International Telecommunication Union (ITU) and other multilateral and bilateral forums.

SCORE: 9

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

CNCERT's score from 2014 remains unchanged, as no available evidence indicates any significant improvement in 2015. China's score would improve if CNCERT were more active internationally in providing assistance to smaller CERTs and in international CERT engagement.

SCORE: 6

2 CYBERCRIME

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

In 2015, there's been increasing evidence of Chinese police enforcing financial cybercrime laws; however, they continue to focus more on enforcing content control than on combating financial cybercrime. It's been suggested that Chinese police turn a blind eye to cybercriminals if the criminals' targets are in foreign countries. China's score would improve with more consistent enforcement of financial cybercrime legislation and improved cooperation with foreign law enforcement partners.

SCORE: 5

3 MILITARY

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

China's Military Strategy, released in May 2015, names cyberspace as a critical security domain, alongside the sea, space and nuclear domains. It outlines a requirement to improve the People's Liberation Army's (PLA's) use of ICT to support warfare, and notes the need for better cyberforces to overcome cyber threats and focus on winning 'informationised' local wars. This indicates that the PLA is aware of the need to adjust its approach to cyber operations and improve its abilities and capabilities in this area. However, there's no indication that the PLA has begun to rationalise its myriad of cyber bureaus in an effort to better coordinate their actions.

SCORE: 8

4 BUSINESS

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

China's score for this category has improved in the light of the government's Internet Plus strategy, announced at the National People's Conference in March 2015. The strategy seeks to foster new industries and business development supported by cyberspace, including e-commerce and online financial services, to improve innovation in China. This is also likely to favour Chinese ICT firms' growth at the expense of foreign ICT companies' investments in China.

SCORE: 5

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

While the digital economy in China continues to grow, China's score has been reduced because it lacked clear government policy until the Internet Plus strategy was announced in March. Evidence of the implementation of this plan will probably improve China's score in future.

SCORE: 6

5 SOCIAL

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

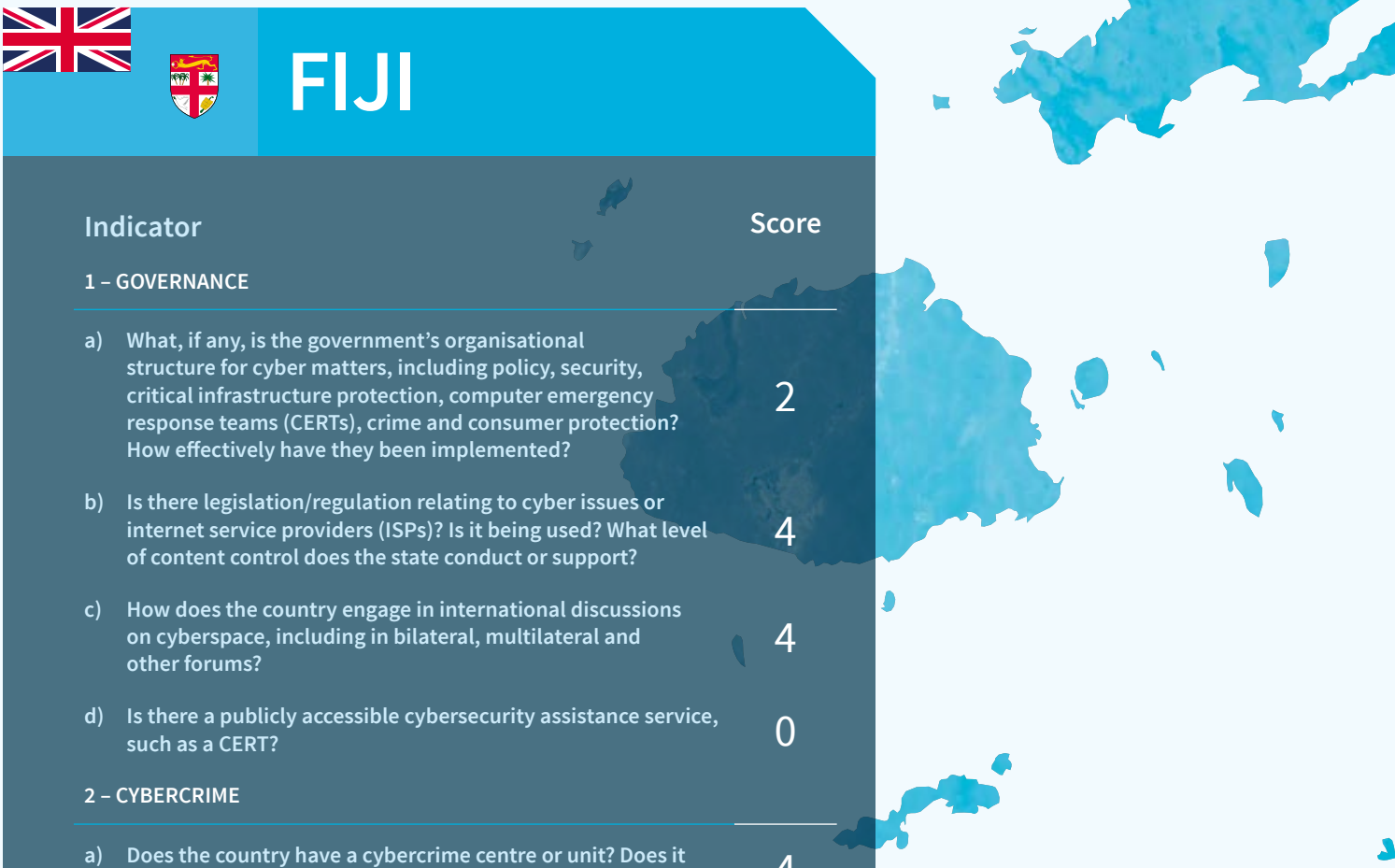
Beijing backed down on its policy requiring the pre-installation of the Green Dam / Youth Escort internet filter on Chinese computers after pressure from industry and civil society. This indicates the government's increasing awareness of the role of cyberspace in maintaining Chinese citizens' approval for its actions. The government also sought comment on its new cybersecurity legislation. China has the world's largest internet population, but self-censorship and official censorship limit the discussion of cybersecurity issues to a significant extent.

SCORE: 5

b) What percentage of the population has internet connectivity?

The China Internet Network Information Centre's 35th *China internet development statistics report* states that 47.9% of Chinese people have access to the internet; of those, 80% use a mobile phone or tablet to connect.[2] The World Bank estimates that 49% of the population has access to the internet.

SCORE: 5



FIJI

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	2
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	2
4 – BUSINESS	
a) Is there dialogue between government and industry on 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?	4
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	3
b) What percentage of the population has internet connectivity?	5

OVERALL ASSESSMENT

The Fijian Government's approach to cyberspace lacks organisational structure and adequate regulation, focusing instead on service delivery. Fiji has a dedicated cybercrime unit, but it has limited response capacity and fails to engage with regional efforts. Similarly, while the government is involved with international cyber forums, Fiji's participation continues to be at a low level. The government ran an initial consultation with the private sector on the development of cyber principles, but that process was inconsistent and lacked follow-through. Fiji acknowledges the potential business benefits of cyberspace, but more clarity and direction are needed to ensure the development of the country's digital economy.

WEIGHTED SCORE: 30.7

1 GOVERNANCE

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

Fiji has no apparent organisational structure or policy for cyber issues. In 2011, it commissioned the Cyber Security Working Group, a public–private partnership, to begin work towards a national strategy, policy and legislation on cyber issues, but there's no evidence that this has been done. The Ministry of Defence, National Security and Immigration appears to be the lead agency for cybersecurity.

SCORE: 2

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

Some relevant legislation exists, such as the *Telecommunications Act 1999*, but there appears to have been little progress on cyber legislation in the past decade. The military government has issued a series of decrees that include requirements for all telephone and internet users to register their personal details with their service providers, and included a computer offences division of the 2009 Crimes Decree. Fiji demonstrates some awareness of the need for legislation and regulation, but hasn't achieved enough to score higher in this category.

SCORE: 4

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

Fiji participates in some bilateral and multilateral international cyber discussions, including the Pacific Islands Telecommunications Association and the Commonwealth Telecommunications Organisation, and has hosted some technical workshops for regional countries. Fiji's score reflects the low level and narrowness of its international engagement on cyber issues.

SCORE: 4

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

Fiji doesn't have an officially recognised CERT. PacCERT, based at University of the South Pacific in Suva, ceased operation in 2014, leaving Fiji and many other Pacific island nations without a CERT capability.

SCORE: 0

2 CYBERCRIME

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

The Fijian Police Cyber Crime Unit, established in 2000, is part of the Criminal Investigation Department Headquarters in Suva. It enforces the computer crime offences included in the 2009 Crimes Decree, the Anti-Money Laundering Guidelines and the Commerce Decree. The unit works with the Financial Intelligence Unit, and has reportedly worked with foreign partners to address money laundering in the country. In February 2015, the Australian Federal Police provided additional digital forensics equipment. Fiji's score reflects the limited response capability of the Fiji Police Force in this area and its lack of participation in significant international cybercrime cooperation.

SCORE: 4

3 MILITARY

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

While the Ministry of Defence, National Security and Immigration appears to play a leading role in cybersecurity policy, there's little apparent acknowledgement of the cyber threat to the Fijian military or action to mitigate it.

SCORE: 2

4 BUSINESS

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

The Fijian Government appears to have sought private-sector input from the beginning of its development of cyber policy; however, the subsequent lack of action on this front indicates that the dialogue has been neither high quality nor consistent.

SCORE: 3

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

Fiji is yet to reap the benefits of the digital economy, but there are some indications that the government is aware of the potential rewards. Digital mapping of Fiji's principal export crop, sugar cane, has been completed, and a GIS portal has been launched in an effort to make this critical industry more efficient. Mobile technology has also been noted as a critical requirement for Fiji's development. Fiji's score would be improved if there were a coherent government strategy to develop the backbone infrastructure required for the growth of digital commerce in Fiji.

SCORE: 4

5 SOCIAL

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

The high cost of entry for access to cyberspace and government censorship mean that there's little discussion of cybersecurity and cyber policy issues in Fiji's national media or online. Media reporting is generally limited to cybercrime and cyberbullying.

SCORE: 3

b) What percentage of the population has internet connectivity?

The World Bank estimates that 42% of Fijians have access to the internet.

SCORE: 5

INDIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	7
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	7
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?	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 on 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) Is there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of the population has internet connectivity?	2

OVERALL ASSESSMENT

Although India has shown a strong awareness of cybersecurity issues, policy ambiguity and inaction have left it without a fully implemented government cyber strategy. Indian cyber legislation is out of date and poorly implemented. Cybercrime facilities have reportedly been used as instruments of state censorship, and a promised military Cyber Command has not been established. Government interaction with the private sector on cyberspace has improved, and there's been a concerted effort to develop India's digital economy. Unfortunately, levels of internet penetration remain very low. Progress on national infrastructure is needed to improve Indian cyber maturity.

WEIGHTED SCORE: 50.0

1 GOVERNANCE

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

The Indian Government's efforts to confront cybersecurity threats appear to have slowed or stalled. The 2013 National Cyber Security Policy was notably vague on measures to deal with cyber threats, and a new policy is not known to be in development. Some measures have been implemented, including government approval to establish the National Cyber Coordination Centre. However, approval was given only in April 2015, despite in-principle approval being granted in May 2013. Without evidence of strong government action to create the structures necessary to manage cyber threats, India's score is likely to decline.

SCORE: 7

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

India hasn't significantly changed its legislative and regulative framework for cybersecurity or cybercrime in 2015. It has struggled to effectively implement the legislation it has, and failed to update legislation to meet the needs of digital commerce. The absence of specific legislation for digital commerce means that business is governed by myriad pieces of legislation, including the *Penal Code 1860* and the *Contract Act 1872*. Significant work is required to update and simplify legislation to enable the growth of digital commerce, while also clearly defining cybercrime so that the law is more readily enforceable.

