CYBER MATURITY IN THE ASIA–PACIFIC REGION 2016

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

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. Peter Jennings was integral to the initial design of this project in 2013, and his ongoing input, insights and guidance have been invaluable. Thanks this year again go to Andrew Davies for his assistance in devising the quantitative elements of the country weightings and ranking system.

A special thanks is reserved for Annaliese FitzGerald for her significant assistance in research and analysis for this report.

WHAT IS ASPI?

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

ASPI INTERNATIONAL CYBER POLICY CENTRE

The ASPI International Cyber Policy Centre (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 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 sponsors.

First published September 2016

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

INTRODUCTION

ASIA–PACIFIC CYBER THREAT TRENDS IN 2016—THE GEOPOLITICS OF INFRASTRUCTURE

In 2015–16, several high-profile network compromises, normally reserved for the most dramatised Hollywood plotlines, unfolded before our very eyes. If 2014–15 was the year of online geopolitical niggling and espionage writ large, 2015–16 quickly followed up as the year of the big infiltration. While many of these incidents occurred far from our region, there are important policy implications, organisational warning signs and lessons for the Asia–Pacific to heed and act upon.

One frequently discussed nightmare cyber scenario is the take-down of critical national infrastructure (CNI) systems, such as energy, water and communications, which could cripple large cities and economic hubs. Events that unfolded in western Ukraine in December 2015 illustrated what's possible when a nation is faced with a determined, sophisticated cyber aggressor. This was the first confirmed cyber incident to take down a power grid, and left more than 230,000 residents without power.

It's expected that by 2020 critical infrastructure security spending in the region will reach US$22 billion. This means that both government cyber policies and regional discussions will need to keep pace with the growing risks associated with this rapid regional development. There's little regional reporting as to what the key threats are, and increased information sharing is urgently needed to get a better grasp on the threat environment. That infrastructure is going to be both simple and complex in its design, with some nations establishing internet and power connections for the first time and others embracing high-end technology such as the Internet of Things (IoT) and smart cities. Rising CNI interconnectivity between nations, particularly within ASEAN, also raises the stakes and reflects the increasingly transboundary nature of CNI security. Asia–Pacific nations have a shared interest in ensuring that the delivery of their critical goods and services is continuous. We're more interconnected than we sometimes like to admit, and this means a situation of shared risk.

Obviously, there are lessons here for increasing resilience, reducing online footprints and boosting the security of industrial control systems, yet for many nations in the Asia–Pacific region simply understanding what their critical assets and services look like would be a good starting point. Each country's domestic circumstances are different and will affect its coordination, policy formulation and regulation in different ways. For some nations, such as China, infrastructure is still largely state-owned and run, whereas in Australia approximately 90% of all infrastructure is now owned by the private sector. Some industries are also much more developed and capable of deflecting incidents than others, even more so than governments in some countries. This makes assigning common roles and responsibilities for critical infrastructure protection a complex task, requiring mature mechanisms for engagement with private-sector owners and operators of CNI and a commonsense approach.

The second key trend over the past year has been the increasing use of data as a tool in national politics and international statecraft. In the past, data acquired through cyber espionage was collected covertly, classified and kept for intelligence analysis or for financial gain. Now, the data's being used as political capital to humiliate the target and cause reputational or financial damage through such actions.

The high-profile theft of US Democratic National Committee emails, opposition research and campaign correspondence in July 2016, and the subsequent release of that information to WikiLeaks, humiliated Democrats during a sensitive time in the election campaign. Clearly designed to have a politically destabilising effect, it raises questions about the use of cyberspace to interfere with democratic processes. With increasing numbers of countries using electronic voting, it also raises the question of whether in an age of the IoT and e-governance we need to reconceptualise what we perceive to be CNI.

We've seen similar tactics used in the Asia–Pacific this year. In July, two Vietnamese international airports had their audio and video systems compromised in an attempt to show offensive and threatening messages in relation to South China Sea disputes. The Vietnam Airlines website was also taken down, and more than 400,000 passengers' data was compromised and 'dumped' online. As with 2015's metric, we're seeing a continuing theme of cyber incidents shadowing events in the physical world. The incident in Vietnam followed on from the ruling of the Permanent Court of Arbitration, which held in favour of the Philippines against China and its claims in the South China Sea. Similarly, the website of the Permanent Court of Arbitration in The Hague was taken offline in 2015, and immediately following the ruling Philippines Government websites were targeted and taken offline.

These incidents highlight the vulnerability of larger powers such as the US, but especially some of the smaller Southeast Asian states, to cyberattacks on their critical infrastructure in response to geopolitical frictions. More than ever, they bring into sharper focus the importance of ensuring that Asia–Pacific governments are responding to the challenges of cyberspace in order to reap the rewards it enables.

GAUGING NATIONAL CYBER MATURITY

This report is the third edition of an annual report examining cyber maturity trends across the Asia–Pacific. It surveys a wide geographical and economic cross-section of the region, encompassing 23 countries from South, North and Southeast Asia, the South Pacific and North America.

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

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

2015–16 MATURITY TRENDS

ASIA–PACIFIC CYBER MATURITY: A GOVERNMENT PERSPECTIVE

Asia–Pacific governments are increasingly engaging with cyber policy issues as the threats and opportunities in cyberspace are better understood by regional policymakers. However, the quality of policy development and implementation remains uneven, and many states have achieved minimal or poor-quality outcomes.

GOVERNANCE GROWTH

In 2016, several states released new policies or strategies, and there was significant movement on new legislation, particularly in Southeast Asia. They have updated existing frameworks to adapt to emerging challenges and address issues in the effectiveness of those frameworks.