SCORE: 5

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

India engages in bilateral and multilateral discussions on cyber policy and security issues with a wide group of states and multilateral organisations, including the European Union, Japan, Australia and ASEAN, and is a founding member of the Global Forum on Cyber Expertise. It also provides assistance to some regional countries to further develop their cybersecurity capability. India hosted an ASEAN–India Cyber Security Conference in January 2015, at which the Ministry of External Affairs Secretary (East) said that India believes that liberty, freedom of expression and the rule of law apply to cyberspace. India is emerging as a regional leader in cyber policy discussions, and further work in this direction will improve its score for this category.

SCORE: 7

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

India established CERT-IN in 2004. However, the agency doesn't appear to have robust response capabilities or the ability to retain the staff needed to improve its capability.

SCORE: 4

2 CYBERCRIME

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

India has 21 anti-cybercrime cells across the country, but their ability to police domestic cybercrime appears limited by the legislative framework. *The Information Technology Act 2000* is the primary legislative instrument for the criminalisation of cyber activities; however, the Home Minister has called for an overhaul in the wake of the suspension of section 66A of the Act by the Supreme Court in March 2015 as unconstitutional. That section, which makes it an offence to send offensive or menacing information from a computer, had reportedly been misused by police to arrest people for critical social media commentary on social and political issues. India is aware of the issue of cybercrime, but needs to do more to develop its own response and to assist regional countries to respond to earn a higher score for this category.

SCORE: 4

3 MILITARY

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

The Indian military is aware of cyber threats and has previously announced plans to establish a tri-service Cyber Command to address them, but there's no evidence that this has occurred. India's score reflects the sustained sluggishness of the military's response to 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 Indian Government understands the critical role of the private sector in developing the country's ICT infrastructure and digital economy. Various public–private bodies, including the Joint Working Group on Cyber Security and the Joint Committee on International Cooperation and Advocacy, are conduits for public–private cooperation on cybersecurity issues, but engagement appears to be narrow. India's score would improve if the government were to engage with a broader cross-section of the private sector.

SCORE: 5

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

India's digital economy is growing and is expected to be worth around US$22 billion in 2015.[3] The Digital India Program launched in August 2014 is the government's strategy to take advantage of the digital economy to grow the Indian economy as a whole. The program focuses mainly on improving access to the internet to grow e-commerce and improve access to government services online. India's score reflects the growth of this sector and the government's acknowledgement of its importance, and will improve if the program is implemented.

SCORE: 6

5 SOCIAL

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

Public debate of cybersecurity issues, primarily on government's role in managing content, continues in India. The public, media and think tanks are increasingly active in discussions of cyber issues, which mainly concern domestic legal issues and the response of the Indian Government to cybersecurity threats. More discussion of wider topics, particularly the international security aspects of cyber policy, would raise India's score for this category.

SCORE: 6

b) What percentage of the population has internet connectivity?

According to World Bank estimates, internet access in India increased from 15% in 2014 to 18% in 2015, demonstrating India's continued problems with the rollout of the infrastructure needed to enable more widespread access.

SCORE: 2

INDONESIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	6
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	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?	4
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has internet connectivity?	2

OVERALL ASSESSMENT

Indonesia has delivered on its promise of a National Cyber Agency—a notable improvement in organisational structure—and new legislation to address cybercrime is under development. Indonesia continues to engage internationally with technical and policing forums, combating cybercrime through collaboration with regional partners in addition to active domestic efforts. The Indonesian Ministry of Defence is playing an active role in cyberspace, addressing areas of cyber strategy, security and offensive capabilities. However, low government–private sector interaction, lack of government initiatives and insufficient telecommunications infrastructure mean that Indonesia is failing to capitalise on the enormous potential of its digital economy.

WEIGHTED SCORE: 46.4

1 GOVERNANCE

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

In January 2015, the Indonesian Government announced that it would form the National Cyber Agency. The agency will aim to coordinate Indonesia's cyber strategies across defence, industry and finance, working with the private and public sectors. It's reported that the new centre is slated for launch in 2016 and will report directly to President Joko Widodo. The Ministry of Defence has also formed a Cyber Operations Centre; announced last year, the centre is believed to be under development. Indonesia still lacks key documents to guide its approach to cyber issues, such as a national cybersecurity strategy.

SCORE: 6

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

The *Electronic Information and Transactions Act 2008* is Indonesia's central law for cyber issues, with provisions for e-commerce, cybercrime and electronic signatures. Indonesia has no stand-alone privacy legislation, but the Act does contain small references to privacy online. A draft *Computer Crimes Act* and *Data Protection Act* are working their way through the Indonesian legislature.

SCORE: 5

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

Indonesia engages in several, mainly regional, multilateral technical and policing gatherings, including APCERT, ASEAN, ASEANPOL and ITU-IMPACT. It has engaged with Japan via ASEAN and bilaterally on some cyber policy and strategic issues. The launch of Indonesia's National Cyber Agency should help to diversify its international engagement beyond technical and crime conferences, exchanges and drills.

SCORE: 5

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

Indonesia has several CERTs and critical security incident response teams (CSIRTs) in both government and the private sector. The Indonesia Security Incident Response Team of the Internet Infrastructure Coordination Center (ID-SIRTII/CC) is Indonesia's national incident response team. It's the point of contact for domestic and international CERTs and is a member of FIRST, APCERT and OIC-CERT. ID-SIRTII/CC is very engaged in regional drills, workshops and meetings and runs a strong domestic program of training workshops for government and private sector ICT workers.

SCORE: 6

2 CYBERCRIME

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

The Sub-Directorate of Information Technology and Cybercrime within the Indonesian National Police is one of the key bodies fighting online crime. The Cyber Crime Investigation Centre established at police headquarters in Jakarta also has offices in Bali and Medan. Indonesia is reasonably active in prosecuting financial crimes and collaborates with international partners in doing so.

SCORE: 4

3 MILITARY

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

Indonesia's Cyber Operations Centre is located at the Ministry of Defence headquarters in Pondok Labu, South Jakarta. It's designed to pre-empt and prevent intrusions, conduct threat analyses and perform recovery actions. A cyberdefence taskforce within the Indonesian Armed Forces is expected to help draft a new cybersecurity strategy. The Indonesian army and navy have dedicated cyber command centres, and the army has signed an agreement with Institut Teknologi Del to develop a cyberdefence and warfare centre that will teach offensive and defensive techniques. While the Indonesian Armed Forces have demonstrated an awareness of cyber threats, its approach appears disjointed, lowering Indonesia's score for this indicator.

SCORE: 5

4 BUSINESS

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

A limited dialogue takes place between the government and industry on cyber issues. It's mainly carried out through ID-SIRTII/CC and policing links to large banks. One of the explicit goals of the new National Cyber Agency will be to improve coordination with industry.

SCORE: 4

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

Indonesia has the potential to foster an impressive digital economy. It possesses many of the same characteristics as other countries in its near neighbourhood, including a young, tech-savvy population. The government is reportedly discussing incentives with local e-commerce companies such as Tokopedia on an ad hoc basis, but it appears that there's no wider strategy beyond that. The sluggish rollout of telecommunications infrastructure compared to mobile network demand is also restricting market access and stifling the growth of e-commerce.

SCORE: 5

5 SOCIAL

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

The Indonesian Government is trying to raise the very low level of public awareness of cyber and information security issues through events such as the National Internet Security Day. There's a solid coverage of cyber issues in the media, mainly about beefing up Indonesia's defences and capabilities vis-à-vis other countries in the near neighbourhood.

SCORE: 4

b) What percentage of the population has internet connectivity?

Indonesia's internet penetration level sits at 18%. The government is trying to boost connectivity, providing inducements to telecommunications companies to expand their physical infrastructure. Telkom Indonesia is rapidly rolling out its new fixed broadband network to around 36,000 premises per day; this work and improved mobile internet capacity will boost access considerably.

SCORE: 2

JAPAN

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	8
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	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 on 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) Is there public awareness, debate and media coverage of cyber issues?	8
b) What percentage of the population has internet connectivity?	10

OVERALL ASSESSMENT

The Japanese Government has a comprehensive, cross-departmental approach to cyber policy. Increased authority for government cyber agencies and the introduction of new cyber legislation speak to a continued and concerted rise in Japanese cyber maturity. Japan continues to be highly engaged in international cyber dialogue and actively enforces cybercrime regulations domestically. The Japan Self-Defense Forces have dedicated cyber bodies that focus on the identification and mitigation of national network vulnerabilities. The government is vigorously facilitating the growth of the Japanese digital economy, and public commentary reveals a high level of cyber awareness.

WEIGHTED SCORE: 85.1

1 GOVERNANCE

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

This year, the Japanese Government reformed the Information Security Policy Council to create the Cybersecurity Strategy Headquarters. Members of the headquarters include the Foreign, Defense, Internal Affairs and Trade ministers, the chairman of the National Public Safety Commission and others deemed appropriate by the Prime Minister. The government also strengthened the legal authority of the new National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which acts as a secretariat to the Cybersecurity Strategy HQ and as a 'control tower' for implementation. The NISC is finalising the latest version of Japan's national Cybersecurity Strategy. These changes bolster an already impressive organisational arrangement and suite of policies.

SCORE: 8

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

The Japanese Government adopted the *Cybersecurity Basic Act* in November 2014. The Act outlines the roles and responsibilities of government in protecting Japan online, including uniform standards for government and new measures at local and national levels. It lays out voluntary standards for cybersecurity firms and companies that run critical infrastructure and compels them to cooperate with government. The Act also formed the legal basis for the reformation of the Information Security Policy Council into the Cybersecurity Strategy HQ and, through a supplemental provision, granted the NISC extra powers and legal authority. The Financial Services Agency has also released new guidelines based on the Basic Act for financial institutions. The agency has the right to exercise punitive power against banks if they fail to meet the minimum standards outlined in the new guidelines.

SCORE: 8

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

Japan engages in a very strong multi-layered program of international engagement in the technical, policing, policy and legislative realms and has produced and shared publicly an International Strategy on Cyber Security. It engages in high-level bilateral discussions on cyber issues with a large number of partners across the region and the world. Japan is very active in regional multilateral forums. It scores highly for this indicator, as it has a very impressive history of delivering capacity-building efforts on the ground, both though ASEAN and via direct bilateral arrangements.

SCORE: 9

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

The Japan Computer Emergence Response Team Coordination Centre (JPCERT/CC) acts as a 'CSIRT of CSIRTs' in the Japanese community, coordinating with government agencies, network service providers, security vendors and industry associations. It produces early warning information for the Japanese Government and CNI operators. Japan conducts an impressive range of workshops, seminars and training sessions domestically and internationally. JPCERT/CC is one of its key vehicles to build capacity in the region, working closely with counterpart CERTs/CSIRTs. JPCERT/CC is one of the founders of APCERT and carries out secretariat functions for the organisation. JPCERT/CC also created the TSUBAME packet traffic monitoring system, which now helps to promote collaboration across the region and improve the sharing of threat information.

SCORE: 10

2 CYBERCRIME

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

In 2004, the National Police Agency created the Cybercrime Division to help prevent and respond to cybercrimes. The division coordinates investigations by local police and works with industry and foreign police forces to improve outcomes. The National Police Agency established the High-Tech Crime Technology Division in 1999 and has since installed high-tech crime technology divisions in each prefectural information communications department to improve the quality of information gathered, reduce response times and boost outcomes. Japan is a signatory to the Council of Europe Convention on Cybercrime.

SCORE: 8

3 MILITARY

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

The Ministry of Defense includes the new Cyber Defense Unit, whose responsibilities include monitoring the ministry's and the Japan Self-Defense Forces' networks for intrusions and collecting and analysing threat data. The Cyber Defense Council, also within the Ministry of Defense, was created as a means to facilitate collaboration between the ministry, the armed forces and private-sector defence contractors and suppliers to tackle defence-specific threats.

SCORE: 7

4 BUSINESS

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

Most Japanese agencies with cyber responsibilities have relatively strong industry engagement programs. They include the NISC, JPCERT/CC, the Ministry of Defense and the National Police Agency. This engagement is generally two-way and vitally important for raising Japan's overall cyber maturity, as understanding and awareness within the private sector are still lacking compared to other developed countries of comparable size.

SCORE: 8

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

In 2014, e-commerce in Japan grew by 7.1% to reach a market size of US$114 billion.[4] Japan uses several strategies to nurture 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 ICT Nation, the Ministry of Internal Affairs and Communications White Paper on ICT, and the Smart Japan ICT Strategy. Japan has a strong level of awareness about the challenges that face a more developed digital economy and is working to address them through forums such as the Council on ICT Strategy and Policy for Growth.

SCORE: 9

5 SOCIAL

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

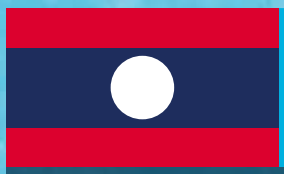
Awareness of cybersecurity issues is very high among the public following several high-profile data breaches, including a hack of the national pension service. Media attention has also focused strongly on cyber issues in the lead-up to the Tokyo 2020 Olympic Games. Several government branches run cyber hygiene awareness campaigns, including Cyber Clean Day and Information Security Awareness Month. Universities and non-government research institutes provide high-level commentary on cyber issues and help to raise awareness and knowledge.

SCORE: 8

b) What percentage of the population has internet connectivity?

91% of the Japanese population is online. This is an increase of 12% since 2012, and the highest internet penetration rate in the region.

SCORE: 10



LAOS

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	4
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	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 on 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?	2
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of the population has internet connectivity?	2

OVERALL ASSESSMENT

Laos shows signs of improved cyber maturity, but that development will be contingent on the delivery of new policy and the implementation of legislation. The country has specific legislation and diversified government agencies dedicated to a range of cyber issues, but there's little evidence of successful implementation. This is reflected in the absence of a cybercrime agency to enforce regulations and in the military's apparent inexperience with cyber threats. A higher score could be achieved through greater engagement with international partners and the private sector, as well as through increasing internet penetration, which remains very low.

WEIGHTED SCORE: 23.3

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 is the main Laotian agency with control of ICT issues. It publicises and disseminates policies and strategic plans, regulations and laws on the management of information on the internet. The Lao National Internet Centre within the ministry has responsibility for LaoCERT and manages the .la top-level domain. It appears that LaoCERT plays a significant coordinating role on a wide range of technical and policy cyber issues, and is heavily involved in the drafting of Laos's cybercrime laws. The National Authority of Science and Technology also has some responsibility for formulating ICT policies and strategies and manages the implementation of the e-government system. The Defence Ministry coordinates responses to criminal cases that threaten 'national stability'. Laos is now developing its National Cyber Security Policy, and its amended Law on Telecommunication clearly defines which agencies have responsibility for various cyber issues. Laos's score for this indicator will improve with the further implementation and finalisation of its cyber strategies and initiatives.

SCORE: 4

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

In 2011–12, Laos introduced several cyber-related laws, including the *Telecommunication Law No. 25, E-Transaction Law*, and has modified elements of its criminal law to encompass online crimes. It's now drafting a critical infrastructure protection law and a stand-alone cybercrime law; consumer and data protection laws are also under consideration. Many of Laos's existing laws are related to the control and monitoring of the internet, and there's little evidence of meaningful implementation of cyber-specific legislation. In late 2014, Prime Minister Thongsing Thammavong signed a 28-point Decree on Information Management on the Internet, which further strengthens government control over internet content. An updated cybercrime law drafted by LaoCERT was passed by the National Assembly in July 2015.

SCORE: 3

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

The bulk of Laos's international engagement involves technical cooperation and the acceptance of foreign-delivered capacity-building efforts. It has held a handful of low-level meetings on cyber cooperation, mainly with neighbouring countries such as Vietnam, Thailand and China. The Laotian Ministry of State Security accepted a donation of 171 computers from the Chinese Government in 2013, and in 2014 the countries' two leaders pledged to work together on cybercrime issues. Laos is a member of ITU IMPACT.

SCORE: 3

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

The Lao Computer Emergency Response team (LaoCERT) was formally established in February 2012, and initial on-boarding training was provided to staff members a year later. LaoCERT continues to upskill its staff with the assistance of other national CERTs and the ITU. It's beginning to play a greater role in incident handling, dealing with a small number of phishing sites and website defacements in 2014–15. LaoCERT serves as the government's coordinator on broader cybersecurity issues and is playing a role in the drafting of new cybercrime laws. LaoCERT joined APCERT in 2014 and frequently attends regional workshops and drills run by APCERT, ASEAN and the ITU.

SCORE: 3

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 centre or any significant online crime fighting capacity. It has taken part in several ASEAN senior officials meetings on transnational crime that have included cybercrime components and has signed a joint anti-crime statement with Vietnam that covers cybercrime.

SCORE: 1

3 MILITARY

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

The Lao military and Ministry of National Defence appear to have limited understanding of cybersecurity threats. In certain government documents, the military has been assigned responsibility for coordinating responses to criminal cases that threaten 'national stability', but there's a lack of open-source literature to demonstrate that this responsibility has been carried out in any way, or that the military has the capacity to do so.

SCORE: 1

4 BUSINESS

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

The Information, Culture and Tourism Ministry is responsible for coordinating with industry to promote internet usage and assist users. The Director General of the Planning and Cooperation Department of the Ministry of Posts and Telecommunications, Mr Sith Xaphakdy, has spoken about the power of ICT as a driver of socioeconomic development. Dialogue between industry and government takes place through the Lao ICT Commerce Association, which sits under the Ministry of Posts and Telecommunications and the Ministry of Science and Technology. The association helps to provide strategic direction in ICT policy development and to promote public–private partnerships.

SCORE: 2

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

In partnership with foreign aid organisations, Laos developed and passed e-commerce legislation in 2012, but evidence of solid implementation is elusive. The business environment is often also constrained by contradictory and unclear regulations and registration requirements, although the government has taken steps to try to rectify this in the lead-up to the implementation of the ASEAN Economic Community in 2015.

SCORE: 2

5 SOCIAL

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

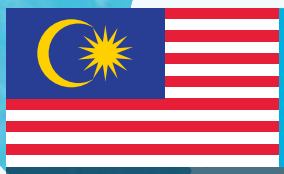
Laos is committed to improving ICT access in schools and universities and, with it, computer literacy. Under the E-government Action Plan established in 2006, the aim is to spread ICT tools across government to help in the delivery of services to the public. Concerns have been raised in the media about Laos's content monitoring and control over ISPs, but have mainly been voiced in and by foreign media.

SCORE: 2

b) What percentage of the population has internet connectivity?

14% of Laotians have access to the internet. Mobile internet has significantly boosted online access in recent years, but low incomes make internet access prohibitively expensive for many Laotians, particularly those who live outside major cities.

SCORE: 2



MALAYSIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	7
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	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?	5
4 – BUSINESS	
a) Is there dialogue between government and industry on 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?	7
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of the population has internet connectivity?	7

OVERALL ASSESSMENT

Dedicated cyber agencies and a more structured legislative framework contribute to Malaysia's increasing cyber maturity. Malaysia has moved beyond a purely technical conceptualisation of cyberspace and now engages with international partners in policy debates and broadens its social awareness through the activities of universities and think tanks. There's a dynamic two-way dialogue with local businesses, and government policy continues to foster the growth of the digital economy. The release of a coherent national cyber strategy to guide the country's cyber developments would raise Malaysia's score.

WEIGHTED SCORE: 68.3

1 GOVERNANCE

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

Malaysia has well-organised government structures for cybersecurity, cyber incident response, policy and strategy development. The National Security Council coordinates the government departments with ICT or cybersecurity responsibilities. CyberSecurity Malaysia is responsible for emergency responses, domestic capacity development, risk assessments, outreach and CNI protection. The Deputy Minister of Science, Technology and Innovation, Dr Abu Bakar Mohamad Diah, has announced that the government is set to review its national cybersecurity policy. The process, to be led by CyberSecurity Malaysia and the National Security Council, will be completed in the next two years. Malaysia would benefit from the creation of a single whole-of-government cyber strategy document to better manage its various frameworks and 'policy thrusts'.

SCORE: 7

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

Malaysia has legislated several cyber-specific laws, including the *Computer Crimes Act 1997*, the *Electronic Commerce Act 2006*, the *Communications and Multimedia Act*, the *Digital Signatures Act* and the *Electronic Government Activities Act*. Malaysia also became the first ASEAN country to enact privacy legislation when it passed the *Personal Data Protection Act* in 2010. Balanced implementation of legislation across the board, particularly financial crimes legislation, would lift Malaysia's score.

SCORE: 7

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

Malaysia is very engaged on international cyber issues bilaterally and multilaterally. It has traditionally focused on more technical cooperation and capacity-building via such organisations as ITU IMPACT, but is increasingly branching out into policy and international security elements of cyber cooperation. It's working with Australia and Russia to produce the ARF Work Plan on Security of and in the Use of ICTs, which underpins the ARF's continued and successful cyber confidence building measures agenda. Malaysia plays an active role in that agenda, co-chairing recent workshops with both Australia and China, and is set to host another with the European Union in March 2016.

SCORE: 8

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

MyCERT is Malaysia's national CERT. Located organisationally within the Ministry of Science, Technology and Innovation, MyCERT is the first point of contact for computer security issues in Malaysia. It runs the Cyber999 computer security incident handling response centre and the CyberSecurity Malaysia Malware Research Centre. MyCERT is very active in the CERT/CSIRT community and is a member and leader in both APCERT and OIC-CERT. It's also very active in its engagement with Malaysian and international private-sector partners.

SCORE: 8

2 CYBERCRIME

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

The Commercial Crime Investigation Department of the Royal Malaysian Police has a Cyber Crime and Multimedia Investigation Branch headed by a deputy director. Malaysia also convened the International Conference on Prevention and Suppression of Hi-Tech crime.

SCORE: 6

3 MILITARY

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

In 2012, it was reported that the Malaysian Army's 4th Division was to expand its role to include urban warfare and cyberwarfare. It was envisaged that a new 5,000-strong unit would assist in the protection of national assets in cities, mainly in the Klang Valley, and in cyberspace. It was reported at the time that Malaysia's other three infantry divisions would create similar units in Kuching, Penang and Malacca. It's not known whether these units were created. The Royal Malaysian Signals Regiment (Rejimen Semboyan Diraja) is responsible for Malaysia's electronic warfare operations. At the 11th Shangri-La Dialogue, the Malaysian Defence Minister called for the establishment of an ASEAN master plan for Southeast Asia's cybersecurity.

SCORE: 5

4 BUSINESS

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

The Malaysian Government conducts relatively strong two-way dialogue with industry on cybersecurity issues. MyCERT runs the Cyber999 emergency service, which is available to all businesses. CyberSecurity Malaysia runs an annual award ceremony, conference and exhibition that aim to drive growth and innovation and facilitate the sharing of knowledge and best practice. CyberSecurity Malaysia has also created the Cyber Security Industry Directory to link businesses and members of the public to Malaysia's ICT industry.

SCORE: 7

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

According to Malaysia's Department of Statistics, the ICT sector contributed 161.6 billion ringgit to 2013 national GDP of 986.7 billion.[5] Malaysia has a very well-developed national plan to harness the digital economy. It consists of three 'strategic thrusts' to move from a supply to a demand focus, to move from consumption- to production-centric models, and to move from low knowledge-add to high knowledge-add business models. The three thrusts cover a total of 12 initiatives that are to be implemented by 2020.