In April 2016, Australia launched its long-awaited Cyber Security Strategy, which promises additional funding and deeper private-sector engagement on cyber policy. New Zealand also delivered its new national Cyber Security Strategy in December 2015, focusing on improving its cyber resilience, capability, international cooperation and cybercrime response.

Cambodia, Laos, Thailand, China, Papua New Guinea and Pakistan have passed new legislation relating to cyber issues, particularly cybercrime, during the past year. Cambodia's new Telecommunications Law and other legislation (which the US is advising on) covering e-commerce and cybercrime are promising examples of growth in cyber maturity in one of the region's cyber underperformers. Laos has also passed new cybercrime legislation that has used definitions from the Council of Europe's Convention on Cybercrime. New cybercrime legislation in Southeast Asia is likely to be driven by an awareness of the opportunities presented by the ASEAN Economic Community, which was formally established on 31 December 2015.

Last year's report noted that governments were increasingly centralising control of cyber policy issues, and that has continued in 2016. Following the release of its new Cyber Security Strategy, Australia has appointed its first cyber minister (Dan Tehan, the Minister Assisting the Prime Minister for Cyber Security) and appointed a new centre-point for government policy (Alastair MacGibbon, Special Adviser to the Prime Minister on Cyber Security).

In Thailand, the establishment of a new ministry to manage digital economic growth is a positive sign of action to embrace the potential of cyberspace. Indonesia committed to establishing a new National Cyber Agency in 2015, but this appears to have been cancelled due to budget difficulties. Other countries, particularly those that are more focused on increasing low levels of connectivity, have generally retained weak policy structures, usually focused on ministries responsible for the management of telecommunications.

MILITARY USE OF CYBERSPACE

How Asia–Pacific militaries are engaging with cyberspace and planning for its use in warfare remains a difficult topic to research. However, in 2016 some regional countries made new disclosures of capability and intent that indicate a growing confidence in the approach of their militaries to integrating cyberspace into modern conflict. As for other indicators, awareness is uneven across the region, as is evidence of work to mitigate cyber threats or develop offensive capabilities.

In 2016, both Australia and New Zealand revealed that they have offensive cyber capability. Australia made this announcement in its new Cyber Security Strategy, which was released after the new Australian Defence White Paper. This means that the Defence White Paper, while committing to new personnel and funding, does not discuss in great detail Australia's views on how and when it might use such capability, or the Defence organisation's broader approach to cybersecurity and operations generally. Conversely, New Zealand chose to discuss its new offensive cyber capability, which it calls its 'cyber support capability' in its Defence White Paper. However, as in Australia, ambiguity remains about the funding, scale and authorities of New Zealand's offensive cyber capabilities.

The other significant development in 2016 was that the US publicly discussed for the first time its use of offensive cyber capability against an adversary, noting that it's conducting operations in cyberspace against Islamic State. Reporting on these operations is scarce, but what has emerged has indicated that they haven't met the expectations of senior US commanders. The US is struggling to recruit the 6,200 cyber personnel it has planned for—a symptom of broader cyber skills shortages across the board.

New national defence policies in Indonesia and Malaysia provide greater detail of how those countries view cyber threats and the role of cyberspace in warfare more generally. Indonesia's Defence White Paper depicts cyberspace as an asymmetric weapon for non-linear warfare, and also displays a good understanding of its broader role in providing integrated support for military operations. Malaysia's National Defence Policy frames cybersecurity within the context of 'information dominance', assessing that the collection and secure dissemination of superior information enhances Malaysia's combat power. Thailand has also advanced its military cyber capability, establishing a new cybersecurity centre.

There's a notable lack of action from some Asia–Pacific armed forces on cyber threats. Many of them, such as those of Cambodia and Laos, don't have the vulnerability of more advanced militaries because they don't operate modern networked capabilities. Other countries have noted the cyber threat to their military capability, but haven't taken action to mitigate threats or establish cybersecurity centres or units. The Philippines and India are notable in this regard: they outlined plans in previous years to establish new cyber units, but no action was recorded in 2016.

INTERNATIONAL ENGAGEMENT

In 2015–16, countries with the highest levels of internationally orientated cyber maturity engaged in an expansive bilateral and multilateral program of activities, dialogues and capacity-building efforts across cyber thematic areas including conflict prevention, diplomacy, policing, and collaboration between computer emergency response teams (CERTs). It's no coincidence that countries that have established both a leadership position for international cyber engagement (such as an ambassador for cyber affairs) and a stand-alone strategy for international cyber engagement (Japan, the US and soon Australia) are carrying out some of the most mature and coordinated engagement efforts in the region.

Barring a few notable hotspots, such as North and South Korea, instances of geopolitical tensions manifested in cyberspace have lessened in comparison with recent years, as the Snowden leaks have increasingly faded into the rear-view mirror. While a bubbling undercurrent of online espionage certainly persists, by and large the region appears to have matured as a whole, seeming eager to get on with business and to collaborate practically against mutual threats. This can be seen in the number of high-level agreements and memorandums of understanding (MoUs) signed this year, most notably between China and the US. The two countries made a mutual undertaking to not engage in theft of intellectual property for the benefit of their respective commercial sectors and additionally agreed to cooperate in countering online organised crime.