SCORE: 7

5 SOCIAL

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

CyberSecurity Malaysia has run several CyberSAFE initiatives to help increase national awareness of the importance of cybersecurity. The Royal Malaysian Police runs the Be Smart Cybercrime Prevention Campaign in conjunction with Limkokwing University. The National University of Malaysia offers a Master of Cyber Security degree in partnership with CyberSecurity Malaysia. The Institute of Strategic and International Studies Malaysia furthers the public debate on cybersecurity issues in Malaysia, and the media actively covers cybersecurity topics.

SCORE: 6

b) What percentage of the population has internet connectivity?

Malaysia's internet penetration level is at 68%, and the government is working to increase access in rural and urban areas with new infrastructure and free Wi-Fi.

SCORE: 7

MYANMAR

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	3
b) Is there legislation/regulation relating to cyber issues or internet service providers (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 on 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?	2
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of the population has internet connectivity?	1

OVERALL ASSESSMENT

Myanmar is aware of cyber issues, but its cyber-specific legislation is limited and there's little evidence of efficient policy implementation. The government continues to adopt a narrow approach to cyberspace, and the country's public and international engagement is focused mainly on infrastructure development. The military boasts some cyber capabilities, but Myanmar's overall preparedness to tackle cybercrime and other threats seems inadequate. Greater internet penetration would facilitate the development of a digital economy and produce a higher cyber maturity score.

WEIGHTED SCORE: 26.9

1 GOVERNANCE

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

Myanmar has a nascent cyber policy and security governance structure, focused on the Ministry for Communications and Information Technology, which appears to also contain the country's National Cyber Security Centre. The ministry is responsible for developing and implementing a national cybersecurity strategy, policy and roadmap. Myanmar's score reflects its awareness of the requirement for cyber governance structures. However, its narrow focus and the scant evidence of active engagement in implementing the national ICT Master Plan reduce its score for this category.

SCORE: 3

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

Myanmar's cyber legislation was largely developed during the military dictatorship and is focused on censoring content. Specific legislation on financial cybercrime offences was enacted through the *Electronic Transactions Law 2005*; a draft Telecommunications Law from 2012 exists, but it's unclear whether it's been enacted. Myanmar's score for this indicator reflects the narrowness of its existing cyber legislation and the lack of evidence of effective implementation.

SCORE: 4

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

Myanmar has engaged in some regional multilateral and bilateral cyber-related discussions, including the ASEAN Telecommunications and IT Ministers meeting, IMPACT and TSUBAME. It has also engaged with South Korea and Singapore to develop its cyber policy and strategy and military cyber capability, respectively. The narrow range of subject matter and international partners and forums Myanmar engages with reduces its score for this category.

SCORE: 4

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

Myanmar's mmCERT was established in 2004 by the e-National Task Force. It works with the public and private sectors to develop cybersecurity awareness in Myanmar. It has engaged with JPCERT to establish best practices and guidelines for the public and private sectors. It's relatively active in publishing daily and weekly security alerts, but its capacity to respond to incidents is not readily discernible. This score is also reduced by Myanmar's relatively narrow and passive international engagement.

SCORE: 3

2 CYBERCRIME

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

The Myanmar Police has announced that it will establish a cybercrime unit, and has reportedly received training from Singapore, Japan and Australia. However, the effectiveness of financial cybercrime enforcement isn't readily apparent, and it appears that ongoing international engagement with other police cybercrime units, beyond receiving training, is minimal.

SCORE: 2

3 MILITARY

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

The Myanmar military is believed to have some sophisticated cyber capability, primarily to monitor internet content and to surveil dissidents in exile. This capability was developed with assistance from foreign partners, formerly Singaporean but now increasingly Chinese. Myanmar's score for this category reflects its apparent understanding of military applications of cyber capability, but would be higher if greater detail of its organisational awareness of cyber threats and efforts to address them were available.

SCORE: 5

4 BUSINESS

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

There continues to be a significant lack of opportunity for Myanmar's private sector to engage with the government on cyber issues. While mmCERT provides some guidance to the private sector, it appears that this is a one-way dialogue.

SCORE: 1

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

Low internet penetration in Myanmar, either fixed or mobile, is still an enormous barrier to the development of the country's digital economy. While the growth of the mobile market is encouraging, it has yet to translate into the development of a significant e-commerce sector.

SCORE: 2

5 SOCIAL

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

Concomitant with Myanmar's low level of internet penetration is its low level of public engagement on cyber policy and security issues. Myanmar's minimal discussion is often focused on digital infrastructure development led by external parties.

SCORE: 2

b) What percentage of the population has internet connectivity?

About 2% of Myanmar's population has access to the internet. Myanmar is working to achieve 50% mobile phone penetration by 2016, but access remains out of reach for much of the country's population.

SCORE: 1

NEW ZEALAND

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	8
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	6
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?	7
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 on 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?	8
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has internet connectivity?	9

OVERALL ASSESSMENT

The New Zealand Government has a well-developed structure and legislative framework for addressing cyber issues. While New Zealand participates actively in Anglosphere cyber forums, greater regional engagement on policy and cybercrime would raise its cyber maturity score. The military appears to be cognisant of cyber threats, but the policy intended to guide its capabilities remains unclear. The rapid growth of New Zealand's digital economy is unfortunately undermined by the lack of an active public–private sector dialogue on the issue. However, public discussion of cyber issues is dynamic and involves a variety of actors.

WEIGHTED SCORE: 72.8

1 GOVERNANCE

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

New Zealand has two clear centres of gravity within government for cybersecurity and cyber policy. The National Cyber Policy Office in the Department of the Prime Minister and Cabinet leads the development and implementation of cyber policy, international cyber engagement and the facilitation of private-sector engagement on cybersecurity issues. The National Cyber Security Centre (NCSC), hosted by the Government Communications Security Bureau, provides cybersecurity services to government and private-sector organisations. It supported the 2015 edition of the *NZ information security manual* and in 2013 released voluntary cybersecurity standards for industrial control systems. New Zealand's score is reduced due to uncertainty about the NCSC's ability to work with private-sector organisations while hosted by the Government Communications Security Bureau.

SCORE: 8

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

New Zealand has developed and implemented a comprehensive suite of legislation to deal with cyber issues. Legislation encompasses cybercrime, spam, some content, copyright infringement through online file sharing, intelligence collection, and interception and surveillance in cyberspace. A cyberbullying bill has also been debated in parliament in 2015. The *Telecommunications (Interception Capability and Security) Act 2013* established a framework under which network operators are required to engage with the Government Communications Security Bureau (through the NCSC) about changes and developments in their networks where they intersect with national security.

SCORE: 8

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

The New Zealand Cyber Security Strategy identified international cooperation as an important part of the strategy. New Zealand participates in several bilateral and multilateral international cyber engagements; however, those engagements seem narrowly focused on the Anglosphere, particularly the Five Eyes states, along with some engagement with NATO. New Zealand's score for this indicator is reduced by its apparent inactivity in the region and the narrow focus of its international cyber engagement.

SCORE: 6

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

The NCSC provides the CERT function for New Zealand. It became a general member of APCERT in March 2012. While the NCSC's efforts are strong domestically, its lack of strong leadership in international CERT–CERT engagement reduces New Zealand's score for this category.

SCORE: 7

2 CYBERCRIME

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

The New Zealand Police National Cyber Crime Centre was established in 2007 as part of the E-Crime Strategy. It handles offences such as scams, fraud, identity theft and malware. A separate unit also addresses online child exploitation across New Zealand. New Zealand is a signatory to the Council of Europe Cybercrime Convention and works closely with Australian law enforcement agencies. Its score for this indicator is reduced because it hasn't strongly engaged in assisting smaller regional countries to tackle cybercrime.

SCORE: 7

3 MILITARY

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

Details of the New Zealand Defence Force's (NZDF's) cyber capability are difficult to discern, but it's clear that the NZDF understands the importance of protecting its digital networks. The 2014 Defence Capability Plan and the 2010 Defence White Paper referred to the asymmetric threat that's present in cyberspace and to the need to preserve the NZDF's ability to cope with cyber threats. This includes being able to take part in 'any whole-of-government response to the threat of cyberattack'. New Zealand's score for this indicator is reduced because it's unclear how the NZDF would contribute to a whole-of-government response, how it draws on the cybersecurity skills of the NCSC and the information security skills of the Government Communications Security Bureau, and how cyberdefence has been integrated into its force structure.

SCORE: 5

4 BUSINESS

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

The New Zealand Government has promoted the benefits of cyberspace to businesses and has developed businesses' awareness of threats through programs such as ConnectSmart Week, which in 2015 focused on small to medium-sized enterprises. Despite those efforts, research suggests that New Zealand businesses are inadequately prepared to protect themselves from cyber threats and have no intention to invest further in cybersecurity. While the New Zealand Government's efforts are notable, New Zealand's score in this category is reduced because there doesn't appear to be a good level of two-way dialogue between government and the private sector.

SCORE: 6

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 growing area of New Zealand's wider economy, growing at 10% per year between 2002 and 2012. New Zealand's favourable business and regulatory environment and the independence of its judiciary were noted by the World Economic Forum's 2014 Network Readiness Index[6] as key strengths for New Zealand in growing its digital economy; however, the price of ICT services is a weakness in this area, reducing New Zealand's score.

SCORE: 8

5 SOCIAL

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

There's significant debate on cybersecurity issues in New Zealand's traditional and social media,and the academic and non-government organisation spheres. InternetNZ is a not-for-profit open-membership organisation dedicated to protecting and promoting the internet in New Zealand; it provided an assessment of the ICT policies of the National and United Futures parties before the most recent national election. There's also been significant debate about the impact on privacy and business of recent legislation—including the *Government Communications Security Bureau Act 2003* and the *Telecommunications (Interception Capability and Security) Act 2013*)—in the wake of the Snowden leaks, the Kim DotCom case and New Zealand's role in the Five Eyes intelligence partnership.

SCORE: 9

b) What percentage of the population has internet connectivity?

86% of New Zealanders have access to the internet. Growth in access has been relatively stagnant: access has increased by only 6% since 2009.

SCORE: 9

NORTH KOREA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	3
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	2
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	1
b) What percentage of the population has internet connectivity?	1

OVERALL ASSESSMENT

North Korea takes a highly structured and regulated approach to cyberspace. However, it suffers from a paucity of policy and cybercrime agencies. Instead, the focus of cyber development is mainly military, and the government is suspected of having sophisticated offensive cyber capabilities. North Korea's isolationism extends to its cyber policy: it has no apparent international engagement on the issue. Domestic computer and internet access is also highly limited, contributing to the country's low level of social and economic engagement on cyber issues.

WEIGHTED SCORE: 16.4

1 GOVERNANCE

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

There's little evidence that North Korea has altered its highly centralised approach to cybersecurity and policy governance. The government exerts total control over access to cyberspace and the national intranet (Kwangmyong), demonstrating that governance structures exist. That control appears to be focused on the military; there's no evidence of the existence of cyber policy, cybercrime or cybersecurity bodies.

SCORE: 3

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

Access to computers and the national intranet is highly regulated. Regulations covering access to the internet by visiting foreigners, such as some prohibiting access to Instagram, have been enacted in response to specific events. There's no indication of regulation beyond content and access control.

SCORE: 1

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

North Korea isn't involved in discussions of international cyber issues beyond resisting accusations made against it over its malicious online behaviour. It probably engages with its traditional partners in China and Russia to discuss ICT developments and trade.

SCORE: 2

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

There's no evidence of a national CERT in North Korea. It's unlikely that the state has plans to establish one, considering its limited access to the internet.

SCORE: 0

2 CYBERCRIME

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

North Korea doesn't appear to have established any function to police financial cybercrime. It's been suggested instead that it uses its highly trained cyberforces to profit from cybercrime.

SCORE: 0

3 MILITARY

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

North Korea maintains a large professional cyber and information warfare group within the military. It has extensively targeted South Korea and sees the use of offensive cyber operations as a tool of national power. This was demonstrated in 2015 when North Korea sought to coerce the US and Sony Corporation to shelve the release of a film depicting the assassination of Kim Jong Un by releasing proprietary information stolen from Sony servers. Reports in early July 2014 indicated that North Korea had doubled its cyber personnel in the General Reconnaissance Bureau, based in North Korea and China, to around 5,900 people. Office No. 91 is believed to be the headquarters of the cyberforce, while the bulk of offensive cyber operators are part of Unit 121, supported by Lab 110, Units 35 and 204 and Offices 31, 32 and 56. An extensive system to identify potential recruits early in their education and foster their skills is reportedly used to develop this cyberforce, and privileges are bestowed on its members to dissuade them from using their access to the global internet to undermine the regime.

SCORE: 8

4 BUSINESS

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

Dialogue isn't apparent, beyond partnerships with some foreign firms that provide ICT services such as the country's ISP, which is jointly owned by a Thai firm.

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 isn't a significant part of North Korea's economy, beyond the construction of a few thousand computers per year by the government-operated Morning Panda company, and the indigenous Arirang smartphone which is an Android clone. These are necessary because foreign-manufactured units are illegal.

SCORE: 1

5 SOCIAL

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

While there's limited discussion of cyber issues within the country, the Sony incident has probably raised greater awareness of cyber issues, albeit through highly regulated government news outlets.

SCORE: 1

b) What percentage of the population has internet connectivity?

In 2015, the total number of domains in North Korea was reduced from 199 to 114. There are only 1,024 IP addresses recorded for the country of 25 million people. The national intranet, Kwangmyong, probably has more users, although exact numbers aren't available. This network is accessible by the handful of computer labs at major North Korean government offices, universities, and a small number of cybercafes in major cities.

SCORE: 1

PAPUA NEW GUINEA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	3
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	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?	2
4 – BUSINESS	
a) Is there dialogue between government and industry on 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) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has internet connectivity?	1

OVERALL ASSESSMENT

Papua New Guinea (PNG) has demonstrated limited improvement in its cyber maturity and continues to take a relatively narrow approach to cyberspace in its government structures and legislation. There's an awareness of the threat of cybercrime and cyber warfare, but the implementation of responsive policy is unclear. Engagement with the private sector and international partners continues to be focused on the establishment of cyber infrastructure. Despite PNG's low level of internet penetration, there's some level of social engagement with cyber issues. A broader approach to cyberspace, with more extensive policy development and implementation, would result in a higher score.

WEIGHTED SCORE: 20.3

1 GOVERNANCE

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

PNG hasn't substantially improved or altered its cybersecurity policy or governance arrangements since 2014. Governance is still focused on the management and development of cyber infrastructure in the country. It will need to implement a broader structure that includes cybersecurity, cybercrime and international engagement to score higher in this category.

SCORE: 3

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

PNG's legislative and regulatory basis for cyberspace is limited to the *National ICT Act 2009* and the *Telecommunications Act 1996*, which criminalise some acts, such as fraudulent or dishonest access to telecommunications networks. Its Cybercrime Policy sets an objective to adopt laws criminalising attacks on the security and integrity of computer networks and electronic transactions. PNG's score would improve with evidence of a broader legislative framework and strong implementation.

SCORE: 3

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

PNG's international engagement on cyber issues is limited to some technical and policy engagement with ITU-IMPACT and various development organisations. It has received foreign aid to develop its IT networks and facilities, including $53.5 million from the Chinese Government for an Integrated Government Information System.[7]

SCORE: 3

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

Since the demise of PacCERT, PNG doesn't have access to a CERT capability. There is no evidence of plans to establish one or reinvigorate PacCERT.

SCORE: 0

2 CYBERCRIME

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

PNG established a cybercrime taskforce in September 2014, with plans to develop legislation, conduct awareness training and establish a cybercrime unit in the PNG Police. Effective implementation of this plan will see PNG's score for this category increase.

SCORE: 1

3 MILITARY

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

Clear evidence of military cyber policy or cybersecurity capability is limited. PNG's 2013 Defence White Paper indicated that the PNG Defence Force is aware of cyber threats, but what's been done to defend against them isn't apparent.

SCORE: 2

4 BUSINESS

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

The PNG Government continues to pursue private-sector partners to further develop the country's ICT infrastructure. However, there's little evidence of strong engagement with business on how to develop the country's economy through digital commerce.

SCORE: 2

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

Digital commerce remains a limited component of PNG's economy. Infrastructure developments may reduce the cost of access for PNG businesses.

SCORE: 1

5 SOCIAL

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

Despite its limited internet access, PNG has a relatively active blogging community, which comments on political issues such as Prime Minister Peter O'Neill's and Australia's influence in PNG, as well as proposals to further regulate SIM cards.

SCORE: 5

b) What percentage of the population has internet connectivity?

The World Bank estimates that 9% of PNG's population has access to the internet. Internet access statistics for PNG show relatively rapid growth of 5% since 2012, after several years of stagnation at about 2% growth.

SCORE: 1

PHILIPPINES

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	5
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	5
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?	3
4 – BUSINESS	
a) Is there dialogue between government and industry on 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) Is there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of the population has internet connectivity?	5

OVERALL ASSESSMENT

The Philippines has diversified cyber legislation and dedicated cybercrime agencies, but continues to suffer from weak enforcement. The government demonstrates only passive engagement in multilateral cyber forums, and awareness of cyber military issues isn't translated into tangible policies or capabilities. Despite the potential for growth, lack of strategic government policy and engagement with the private sector renders the digital economy relatively underdeveloped.

WEIGHTED SCORE: 46.8

1 GOVERNANCE

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

The Philippines appears to have done very little in 2015 to justify an increase in its score for this category. Plans to establish a new Department for ICT and Communications remain unrealised, and Freedom House notes that government agencies with responsibility for cybersecurity policy have ambiguous or overlapping mandates, slowing the development of appropriate cybersecurity governance structures.

SCORE: 5

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

The Philippines' extra point in this category for 2015 reflects the end of deadlock in the Supreme Court over the *Cybercrime Prevention Act* of 2012, which had been suspended for a year while under the court's examination. The court upheld a provision that punished online libel with jail terms but struck down others that enabled warrantless content blocking and monitoring. Otherwise, the Philippines continues to struggle to implement effective cyber legislation.

SCORE: 5

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

The Philippines continues to maintain a relatively narrow range of bilateral cyber discussions, principally with the US and Japan. It also participates in regional multilateral forums but doesn't take a leadership position on the issues discussed. Broader and more consistent engagement on issues that are relevant to the Philippines, notably cybercrime, would increase its score for this indicator.

SCORE: 5

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

PH CERT is the Philippines national CERT, but it's a non-profit voluntary organisation that requires the sale of memberships and sponsorships to operate. PH CERT is a member of TSUBAME but not of APCERT. Apparent resource constraints and a lack of activity mean that PH CERT's score is reduced this year.

SCORE: 3

2 CYBERCRIME

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

Cybercrime is a significant issue for the Philippines, and several bodies have been established to stem its tide. The Office of Cybercrime in the Department of Justice is the central authority for international assistance and extraditions of cybercrime suspects. The Cybercrime Investigation and Coordination Center is a multiagency body under the Office of the President. The National Bureau of Investigation also maintains a Cyber Crime Division. The lifting of the suspension of the *Cybercrime Prevention Act 2012* has led to more prosecutions for cybercrime. The Philippines' score for this indicator is likely to increase in future with greater international engagement.

SCORE: 5

3 MILITARY

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

The Armed Forces of the Philippines appear to have some awareness of cyber threats, but there's no evidence to suggest that they have done much to counter them. In 2014, it was noted that a Security Operations Center with a defensive cyber role had been established, but it has not been possible to discern whether the centre is operational. The Philippines' score would be increased if evidence of a systematic approach to mitigating cyber threats were apparent in the country's armed forces.

SCORE: 3

4 BUSINESS

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

The Philippines Government has found that it needs the assistance of the private sector to deal with cyber threats. It has engaged Microsoft to assist with cybercrime enforcement, and ISACA, a sector-specific education and training program that promotes cybersecurity certification in the public and private sector. However, without a clear strategy or program of public–private cooperation on cybersecurity, the Philippines' score remains low for this category.

SCORE: 4

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

The Philippines' largest export is electronic products (mainly semiconductors), which made up 50.6% of exports in April 2015. This is a growing industry, increasing by 17.8% since April 2014.[8] The Philippines is also a global services provider, providing data processing and other back-end services to the world. While the Filipino business community appears to have embraced the digital economy, there remains a lack of government action to develop it further.

SCORE: 6

5 SOCIAL

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

Freedom House notes that the Filipino blogosphere is particularly active and is used by public and private figures to discuss political issues.[9] This is especially so during elections. Further academic and think-tank research on cybersecurity policy issues is needed to produce a higher score for this indicator.

SCORE: 6

b) What percentage of the population has internet connectivity?

About 40% of Filipinos have access to the internet; there has been significant growth since 2009, when only 9% had access.

SCORE: 5

SINGAPORE

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	9
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	7
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?	7
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has internet connectivity?	9

OVERALL ASSESSMENT

Singapore has continued to implement a coherent government cyber policy, aided by the National Cyber Security Masterplan 2018. The government has comprehensive cyber legislation, internet regulation and military network defence. Singapore participates in multilateral cyber forums, but could adopt a more active role in regional capacity building. There's a high level of internet penetration and lively social engagement on cybersecurity issues. A higher score could be achieved with greater legislative enforcement and clarity about the division of responsibilities between government agencies.

WEIGHTED SCORE: 81.8

1 GOVERNANCE

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

Singapore's increased score this year largely reflects the continued implementation of a strong government cybersecurity architecture under the National Cyber Security Masterplan 2018. This is mainly apparent in the establishment of the Cyber Security Agency on 1 April 2015. This agency, under the Prime Minister's Office, will combine the Singapore Infocomm Technology Security Authority with some cybersecurity functions from the Infocomm Development Authority, such as SingCERT, and the Ministry of Home Affairs. Singapore has also appointed the Minister for Communications and Information, Mr Yaacob Ibrahim, as minister in charge of cybersecurity.

SCORE: 9

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

Singapore has a strong suite of cyber-specific or cyber-related legislation and regulation covering cybersecurity, cybercrime, ISP licensing and regulation, electronic transactions, spam, and copyright infringement. The *Computer Misuse and Cyber Security Act* empowers the government to compel critical infrastructure companies to provide information on their networks if it's needed to detect, identify or counter cyber threats. Further evidence of successful implementation of this legislation is needed to improve Singapore's score in this category.

SCORE: 8

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

Singapore continues its successful involvement in multilateral CERT engagement and anti-cybercrime collaboration and its bilateral policy engagement with regional states, including Malaysia and Australia, as well as the US and the UK. As noted in 2014, Singapore's score would rise if it took a greater leadership role in regional and global cyber policy and security issues.

SCORE: 7

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

SingCERT became a part of the new Cyber Security Agency in 2015. Singapore's score is reduced from 2014, as it hasn't expanded its leadership of regional CERT exercises or training despite its considerable technical capabilities.

SCORE: 7

2 CYBERCRIME

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

The Technology Crime Division is a unit of the Criminal Investigation Department of the Singapore Police. It investigates, forensically examines and prosecutes technology-related offences committed under the *Computer Misuse and Cyber Security Act*. Singapore also hosts INTERPOL's Global Complex for Innovation. Singapore's score is reduced because it doesn't appear to be strongly engaged in training or supporting other regional cybercrime units.