Beyond bilateral agreements, there have been two additional cyber workshops this year within the purview of the ASEAN Regional Forum, designed to build confidence and prevent conflict during periods of heightened tension and to strengthen cyber incident response frameworks. The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) will meet again in 2016–17 to push forward discussions on norms for appropriate behaviour online, with a particular focus on consolidating and implementing norms put forward during previous discussions. Several Asia–Pacific countries, such as Indonesia, India and Australia, will make a return to the UNGGE in what will be an important year for establishing the vehicle for continuing discussion of the norms agenda after 2017.

CERT–CERT engagement continues to be an important means for breaking down barriers between countries in the region, and the Asia–Pacific team (APCERT) continues its vital role in this area. But concerningly, some national CERTs seem to have cut back on their international engagement, often for resourcing or budgetary reasons. There's a clear opportunity in several Southeast Asian countries and the Pacific islands more broadly to help build vital CERT capacity. Although not included in this year's metric, Tonga's new CERT is an excellent example of what can be achieved with proactive and enthusiastic internal and external cooperation and capacity building.

A BUSINESS PERSPECTIVE

The internet is now so intertwined with our economies and everyday lives that it's easy to forget that it's only 25 years old. In the Asia–Pacific, it's useful to pause and comprehend how quickly the internet has enabled so much social and economic capital in such a relatively short time. Since the emergence of the internet, the Asia–Pacific has had a fundamental change in its financial evolution from one of the more economically immature regions of the world to one of the most dynamic international markets, in which almost every country is working to leverage the market opportunities presented by the online world.

Economic growth in the Asia–Pacific continued in 2016. It's expected that the region's economy will grow by some 6.3% this year and that it will continue to account for one-third of total global growth (twice the combined contribution of all other developing regions). In the Asia–Pacific, the digital economy is rapidly becoming a larger percentage of national and regional GDP. As digital infrastructures expand their reach, often enabled by internet-connected mobile devices, new services are being made accessible to more people.

Yet while there are some encouraging new growth patterns in the digital domain, there are still obstacles to overcome. Many governments are developing policies to foster digital economic growth but have understandable problems in prioritising those policies over more pressing development needs, such as access to health and education.

India exemplifies this regional dichotomy well. The Modi government has made some impressive moves to develop a large skilled workforce. Through its Skill India program, and partnering with Google, India will train 2 million Android developers across the country over the next three years. It's hoped that the program will reach 2,000 universities and train 4,000 faculty in a bid to train more than 250,000 developers each year. India's the world's second-largest user of mobile apps and is expected to have the largest developer base in 2017–18.

India's IT industry contributed 25% of India's total exports in 2012–13, and the Modi government recognises that the digital economy has significant potential to accelerate the country's development. However, the 12.5 million people employed directly and indirectly by the IT sector amount to a mere 2.5% of the national labour force of 496 million in a country with 1.25 billion people, and India remains a predominantly agrarian society. Seven out of 10 Indians live in villages, and a little over half of the nation's workforce is engaged in agriculture and allied activities. Unless India works more actively to diversify its workforce through training, education and the proactive implementation of sound cyber policy, its digital economy will remain an unharnessed jewel in the emerging modern Indian economy.

There are also some concerning cases of over-regulation, in which stiff, top-down attempts to assert government control of cyberspace are inhibiting the fulfilment of some countries' digital potential and undermining the prosperity that flourishing digital economies can bring.

Countries such as Laos, which has had a history of difficult relations with foreign mobile telecommunications carriers, are at risk of regulating their digital economic growth into the ground. Reactionary over-regulation for security, information control or economic reasons is concerning, as it has the potential to slow or even reverse the encouraging development of e-commerce markets in Southeast Asia and further afield. Rather than restricting the parameters of growth through overzealous telecommunications market and online controls, these countries should be shaking off the shackles in order to allow a boom in those markets over the coming years.

Fortunately, there's still enormous potential for the Asia–Pacific in its increasing adoption of disruptive business models. Many people in the region don't yet have credit cards or even bank accounts. This is inhibiting the growth of e-commerce and creates a reliance on 'cash on delivery' models, which account for about 95% of total sales transactions in countries such as Pakistan. There's significant potential for the increase in mobile phone internet access and new fintech models to turn the region's 'underbanked' and 'unbanked' into participants in the digital economy. This will have significant implications for Asia–Pacific growth by encouraging online purchases and the use of other digital services. The increased requirement for investments in sound cyber policy and proactive cybersecurity across government and the private sector is clearer than ever before.

CYBERCRIME

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

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

This broad range of Asia–Pacific cybercrime maturity is generating interesting trends in the origins and flow of malicious internet traffic. Cybercriminals are seeking out the points of least resistance in the Asia–Pacific. Jurisdictions with little cybercrime legislation, or weak enforcement, are attracting cybercriminals as vantage points from which to conduct attacks into the networks of more advanced countries. For example, South Korean nationals have been carrying out attacks from Cambodia and the Philippines, and similar tactics are being used by Taiwanese criminals in Indonesia.

This is intensifying the Asia–Pacific's understanding of cybercrime as a transnational issue, and one that requires robust cooperation efforts. In response, we're seeing growing collaboration between national cyber law enforcement agencies in order to apprehend and convict cybercriminals. The September 2015 cybercrime agreement between China and the US, resulting in collaborative cybercrime arrests between the Chinese Government and the Federal Bureau of Investigation (FBI) stands out as a significant development. Such bilateral cooperation is combined with permanent multilateral institutions that combat cybercrime as collectives, such as ASEANPOL and INTERPOL.

Sophisticated countries are also continuing to work to improve the local cybercrime capabilities of 'weak-link' countries so that they can address the problem on their own in the future. Countries such as the US, Australia, South Korea and Japan are extending capacity-building efforts, offering training in cybercrime detection and enforcement to countries including Bangladesh, Myanmar and Fiji.

A growing awareness that a secure online environment is a prerequisite for the region fulfilling its enormous digital economic potential and reaping the associated financial rewards is driving stronger efforts to combat cybercrime across the board in the Asia–Pacific.

METHODOLOGY

CHANGES TO THE METHODOLOGY

The ICPC is committed to continual refinement of the method used to develop this report. In 2016, we have made some further changes to ensure that it continues to reflect the development of cyber policy and security issues in the region. We have also included three new countries (Solomon Islands, Bangladesh and Pakistan), bringing the total number of countries assessed to 23.

In 2016, the only major change is the division of the question on internet connectivity (question 5b in 2015), into separate questions for fixed (5b) and mobile (5c) broadband subscriptions. The weight for both 5b and 5c has been set at the weight used for question 5b in 2015 (7.0). This change has been made to better reflect the development of connectivity in the region through increased access to mobile connectivity, particularly in countries that don't have legacy fixed telecommunications infrastructure. The scores are based on data supplied by the International Telecommunication Union (ITU), and there may be discrepancies between this data and other published figures. Using a single dataset for these questions means that our assessment is based on a common dataset for all countries reviewed.

Minor word changes have been made to the scoring breakdown (Appendix 1). Those changes were made to provide greater clarity about the breakdown and don't have a substantive effect on the final result.

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 Asia–Pacific states.

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

Strong organisational structures within government for dealing with cyber matters suggest an awareness of those issues. The effectiveness and breadth of the structures are indicators of the sophistication of governments' awareness 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 Asia–Pacific.

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

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

d) Is there a publicly accessible cybersecurity assistance service, such as a Computer Emergency Response Team (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.

e) 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 Asia–Pacific 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, are indicators 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 fixed broadband internet connectivity?

c) What percentage of the population has mobile broadband 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 has been divided between fixed broadband and mobile broadband subscriptions.

COMPONENTS OF THE METHODOLOGY

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

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

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

In the final step, each country was then rated against the 10 factors, 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 possible, a comparison with the 2014 and 2015 research and results.

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

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

where $\overline{S}$=Weighted Score, S=Score and w=weight.

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

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

TABLE 1: WEIGHTING ASSIGNED TO EACH CATEGORY, 2016

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)	Fixed broadband penetration
7.0	5c)	Mobile broadband penetration

TABLE 2: WEIGHTED SCORES, 2016

Country		Weighted score
1	United States	88.1
2	South Korea	83.6
3	Japan	82.9
4	Australia	80.9
5	Singapore	80.2
6	New Zealand	74.6
7	Malaysia	67.7
8	China	63.0
9	Thailand	52.7
10	India	48.4
11	Vietnam	48.1
12	Indonesia	47.4
13	Brunei	42.8
14	Philippines	41.6
15	Cambodia	30.0
16	Bangladesh	28.3
17	Myanmar	28.1
18	Pakistan	26.6
19	Fiji	25.3
20	Laos	21.3
21	Papua New Guinea	18.7
22	North Korea	16.7
23	Solomon Islands	11.9

TABLE 3: COUNTRY SCORES, BY CATEGORY, 2016

Country	1a	1b	1c	1d	2	3	4a	4b	5a	5b	5c	Weighted score
Australia	8	8	9	8	9	8	8	9	9	3	10	**80.9**
Bangladesh	4	3	2	2	3	1	4	4	5	1	2	**28.3**
Brunei	6	6	4	6	5	4	5	5	3	1	1	**42.8**
Cambodia	4	4	3	3	2	1	3	3	4	1	5	**30.0**
China	9	7	9	6	6	8	5	6	5	2	6	**63.0**
Fiji	2	4	3	0	4	1	2	3	3	1	5	**25.3**
India	7	5	7	5	4	3	5	7	7	1	2	**48.4**
Indonesia	5	5	5	6	4	6	5	5	5	1	5	**47.4**
Japan	9	8	9	10	8	7	8	9	9	4	10	**82.9**
Laos	4	3	2	3	1	1	2	2	2	1	2	**21.3**
Malaysia	7	7	8	8	6	6	7	8	6	1	10	**67.7**
Myanmar	3	4	4	3	2	5	1	2	2	1	4	**28.1**
New Zealand	8	8	6	7	7	6	8	9	9	4	10	**74.6**
North Korea	3	1	3	0	0	8	0	1	1	1	1	**16.7**
Pakistan	3	3	2	1	4	4	4	3	2	1	2	**26.6**
Papua New Guinea	4	3	2	0	1	1	2	1	5	1	1	**18.7**
Philippines	5	6	5	0	6	3	4	5	6	1	5	**41.6**
Singapore	9	8	7	7	8	8	10	9	9	3	10	**80.2**
Solomon Islands	3	0	2	0	1	0	2	1	1	1	2	**11.9**
South Korea	8	9	8	8	8	9	9	9	9	5	10	**83.6**
Thailand	6	6	5	5	5	5	4	6	6	2	8	**52.7**
United States	10	8	9	8	10	10	9	9	10	4	10	**88.1**
Vietnam	6	7	5	6	6	3	4	6	4	1	4	**48.1**

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 we 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 subquestion. 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 AND DEVELOPMENT