SCORE: 7

3 MILITARY

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

The Singapore Armed Forces continue to display a good awareness of cyber threats. They have sustained the development of the Cyber Defence Operations Hub, and continue to work with the Cyber Security Agency to protect their networks. Singapore's score isn't higher because the division of responsibility between military and civilian agencies is unclear, and because of its low levels of international engagement.

SCORE: 8

4 BUSINESS

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

There's significant interaction between Singapore Government agencies and the country's private sector as they work together to secure Singapore from cyber threats and leverage the benefits of Singapore's highly educated workforce to grow the digital economy. The National Cyber Security Masterplan 2018 emphasises the need for a public–private partnership to grow the state's pool of cybersecurity experts. Several multinational firms, including Israel Aerospace Industries and Boeing, have also opened cybersecurity centres in Singapore. Singapore has committed to becoming a 'smart nation' and has implemented initiatives across infrastructure, software and services identified as necessary components to support Singapore as a centre of digital commerce.

SCORE: 9

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

Singapore regularly ranks among the top of the pack globally for digital business. The Infocomm Development Agency reported that Singaporean ICT firms employed 146,700 people and had revenues of $148.11 billion in 2014.[10] The World Economic Forum's *Global information technology report* singles out Singapore's favourable environment for digital business, including its constantly improving ICT infrastructure, high-quality education system and clear government strategy, as key enablers for the continued strength of the country's digital economy.[11]

SCORE: 9

5 SOCIAL

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

Singapore continues to conduct a healthy discussion across sectors on cybersecurity issues and threats. As part of its overall cyber strategy, the government is working with the private sector to increase the status of ICT and cybersecurity professionals and raise awareness of cyber threats in the community.

SCORE: 9

b) What percentage of the population has internet connectivity?

The World Bank estimates that 82% of Singaporeans have access to the internet.

SCORE: 9

SOUTH KOREA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	8
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	7
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?	9
4 – BUSINESS	
a) Is there dialogue between government and industry on 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) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has internet connectivity?	9

OVERALL ASSESSMENT

South Korea demonstrates a strong understanding of cyber issues and efficient coordination of its various cyber agencies through an overarching cyber policy. The persistent threat from North Korea has resulted in a clear prioritisation of cybersecurity issues and offensive cyber capabilities, both domestically and in South Korea's foreign engagement. The government encourages growth in the digital economy by providing public funding and information, as well as strong enforcement of cybercrime legislation. This highly networked society engages in sophisticated and diverse public discussion in cyberspace. However, South Korea's score would increase with a broader government consideration of cyber issues, expanding international dialogue beyond security and into policy and governance.

WEIGHTED SCORE: 82.8

1 GOVERNANCE

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

South Korea has continued to implement an effective centralised cybersecurity governance and response structure. In April 2015, President Park appointed Brigadier General Shin In-Seop as South Korea's cybersecurity tsar within the National Security Office. This position is designed to further strengthen the country's 'control tower' and enable more effective responses to cyber threats. South Korea continues to show a good awareness of cybersecurity risks in the face of North Korean threats, demonstrated by strong central oversight of cyber policy and security operations.

SCORE: 8

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

South Korea's cyber legislation and regulation have been developed to enable the protection of the state's cybersecurity, its information and communications infrastructure and the privacy of South Koreans. In lockstep with the development of its governance structure, South Korea has implemented an effective legislative framework for its cybersecurity. It has also encouraged the growth of e-commerce by implementing effective cybercrime and electronic transaction protection legislation.

SCORE: 8

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

South Korea is seeking to be a regional and global leader of international cyber policy discussions. Its score reflects its work in establishing bilateral cyber policy dialogues with Japan and China, but South Korea won't score higher unless it can broaden its engagement beyond security issues to encompass more holistic cyber dialogue, including on internet governance and crime.

SCORE: 7

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

In 2015, South Korea maintained an effective CERT capacity. KrCERT, under the Korea Internet Security Agency, works with the private sector, while KNCERT is responsible for public-sector responses as a part of the National Cyber Security Center, and for engagement with private CERTs. In 2014–15, KrCERT reported strong international cooperation with China and Japan and established stronger links with India and the UK. It also held five domestic cyber drills in 2014 and assisted 1,001 organisations affected by distributed denial-of-service (DDOS) attacks through its DDOS Cyber Shelter.

SCORE: 8

2 CYBERCRIME

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

The National Police Agency's Cyber Bureau was established in June 2014, but a computer crime investigation team was first established in 1997. Since 2000, the National Police Agency has hosted the annual International Symposium on Cybercrime Response. The *Criminal Act*, the *Act on Promotion of Information and Communications Network Utilization and Information Protection*, the *Personal Information Protection Act* and the *Act on the Protection of Information and Communications Infrastructure* provide the legislative basis for the enforcement of cybercrime law in South Korea. South Korea's score would improve with further evidence of international engagement and capacity-building assistance on cybercrime issues.

SCORE: 7

3 MILITARY

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

The South Korean military reportedly possesses both defensive and offensive cyber capabilities, mainly developed to counter North Korea's cyber capability. Seoul estimates that the North has doubled its offensive cyber cadre, and in the face of increasing cyber incidents South Korean officials have stated that they have been forced to move from a passive cyber defence posture to a more active one, including taking pre-emptive action if threatened. The military's cyber capability is housed within the Cyber Command established in 2010. How successful an active defence strategy might be is debatable, taking into consideration North Korea's largely disconnected state, which makes it far less vulnerable than the South, and concerns about interfering in China, where many of North Korea's hackers are reportedly based. South Korea exhibits an excellent awareness of cyber threats to its military and has implemented measures to mitigate them. Its score will improve if its offensive cyber operations doctrine is more clearly described.

SCORE: 9

4 BUSINESS

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

South Korea's business community generally enjoys a cosy relationship with the government, which supports businesses' efforts to grow ever larger. The National Information Security Alliance is composed of representatives of public and private sector and academic institutions. This has extended to the digital economy, in which government funding supports a thriving start-up sector. The Ministry of Science, ICT and Future Planning's 2014 budget included US$2 billion for direct funding to start-ups and the elimination of restrictions on venture capitalism to promote the growth of a creative digital economy.[12]

SCORE: 9

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

Within the OECD, South Korea is second only to Ireland for ICT value added to GDP (the difference between ICT sector gross output and intermediate consumption).[13] ICT exports of US$93.3 billion, third only to those of the US and China, demonstrate the critical importance of the digital economy to South Korea's wider economy.[14]

SCORE: 9

5 SOCIAL

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

South Korea is renowned as the world's most connected country, so discussions of cybersecurity and policy issues are widespread in its traditional media, social media and academic debates. Digital media are playing an increasingly important role in informing the opinions of South Koreans; the government has noted this trend, but has been criticised for attempting to control content critical of government policy.

SCORE: 9

b) What percentage of the population has internet connectivity?

The steady growth of internet access in South Korea has now connected 85% of South Koreans to the internet.

SCORE: 9

THAILAND

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	6
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	4
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has internet connectivity?	4

OVERALL ASSESSMENT

Thailand has a maturing cyber governance structure and is now developing additional cyber legislation. The implementation of its new policies, in concert with current growth trends, should deliver significant expansion of the country's digital economy and internet penetration levels. Although Thailand has shown an awareness of and interest in the military applications of cyberspace, evidence of tangible policy and capabilities in this area remains elusive. Thailand demonstrates a moderate engagement with international cyber discussions, but would benefit from participating in a more comprehensive debate that goes beyond capacity building to cybersecurity and governance.

WEIGHTED SCORE: 49.1

1 GOVERNANCE

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

In 2015, Thailand recast the former Ministry of Information and Communications Technology as the Ministry for Digital Economy and Information Technology, reflecting the government's intent to further develop the country's digital economy. Plans to establish the Office of the National Cyber Security Committee appear stalled as the *Cyber Security Bill* awaits consideration by the National Legislative Assembly, along with other cyber legislation. Thailand's score for this indicator reflects a good awareness in government of the need to manage cybersecurity and policy, but is reduced by the slowness of its implementation of new governance structures.

SCORE: 6

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

Thailand's cyber legislation remains a work in progress, but further work in 2014–15 led to several cyber bills progressing to the National Legislative Assembly; one (*the Information and Communications Technology Ministry Reform Bill*) has been enacted. Thailand's score reflects the broad scope of its current and draft legislation, which covers cybersecurity, the digital economy, electronic transactions, personal data protection and cybercrime. The enactment of bills currently under review and the implementation of the agencies created under that legislation would increase Thailand's score in this category.

SCORE: 6

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

Thailand engages in regional multilateral forums such as the ASEAN Regional Forum, and has significant CERT interactions with regional countries. Greater involvement in the international security dimensions of cyber policy and broader engagement would increase Thailand's score for this indicator.

SCORE: 5

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

ThaiCERT is Thailand's national CERT, reporting to the Electronics Transaction Development Agency of the Ministry for Digital Economy and Information Technology. ThaiCERT reported dealing with 4,008 incidents in 2014, an increase of 229% from 2013. It's also a participant in regional cyber drills, but doesn't appear to take a leadership role in regional CERT engagement, reducing its score.

SCORE: 5

2 CYBERCRIME

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

The Economic and Cybercrime Division of the Royal Thai Police enforces the country's financial cybercrime legislation, which is under review by the National Legislative Assembly. While Thailand has participated in the arrest of several international cybercriminals, such work has usually been done by the Immigration Section of the Thai Police instead of the Cybercrime Division. Further evidence of the enforcement of financial cybercrime law is necessary for Thailand's score to improve.

SCORE: 4

3 MILITARY

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

There's little evidence that the Thai military has an effective cyber defence capability, but it appears that a small cyber unit is being stood up. Since the most recent coup, the military has had a leading role in setting cyber policy direction for the country, but this has been largely unrelated to the capabilities of the Thai Armed Forces.

SCORE: 5

4 BUSINESS

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

Despite the clear intent of the Thai Government to enhance the country's economy by leveraging the internet, there's little evidence of significant dialogue between the public and private sectors on cybersecurity and digital economy issues, other than consultation on some aspects of proposed legislation.

SCORE: 3

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

The Thai digital economy is estimated to be worth about US$21 billion a year.[15] The government's proposed cyber legislation has a heavy emphasis on improving the legal framework that supports the digital economy to better enable its growth. In July 2015, the Digital Economy Committee, led by Prime Minister Prayut Chan-o-cha, ordered the development of the Digital Economy Strategic Plan by 2016. The government's awareness of the benefits of digital economy, and its plans to better enable that sector, mean that Thailand's score could increase with the strong implementation of measures currently under consideration.

SCORE: 6

5 SOCIAL

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

Awareness of cyber policy and security issues is still emerging in Thailand and is largely linked to debate about new and revised cyber-related legislation. One example is the change.org petition launched by the Thai Netizen Network, an online privacy advocacy group, calling for a stop to the government's cyber legislative agenda; the petition received 5,000 signatures in the first 24 hours. Beyond privacy and content control concerns, there's a general low level of awareness of cybersecurity issues in the Thai community.

SCORE: 5

b) What percentage of the population has internet connectivity?

Internet penetration in Thailand continues to grow, climbing from 29% to 35% between 2013 and 2014.

SCORE: 4

UNITED STATES

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	9
b) Is there legislation/regulation relating to cyber issues or internet service providers (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 on 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) Is there public awareness, debate and media coverage of cyber issues?	10
b) What percentage of the population has internet connectivity?	9

OVERALL ASSESSMENT

The United States (US) delivers strong cyber policy through a sophisticated government structure and comprehensive legislative framework. The establishment of new cyber laws has been relatively successful, and the Obama administration has also enacted several executive orders in relation to the regulation of cyberspace. The US has a high success rate in addressing cybercrime domestically and internationally, as well as robust military cyber capabilities governed by clear policy and strategy. The US Government prioritises the invigoration of the country's digital economy, and this is achieved through a mature relationship with the private sector and other policy initiatives. The US has maintained its role as a global leader in cyberspace, although a higher score could be achieved through engaging more with Southeast Asia.