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

DEVELOPMENT

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

TABLE 4: ASIA–PACIFIC CYBER ENGAGEMENT OPPORTUNITIES

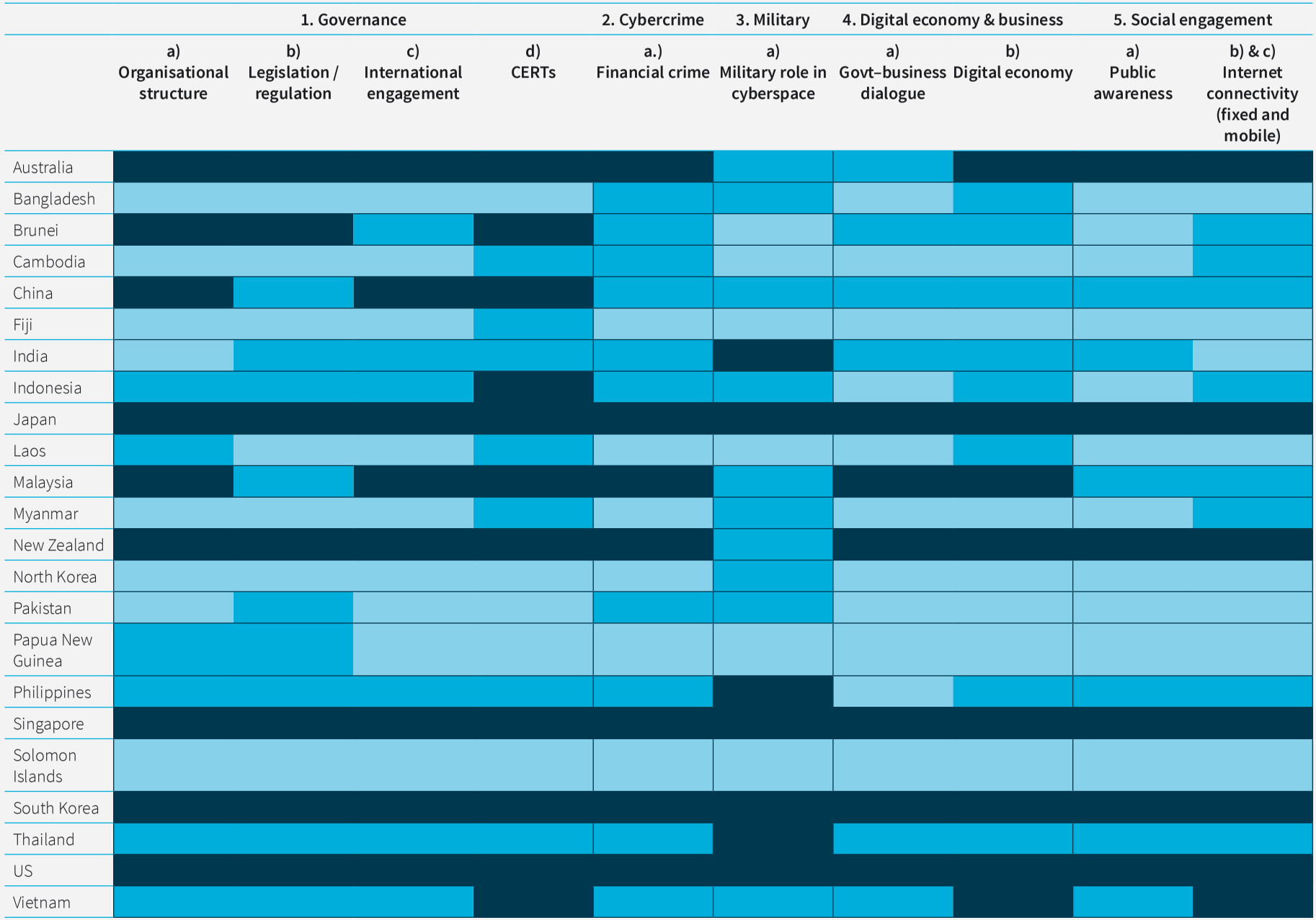


TABLE 5: ENGAGEMENT OPPORTUNITIES INDICATORS

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

Indicator	Mature engagement	Engagement & 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 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's cyber concerns. • Healthy business environment for investment on cyber issues.	• Limited government–business dialogue on cyber issues, characterised by one-sided interactions or inability to act on areas of concern.	• Little or no government–business dialogue.
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	• Strong digital economy business culture, including clear concerns about cybersecurity, supply-chain security and other cyber issues. • Highly educated and knowledgeable workforce. • Solid, digitally developed business environment for investment.	• Digital economy is a growth area. • Strong potential for investment, especially in digital infrastructure.	• Few near-term investment opportunities in the digital economy.
5—SOCIAL			
a) Are there public awareness, debate and media coverage of cyber issues?	• Strong public awareness of cyber issues through new and traditional media outlets. • Cyber-knowledgeable end-users and wide adoption of digital media offer strong opportunities for business-to-customer interactions.	• Some awareness of cyber issues, mainly limited to new media (blogs, social media). • Opportunity to aid in the building of civic understanding of cyber issues.	• Little or no public awareness of cyber issues. • Opportunity for wide range of educational, outreach and capacity-building efforts on cyber issues.
b) What percentage of the population has fixed broadband 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.
c) What percentage of the population has mobile broadband 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

Rank 2016: 4th

2015: 5th

↑

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	8
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	8
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	9
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has fixed broadband internet connectivity?	3
c) What percentage of the population has mobile broadband internet connectivity?	10

OVERALL ASSESSMENT

The release of Australia's new Cyber Security Strategy, the first since 2009, as well as the National Innovation and Science Strategy and Defence White Paper, has revitalised the approach of the Australian Government to cyber policy, cybersecurity and digital commerce. Strong steps to implement these programs have begun, but are not yet complete. Australia is an Asia–Pacific leader in cybercrime enforcement and engagement, CERT engagement activities and global discussions on norms and confidence building. More work on public–private partnerships has begun, but will need to focus on closer engagement with critical national infrastructure operators to ensure the effectiveness of whole-of-nation cybersecurity measures.

WEIGHTED SCORE 80.9

1 GOVERNANCE

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

Australia's increased score for this category reflects the successful delivery of the Australian Cyber Security Strategy in April 2016. The strategy, in conjunction with the National Innovation and Science Agenda and the Defence White Paper, sets clear goals for the Australian Government to secure cyberspace and enable greater digital economic growth. The establishment of new leadership positions (the Minister assisting the Prime Minister on Cyber Security, the Special Adviser to the Prime Minister on Cyber Security and a Cyber Ambassador) is evidence of the importance the government places on cyber policy issues and a move to have clearer responsibilities and accountabilities for cyber policy decisions. The repercussions from the recent suspension of Australia's Census website aren't yet known, but that event should focus further attention on the implementation of the Cyber Security Strategy and government cyber incident management arrangements. Continued progress in implementing the strategy should see Australia's score for this category increase further in future years.

SCORE: 8

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

There have been no significant changes in Australian legislation and regulations relevant to cyber issues in 2016, and Australia's score for this category remains steady. New legislation to be considered by parliament in the second half of 2016 mandates the disclosure of serious data breaches, compels organisations to notify customers affected by data breaches and imposes civil penalties for serious or repeated infringements of mandatory disclosure requirements. The penalties may apply even if a company is unaware of a data breach but would reasonably be expected to have detected it. The government has also issued guidelines that clarify 'best practice' for agencies that may invoke section 313(3) of the Telecommunications Act to interrupt or disrupt access to online services to assist law enforcement and national security agencies.

SCORE: 8

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

Australia maintains steady efforts to achieve its international cyber policy goals, and its score for this category remains unchanged. The Cyber Security Strategy outlines three key areas for Australia's international cyber engagement efforts: championing a free, open and secure internet; preventing cybercrime; and building Asia–Pacific cybersecurity capacity. The impending appointment of Australia's first Cyber Ambassador and the development of a specific international cyber engagement strategy should see greater definition of ends, ways and means to achieve those goals in 2017 and beyond.

SCORE: 9

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Australia's national CERT, CERT Australia, received additional funding and responsibility in the new Cyber Security Strategy. A further $21.5 million to expand the agency's capacity and $2 million to expand the government's cyber exercise program to include private-sector partners are welcome enhancements to CERT Australia. Greater private-sector engagement will also be enabled by its movement out of an intelligence agency building, announced in the Cyber Security Strategy. CERT Australia also has a strong role in the Asia–Pacific CERT community as the chair of APCERT and maintains excellent links with the private sector, In 2015, it collected and published data from its private-sector partners in the first Australian Cyber Security Centre survey of major Australian businesses.

SCORE: 8

2 CYBERCRIME

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

The Australian Federal Police and state law enforcement agencies maintain strong capabilities to monitor and enforce financial cybercrime, and an online reporting tool (ACORN) that assists law enforcement efforts. Australia is an active participant in Asia–Pacific and international efforts to counter financial cybercrime, including by supporting INTERPOL's Virtual Global Task Force and Cyber Safety Pasifika and by assisting countries such as Indonesia to train police in cybercrime detection and enforcement. Australia's strong domestic capability and extensive international engagement efforts mean it maintains a high score for this category.

SCORE: 9

3 MILITARY

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

The announcement that the Australian Signals Directorate maintains offensive cyber capabilities was a significant development for Australia in this category in 2016. However, there's very little detail available on how Australia might use that capability, and details of other ADF cybersecurity roles and capability are similarly slim. The announcement of offensive cyber capability was made as part of the new Cyber Security Strategy, rather than the Defence White Paper that preceded the strategy. While the White Paper makes a welcome commitment to new funding and staff for cybersecurity operations and research, it doesn't describe the Defence organisation's approach to cybersecurity and operations. Further evidence of a sophisticated understanding and approach to cyber operations, such as an unclassified policy, is needed before Australia's score for this category can increase further.

SCORE: 8

4 BUSINESS

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

The Australian Government consulted extensively with the private sector in the development of the Cyber Security Strategy, and has committed to a 'National Cyber Partnership' between government and the private sector in implementing the strategy. This should include an annual cybersecurity leaders' meeting with the Prime Minister and business leaders, a streamlining of cybersecurity governance structure, the relocation of the Australian Cyber Security Centre to enable greater cooperation, and the establishment of 'joint cyber threat centres' and online cyber threat sharing portals. This commitment to public–private partnership and a genuine role for the private sector in influencing national cyber policy have increased Australia's score for this category; however, sustained commitment to this level of engagement is needed to maintain or elevate Australia's score further.

SCORE: 8

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

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

SCORE: 9

5 SOCIAL

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

The Australian public has a general awareness of cyber issues, and there has been a range of opinions in mainstream media on general cyber threats and other topical cyber issues in 2016. This has included encryption, privacy and security of information, particularly concerning the cyber incident affecting the Census website. However, there's minimal discussion on international cyber policy and governance issues, such as internet governance and norms. Commentary and research on cyber issues from think tanks and the academic community is growing, and new academic cyber centres flagged in the Cyber Security Strategy should increase the research focus of this sector on cyber issues.