WEIGHTED SCORE: 90.7

1 GOVERNANCE

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

In 2015, the US Government continued to refine its governance structure for cybersecurity and policy. Major incidents, including the hacking of Sony Corporation and data breaches in the Office of Personnel Management, put the spotlight on the government's policy response to foreign hacking and on technical responses to its own cybersecurity deficiencies. Many US departments have responsibility for cybersecurity and policy, which can make things appear chaotic, but this reflects the maturity of the US's whole-of-government approach to this ubiquitous issue. Of note is the significant effort by the US to aggregate and evaluate threat intelligence feeds from across government, including the new Cyber Threat Intelligence Integration Center under the Office of the Director of National Intelligence, announced in February 2015. The centre will be an intelligence fusion centre for cyber threat information from across the US Government, incorporating intelligence from the National Cybersecurity and Communications Integration Center within Homeland Security, the National Cyber Investigative Joint Taskforce and US Cyber Command. While lines of responsibility appear vague from outside, this significant effort to make myriad threat intelligence feeds useful demonstrates a high level of maturity.

SCORE: 9

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

In 2015, the US has been active both legislatively and in the production of cybersecurity standards, with varying levels of success. Cybersecurity legislation, previously deadlocked, is gathering momentum. The White House proposed new legislation to Congress in January that included information-sharing and data-breach notification provisions. The House passed two similar bills in April, and the Senate Intelligence Committee passed the *Cybersecurity Information Sharing and Protection Act* in July. If the House and Senate can agree, the new legislation will provide a strong legislative basis for government and private-sector cybersecurity efforts. While debate continues in Congress, the administration has issued an executive order to encourage the development of information sharing and analysis organisations, and another that authorises the imposition of sanctions on individuals and entities who have affected the national security or economic health of the US through malicious cyber activity. The administration has continued to roll out the Cybersecurity Framework developed by the National Institute of Standards and Technology and the institute's special publication 800-171, providing federal agencies with recommended requirements for information security. The framework is expected to be used for information security specifications in future government contracts.

SCORE: 8

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

The US continues to be a global leader of cyber policy discussions, including the recently concluded 2015 UNGGE meeting, where US influence secured the inclusion of new voluntary norms. While most attention falls on the US–China cyber relationship, the US has also announced cyber policy discussions with Brazil, India, Japan, the UK and the Gulf Cooperation Council. It has also raised cyber policy issues in the G7, been a founding member of the Global Forum on Cyber Expertise, participated in NATO cyber exercises and continued to support international cybercrime prevention efforts by expanding the Federal Bureau of Investigation's Cyber Assistant Legal Attaché program. The only factor reducing the US score in this category is underdeveloped engagement in Southeast Asia.

SCORE: 9

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

There are 70 US members of FIRST, including many corporate incident response teams and some providing services for fees. US CERT is the operational arm of Homeland Security's National Cybersecurity and Communications Integration Center. While the US has strong incident response capability, its score would increase if it also implemented a stronger international engagement and capacity-building program.

SCORE: 8

2 CYBERCRIME

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

The US is a global leader in prosecuting financial cybercrime in the US and internationally. Notable cases in 2014–15 included shutting down Silk Road, closing Darkode, overcoming the Gameover Zeus botnet, arresting a Chinese professor for economic cyber-espionage, and indicting five PLA officers for cyber-espionage linked to US corporate engagement with Chinese state-owned enterprises. With the support of the US, numerous individuals across the world were arrested by international law enforcement agencies, supported by a network of US liaison officers. Without the capacity provided by the US in this area, and its advocacy of financial cybercrime enforcement, the fight against cybercrime would be an even tougher battle.

SCORE: 10

3 MILITARY

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

In 2015, the US military has further demonstrated its commitment to the full integration of offensive and defensive cyber operations, as demonstrated through the Department of Defense's updated Cyber Strategy. The strategy outlines how the department will build the capability to defend itself and the US and to provide cyber operations to support conventional military operations. While the department admits difficulties in recruiting the required number of personnel to its cyber mission teams, the publication of the strategy demonstrates the maturity of the US military's consideration of cyber operations and their implications for military operations.

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 sustained its strong dialogue with the US business community in 2015. The link is particularly strong among large US firms in the tech, finance and defence fields. The government has a clear understanding of the role of the private sector in securing the US information environment. It's working cooperatively through such initiatives as the White House Summit on Cybersecurity and Consumer Protection and Homeland Security's Cyber Information Sharing and Collaboration Program to better share threat information with the private sector. The digital economy is seen as a key factor in revitalising the American economy and securing the US's military advantage by leveraging the innovative skills of Silicon Valley through the Defense Innovation Unit—Experimental. The US's score would improve if the government were to engage with small to medium-sized enterprises with the same vigour it shows towards larger companies.

SCORE: 9

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

The US is home to some of the most sophisticated digital companies. US Census Bureau statistics show sustained growth in e-commerce as more Americans purchase goods and services online (providing US$443 billion of selected service industry revenue in 2013). The US Government sees an opportunity to boost the country's sluggish economy through cyberspace; its initiatives to make consumers feel more secure using e-commerce include the executive order on consumer protection and the Buy Secure program.

SCORE: 9

5 SOCIAL

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

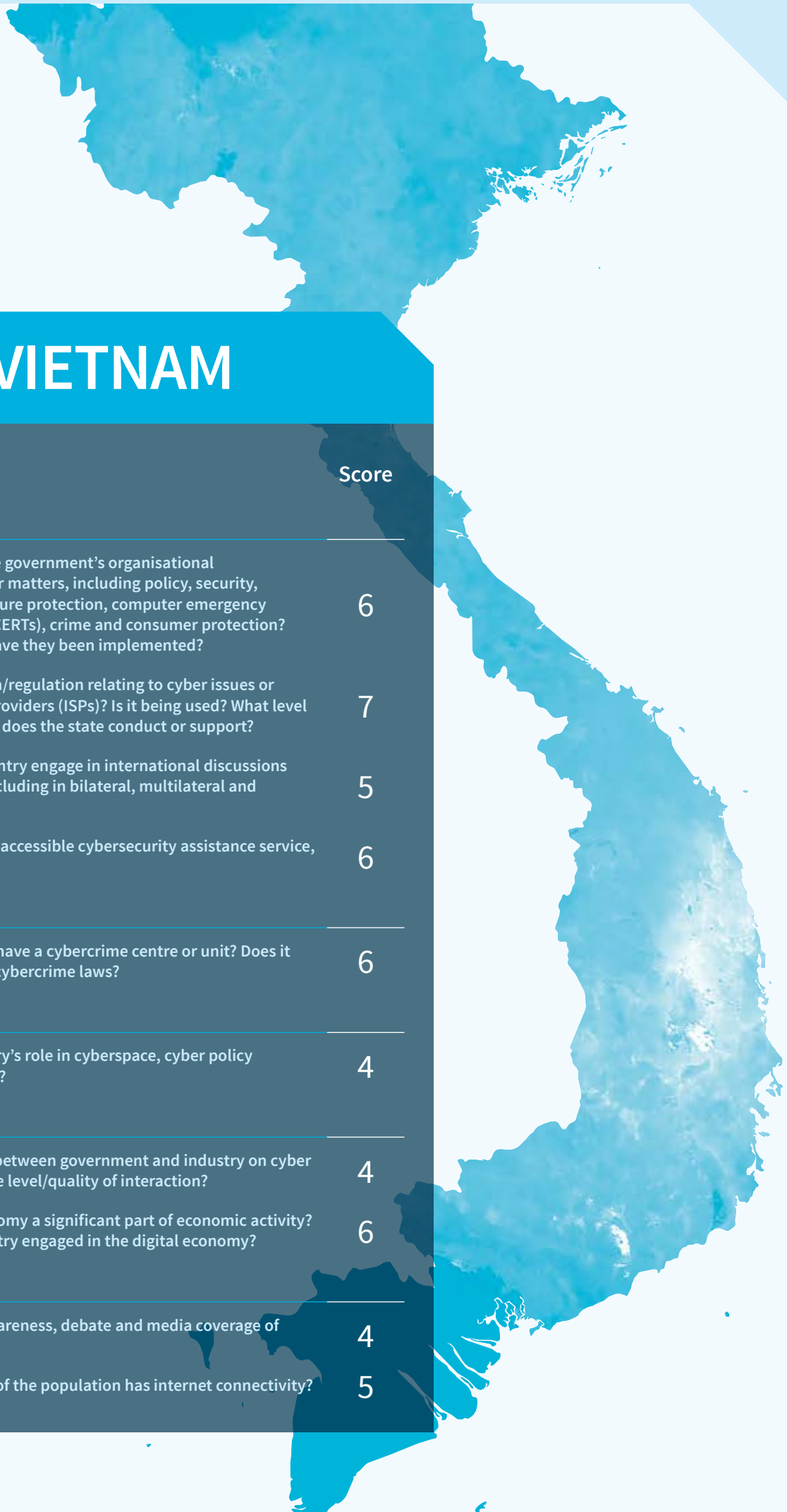
High-profile incidents in 2015 have raised the bar for public awareness and debate in the media, think-tank and academic spheres. Sony and the Office of Personnel Management provide two examples of the engagement of the US public in debates on cybersecurity, in which many demanded that the US take quick action to punish those responsible. The differing US responses in the two cases confused some pundits, while others pointed to the precedent that the US has set in responding to state-sponsored commercial espionage but not the theft of government secrets by foreign powers. Other issues, such as net neutrality, also arouse public interest, as do legislative debates on cybersecurity legislation that arouses the suspicions of privacy advocates.

SCORE: 10

b) What percentage of the population has internet connectivity?

The proportion of US citizens online continues to grow. In 2014, the number of Americans with access to the internet grew by 3%, with 87% of the population now online.

SCORE: 9



VIETNAM

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection? How effectively have they been implemented?	6
b) Is there legislation/regulation relating to cyber issues or internet service providers (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?	6
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 on 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) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has internet connectivity?	5

OVERALL ASSESSMENT

Vietnam has a modest government structure and legislative framework for addressing cyber issues. The government is involved in international efforts to combat cybercrime, but its ad hoc indications of interest in military applications of cyberspace suggest limited capabilities in that area. There's been a natural growth in Vietnam's digital economy, but the government's dialogue with local industries gives minimal attention to cybersecurity issues. For Vietnam to earn a higher score, this area needs improvement.

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 Communication and the National Steering Committee on Information Technology are responsible for implementing the National Strategy on Transforming Vietnam into an Advanced ICT Country. Since 2009, they have produced a yearly *White book on ICT*. In September 2014, the Authority of Information Security was created within the ministry with the role of formulating laws, policies and other documents relating to information security. The authority also coordinates with other government agencies and external stakeholders to improve their information security, works with international organisations and governments and builds public awareness about information security. The Ministry of Public Security houses the Department of Cyber Security, which protects Vietnamese networks and infrastructure in conjunction with VNCERT and the Ministry of Defence.

SCORE: 6

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

Vietnam's legislation includes the *Law on E-Transactions 2005*, the *Law on Information Technology 2006*, the *Management and Use of Internet Services Decree 2001*, the *Telecommunication Law 2009*, the *Criminal Law (2009 amendment)* and the *Law on Protection of Consumers' Rights 2010*. Vietnam's National Assembly is now debating the draft Law on Internet Information Security. The draft law is intended to help clarify organisational cybersecurity arrangements and provide a clear legal basis for prosecuting cybercrimes. It covers three tiers (cyber information violations, cyber information conflicts and cyberwarfare) and is due to be implemented in October 2015. While there's evidence that existing cyber laws are used to prosecute both cybercriminals and online dissidents, more general laws such as the Penal Code are often used instead of newer legislation.