SCORE: 9

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 3

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 10

Australia has a high rate of internet connectivity: 27/100 Australians have a fixed-line broadband internet subscription, and 112/100 have an active mobile broadband subscription. The World Economic Forum has noted that, despite high rates of connectivity in Australia, prices for broadband subscriptions remain high by world standards.

BANGLADESH

Rank 2016: 16th

2015: NA

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

OVERALL ASSESSMENT

Bangladesh faces significant hurdles in becoming a digital society. Poor infrastructure, including for telecommunications and electricity generation, complicate connections with the internet, and low rates of literacy persist. Despite a clear awareness in government, the business community and parts of Bangladeshi society of the potential benefits of cyberspace for the country's development, Bangladesh has struggled to develop and implement appropriate measures to build its connectivity and cybersecurity. This was brought home in 2016 when the Central Bank lost US$80 million to cybercriminals.

WEIGHTED SCORE 28.3

1 GOVERNANCE

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

Bangladesh's 2008 National Cyber Strategy indicated that the government was intending to establish a National Coordinator for Cybersecurity and a National Cyber Council; however, neither appears to have been established. Prime Minister Sheikh Hasina's 'Digital Bangladesh' election policy has informed the 2015 revision of the national broadband policy. It aims to maximise the use of technology to enable better government services, promote digital development and reduce regulation. However, it's been criticised for its complexity: it contains 10 special objectives, 56 strategic themes and 306 action programs. The ICT Division of the Ministry of Posts appears to be the policy lead for government, overseeing the Bangladesh Telecommunication Regulatory Commission and the Bangladesh Computer Council. Improved policy development and implementation are needed for Bangladesh to score higher for this category.

SCORE: 4

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

Bangladesh's *Information and Communication Technology Act* and *Telecommunication Regulation Act* are the chief legislative instruments for the management and regulation of cybersecurity and cybercrime. The ICT Act has been criticised for the wide remit it grants law enforcement to confiscate computer equipment, which it's been suggested was included to protect government agencies involved in surveillance. A new *Digital Security Act* has been discussed in the media, but it's not clear whether it has been enacted. It includes 20-year jail sentences for 'cyber terrorism' and allows suspects to be arrested without a warrant. The *Pornography Act* and the *Indecent Advertisement Act* have also been applied to the internet, and it appears that much effort is expended on regulating content considered indecent or false, including information critical of the government.

SCORE: 3

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

Bangladesh's international cyber engagement appears to be limited in scope and reach. It has discussed cybersecurity in bilateral engagements with the US and China, and engaged in technical groups including APCERT and IMPACT. It's also a member of the Conference on Interaction and Confidence Building Measures in Asia, and hosted a conference on digital government in March 2016. Bangladesh would need to engage more widely on cyber issues and become more involved in international confidence and capacity building to improve its score for this category.

SCORE: 2

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Bangladesh's bdCERT was established in 2007 and consists of 12 volunteers who are otherwise employed in the IT industry. It's is a member of APCERT, TSUBAME and OIC-CERT and participates in some international CERT exercises. Limited information is available on bdCERT's capacity to handle cyber incidents.

SCORE: 2

2 CYBERCRIME

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

The Ministry of Home Affairs appears to have a cybercrime investigation cell, and the police are reportedly establishing an 'IT Crime Forensic Lab' within the Forensic Division. Bangladesh has received assistance from South Korea and the US to train police in cybercrime investigation, particularly after the cyber theft of US$80 million from the Central Bank. Australia has also expressed an interest in training Bangladeshi police. Stronger evidence of financial cybercrime enforcement capacity and engagement with international partners is necessary for Bangladesh to score higher for this category.

SCORE: 3

3 MILITARY

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

There's limited information available to suggest that Bangladesh's armed forces have an adequate awareness of cyber threats or have taken action to mitigate them. The Directorate General of Forces Intelligence is understood to have some cyber surveillance capability.

SCORE: 1

4 BUSINESS

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

Engagement between the government and the private sector on cybersecurity and the digital economy appears to be largely government-led. It's not clear whether the emerging digital business community has significant opportunities to influence government policy to enable the growth of the sector. The government has partnered with foreign firms, such as Infosys from India, to establish new technology parks to encourage the growth of Bangladesh's digital economy, particularly the software development and graphic design industry. Further evidence of two-way engagement between the public and private sectors on cyber issues is required for Bangladesh's score to improve.

SCORE: 4

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

Bangladesh's government recognises the opportunity that the digital economy offers to advance the development of the country. Dhaka's start-up scene is growing, and local apps and online services for music streaming and grocery delivery are emerging as digital payments start to roll out. Some overseas tech companies have invested in Bangladesh's start-up industry and several incubators have been established, but venture capital is in short supply and government policy restricts local venture funds. The digital economy remains a small proportion of overall economic activity, accounting for less than 0.5% of total jobs.

SCORE: 4

5 SOCIAL

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

Bangladeshi media coverage of cyber policy and security has focused on new cybercrime legislation, the Central Bank hack and occasionally on the development of the digital economy. This coverage indicates that there's a keen awareness among some that government policy and legislation regarding cybercrime have allowed the government to arbitrarily block content and access. An example of this was the blockage of Facebook and messaging apps for 22 days in 2015 by the government, which cited security concerns.

SCORE: 5

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 2

Bangladesh has undertaken to expand the reach of internet connectivity in recent years, including by establishing village centres to provide low-cost internet access. However, poor infrastructure, cost and low literacy mean that connectivity remains low. The mobile sector in Bangladesh continues to grow. The World Economic Forum estimates that Bangladesh's six mobile phone operators serve 131 million subscribers, 55 million of whom use mobile internet services.