SCORE: 7

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

Vietnam has recently added cyber issues to several of its bilateral dialogues and agreements with regional and other partners. Many of the agreements relate to cooperation and information sharing on cybercrime, but many are also beginning to cover more developed policy and policing discussions. Vietnam also participates in multilateral exercises and policy discussions through ASEAN, ITU-IMPACT and INTERPOL. It was the only Southeast Asian country to sign up to the Global Forum on Cyber Expertise launched at the Global Conference on Cyber Space. Vietnam's score for this indicator would improve with a more active contribution to international cyber policy and conflict prevention discussions through mechanisms such as the ASEAN Regional Forum.

SCORE: 5

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

The Vietnam Computer Emergency Response Team (VNCERT) was established in 2005 as Vietnam's national CERT. VNCERT, which sits within the Vietnam Ministry of Posts and Telematics, implements strategies to help prevent computer security incidents and to act when they occur. VNCERT serves both the government and civil society and has signed memorandums of understanding with private industry leaders, including Microsoft. It's a member of APCERT and shares data, research and early warning notifications with CERTs around the world. VNCERT handles and resolves a significant number of incidents, including phishing, website defacements and malware attacks.

SCORE: 6

2 CYBERCRIME

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

The General Department of the Vietnam Police is home to the Cyber Police Department. The Australian Federal Police assisted the Ministry of Public Security, which controls the Vietnamese Police, to establish a hi-tech crime division in 2007. The team investigates serious technology-enabled criminal activity, has active links to overseas police forces and cooperates in joint investigations and information sharing. In 2014 the Vietnamese Police force investigated more than 400 cybercrime cases. The lack of standardised legal frameworks between Vietnam and other states acts as an obstacle to increased cooperation and the extradition of offenders.

SCORE: 6

3 MILITARY

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

Vietnam's 2004 Defence White Paper noted that the Vietnamese People's Army Technology General Department would work to improve ICT capabilities through research, development and the application of new technologies to help protect the country in 'hi-tech conditions'. The 2009 Defence White Paper made no mention of cyber issues, and the established view is that Vietnam has only minimal defensive capabilities and possesses only limited organisational frameworks. A warming of relations between the US and Vietnam led to the signing of a comprehensive partnership between the two countries in October 2014. The agreement covered enhanced cybersecurity cooperation, which could help to clarify and build Vietnamese thinking on cyberspace.

SCORE: 4

4 BUSINESS

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

There's a relatively strong level of interaction between the government and large state- and foreign-owned corporations. In the case of foreign-owned companies, much of this interaction seems to be geared towards gaining new or increased foreign investment. Engagement on cybersecurity and privacy beyond the work of VNCERT seems to be minimal.

SCORE: 4

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

Vietnam has established the E-Commerce and Information Technology Agency (VECITA) and has implemented the Law on E-Transactions, which is based on the UN Commission on International Trade Laws' Model Law on Electronic Commerce. Vietnam has implemented the National E-Commerce Development Program 2014–2020 and a Decree on E-Commerce. The number of Vietnamese who shop online has grown exponentially in the past few years; some surveys put the proportion at around 12% in 2014.[16] According to VECITA, business-to-consumer e-commerce sales would amount to more than US$4 billion by 2015. The government and several large international companies have established training programs to boost Vietnam's skilled workforce.

SCORE: 6

5 SOCIAL

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

There's an emerging debate about cyber issues, driven mainly by the media and international non-government organisations. The Vietnam Information Security Association collaborates with industry and government to help build information security practices among the general population. In 2015, several high-profile cyberbullying incidents have raised awareness of cyber issues in the community and boosted policing efforts and the implementation of cyber-related laws.

SCORE: 4

b) What percentage of the population has internet connectivity?

Around 48% of the population has internet access. This penetration is largely driven by smartphones, which are owned by a third of the population. Viettel and Mobiphone, two of Vietnam's largest carriers, have expanded 3G infrastructure across the country. Data prices remain some of the world's lowest, contributing to high levels of mobile internet penetration.

SCORE: 5

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 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.

Key indicators	Scoring breakdown
1c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	0 = No international engagement. 1 = Some passive international engagement. 2 = Some intent to engage internationally, as yet unrealised. 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 and policy. 6 = Strong bilateral engagement and some multilateral engagement. 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.
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.

Key indicators	Scoring breakdown
2a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	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.
3a) What is the military's role in cyberspace, policy and security?	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.
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.

Key indicators	Scoring breakdown
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. 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) Is there public awareness, debate and media coverage of cyber issues?	0 = No dialogue on cybersecurity issues. 1 = Very little coverage of cybersecurity issues. 2 = Some coverage, mainly external. 3 = Insubstantial domestic media interest in cybersecurity 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 cybersecurity issues. 8 = Very strong public, media and private-sector debate on cybersecurity issues. 9 = Strong public, media, academic and private-sector debate on cybersecurity issues. 10 = Very strong public, media, academic and private-sector debate on cybersecurity issues.
5b) What percentage of the population has internet connectivity?	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:
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**
US	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 3:
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	Philip-pines	Philip-pines	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**

Note: Due to the inclusion of a new question in 2015, questions 3a), 3b), 4a) and 4b) in Appendix 3 are questions 4a), 4b), 5a) and 5b) respectively in Appendix 2.

APPENDIX 4:
SELECTED KEY INDICATORS

	Freedom on the net report[a]	World Bank World DataBank World Development Indicators: Internet use per 100 people (2014)[b]	FIRST membership[c]	World Economic Forum *2015 Global information technology report*: Knowledge-intensive jobs, % workforce (rank)[d]	ITU–IMPACT membership[f]	APCERT operational member teams[g]
Australia	Free	85	6	43.8 (15)	No	CERT Australia, AusCERT,
Brunei	n.a.	69	1	n.a.	Yes	BruCERT
Cambodia	Partly free	9	0	4.1 (113)	Yes	n.a.
China	Not free	49	4	7.4 (106)	Yes	CCERT, CNCERT / CC
Fiji	n.a.	42	0	n.a.	Yes	n.a.
India	Partly free	18	1	n.a.	Yes	CERT-IN
Indonesia	Partly free	17	1	8.9 (104)	Yes	ID-CERT, ID-SIRTII/CC
Japan	Free	91	24	24.3 (63)	No	JPCERT/CC
Laos	n.a.	14	0	n.a.	Yes	LaoCERT
Malaysia	Partly free	68	2	24.7 (58)	Yes	MyCERT
Myanmar	Partly free	2	0	n.a.	Yes	mmCERT
New Zealand	Free	86	1	42.9 (17)	No	New Zealand National Cyber Security Centre
North Korea	n.a.	0	0	n.a.	No	n.a.
Papua New Guinea	n.a.	9	0	n.a.	Yes	n.a.
Philippines	Free	40	0	23.7 (65)	Yes	n.a.
Singapore	Partly free	82	8	52.7 (2)	No	SingCERT
South Korea	Partly free	84	6	21.4 (70)	No	KrCERT/CC
Thailand	Not free	35	1	13.9 (99)	Yes	ThaiCERT
US	Free	87	70	38.0 (26)	No	n.a.
Vietnam	Not free	48	0	10.0 (103)	Yes	VNCERT

n.a. = not available

a https://freedomhouse.org/report-types/freedom-net#.VdWySJfNx8E

b http://databank.worldbank.org/data//reports.aspx?source=2&country=&series=IT.NET.USER.P2&period=

c https://www.first.org/members/map

d http://www.weforum.org/reports/global-information-technology-report-2015

f http://www.impact-alliance.org/countries/alphabetical-list.html

g http://www.apcert.org/about/structure/members.html

ACRONYMS AND ABBREVIATIONS

ADF	Australian Defence Force
AFP	Australian Federal Police
APCERT	Asia Pacific Computer Emergency Response Team
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
AusCERT	Australia CERT
CamCERT	Cambodia CERT
CBMs	confidence building measures
CCERT	China Education and Research Network Emergency Response Team
CERT	computer emergency response team
CERT-IN	CERT India
CNCERT	China CERT
CNI	critical national infrastructure
CSIRT	computer security incident response team
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)
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
ISP	internet service provider
IT	information technology
ITU	International Telecommunication Union
JPCERT/CC	Japan CERT/Coordination Center
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
MyCERT	Malaysia CERT
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre (Singapore, New Zealand) National Cyber Security Center (South Korea)
NISC	National Center of Incident readiness and Strategy for Cybersecurity (Japan)
NZDF	New Zealand Defence Force
OECD	Organisation for Economic Co-operation and Development
OIC-CERT	Organisation of Islamic Cooperation CERT
PacCERT	Pacific CERT
PH-CERT	Philippines CERT
PLA	People's Liberation Army
PNG	Papua New Guinea
SingCERT	Singapore CERT
ThaiCERT	Thailand CERT
TSUBAME	Internet Traffic Monitoring Data Visualisation Project
UK	United Kingdom
UN	United Nations
UNGGE	UN Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security
US-CERT	United States CERT
USPACOM	United States Pacific Command

NOTES

1 http://www.mckinsey.com/insights/energy_resources_materials/three_paths_to_sustained_economic_growth_in_southeast_asia.

2 http://www1.cnnic.cn/IDR/ReportDownloads/.

3 https://www.pwc.in/en_IN/in/assets/pdfs/publications/2015/ecommerce-in-india-accelerating-growth.pdf.

4 http://www.ekosglobal.com/markets/asia-and-australasia/japan/.

5 http://www.digitalnewsasia.com/digital-economy/pm-najib-announces-more-digital-malaysia-initiatives#sthash.P7rBTZe5.dpuf.

6 http://reports.weforum.org/global-information-technology-report-2014/.

7 http://www.lowyinstitute.org/chinese-aid-map/#.

8 http://web0.psa.gov.ph/content/merchandise-exports-performance-april-2015.

9 https://freedomhouse.org/report-types/freedom-net#.VdWySJfNx8E.

10 http://www.ida.gov.sg/Annual%20Report/2013/infocomm.html.

11 http://reports.weforum.org/global-information-technology-report-2014/.

12 http://www.forbes.com/sites/alanmcglade/2014/02/06/why-south-korea-will-be-the-next-global-hub-for-tech-startups/.

13 https://data.oecd.org/ict/ict-value-added.htm#indicator-chart.

14 https://data.oecd.org/ict/ict-goods-exports.htm#indicator-chart.

15 http://www.buyusainfo.net/docs/x_1061713.pdf.

16 http://www.globalpost.com/dispatch/news/xinhua-news-agency/150302/online-shopping-continues-increase-vietnam-survey.

AUTHOR BIOGRAPHIES

DR TOBIAS FEAKIN

Tobias Feakin joined ASPI as Senior Analyst for National Security in October 2012. He is Director of ASPI's International Cyber Policy Centre and examines issues relating to national security policy, cybersecurity, global counterterrorism, resilience, critical infrastructure protection, and the environment and security. He was previously Senior Research Fellow and Director of the National Security and Resilience department at the Royal United Services Institute for Defence and Security Studies in London, and is still a Senior Associate Fellow of the institute.

JESSICA WOODALL

Jessica Woodall joined ASPI in April 2013. She is currently working in ASPI's International Cyber Policy Centre researching and writing on international and domestic cybersecurity issues. Before joining ASPI, Jessica worked as an analyst in the Department of the Prime Minister and Cabinet and as a researcher in Queensland's Department of the Premier and Cabinet. Jessica holds a Master's in International Affairs degree from the Australian National University.

LIAM NEVILL

Liam Nevill joined ASPI in June 2015. He is currently working in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber policy issues. Before joining ASPI, Liam worked at the Department of Defence on strategic and international defence policy issues. He has previously worked in policy roles in the Department of Health and Ageing and the Northern Territory Treasury. Liam holds a Master of Arts in Strategy and Security and a Bachelor of Arts in History, Politics and International Relations from the University of New South Wales.