BRUNEI

Rank 2016: 13th

2015: 10th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	6
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	4
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	5
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	3
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	1

OVERALL ASSESSMENT

Brunei has shown little change in its national approach to cyberspace this year. Overbearing government regulation is stifling the development of its digital economy, and strong censorship laws inhibit the maturation of the social debate. This focus on content control continues to detract from efforts against cybercrime, and Brunei's international cooperation remains limited and technically focused. Improving the affordability of Brunei's internet services will help increase connectivity and support further growth of the digital economy.

WEIGHTED SCORE 42.8

1 GOVERNANCE

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

The Prime Minister's Office oversees multiple agencies that manage infrastructure development, the ICT industry and the delivery of national cybersecurity services. Brunei continues to implement long-term strategies for ICT development that include the 2009 E-government Plan, the 2014 National Broadband Policy and the 2015 Digital Government Strategy. These measures aim to diversify the Bruneian economy and streamline the delivery of government services. Brunei's complex bureaucratic structure for ICT governance continues to undermine the efficiency of policy delivery. Clearly defined departmental roles would boost Brunei's score for this category.

SCORE: 6

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

The Broadcasting Notification of 1998, the *Copyright Act* of 2000, the Broadcast Notification of 2001, the Internet Code of Practice of 2001 and the *Computer Misuse Act* of 2007 form Brunei's cyber legislative framework. These laws outline provisions for cybercrime, electronic transactions, copyright infringement and digital content regulation. The last continues to be a strong government focus to ensure that online material is not subversive and aligns with Brunei's centrally directed religious values.

SCORE: 6

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

Brunei's international engagement is mostly focused on the Asia–Pacific and on technical issues. It participates in APEC and ASEAN cybersecurity discussions and is a member of various CERT organisations, including APCERT, the Forum Incident Response and Security Teams (FIRST) and the Organisation of Islamic Cooperation CERT (OIC-CERT). It hosted IMPACT conferences in 2010 and 2012 and as part of the Asia–Pacific Telecommunity in 2014. However, since that time Brunei has taken little action in broader multilateral engagement, reducing its score for this category.

SCORE: 4

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

BruCERT was established in May 2004 in collaboration with the Authority for Info-communications Technology Industry and the Ministry of Communication. Brunei is a member of APCERT, FIRST and OIC-CERT. Its score for this category would be enhanced if its CERT were to engage and cooperate more closely with the Asia–Pacific CERT community.

SCORE: 6

2 CYBERCRIME

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

The Commercial Crime Investigation Division in the Royal Brunei Police Force is responsible for managing cybercrime in Brunei. The division uses its digital forensic skills to address domestic cybercrime. Brunei must demonstrate more willingness to engage and cooperate with international cybercrime partners in order to raise its score for this category.

SCORE: 5

3 MILITARY

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

Brunei is cognisant of the threat that cyberwarfare poses to its national security, economic stability and military decision-making superiority. Its 2011 Defence White Paper recognised the importance of adopting strong defences for its networks in order to withstand a potential cyberattack. Clear implementation of policies that achieve that goal and instil cybersecurity by design in military acquisitions may raise Brunei's score for this category.

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 acknowledges the value of the private sector in driving the digital economy and has sought to foster dialogue with industry to help drive growth in this area. The Brunei Information Technology Council brings together government and private-sector representatives and is the lead organisation driving the expansion of Brunei's ICT sector. Measures to improve ICT infrastructure and digital services are outlined in the country's 2008 Strategic Plan and 2009 E-government Strategic Plan; however, the dialogue is dominated by government. Closer collaboration with the private sector in this space would increase 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's economy has traditionally been reliant on the exploitation of natural resources such as oil and gas; however, the government recognises the economic value of developing a digital sector. Brunei's plan to transform its economy starts with getting people connected—expanding internet infrastructure, lowering service costs and improving broadband connection as outlined in the 2014 National Broadband Policy. However, strong government regulation inhibits organic bottom-up growth, and that will need to be adjusted in order to achieve Brunei's digital potential.

SCORE: 5

5 SOCIAL

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

State regulation means there's little evidence of significant public awareness, debate or media coverage about cybersecurity and cyber policy in Brunei. Debate is limited due to strict government content control; many press outlets are state-owned and others self-censor. As a result, Brunei came 121st out of 180 countries in the 2015 Reporters without Borders Press Freedom Index. The liberalisation of online discussion forums and a relaxation of regulations will be necessary to help overcome this issue and strengthen national cyber debate.

SCORE: 3

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 1

According to ITU statistics, Brunei is the only country in this study in which more people connect to broadband internet via fixed-line infrastructure rather than through mobile devices (8% and 4%, respectively). Other reports indicate that Brunei possesses strong internet infrastructure, and that more than 99% of all internet subscriptions are broadband. Local telecom leader, Telbru, introduced a nationwide Wi-Fi initiative in December 2015. While the use of mobile cellular devices has risen above 100%, the low take-up of mobile broadband connectivity may be reflective of the very high cost of Brunei's services. The discrepancy between ITU and Brunei Government data means that some caution must be used when assessing this indicator.

CAMBODIA

Rank 2016: 15th
2015: 18th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	4
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	3
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	3
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	5

OVERALL ASSESSMENT

Cambodia has made steady gains in some key cyber policy and security areas. The government has passed new telecommunications legislation and is considering several other key pieces of legislation. E-commerce in Cambodia is gathering pace, but starting from a low base, and the government's slow approach to establishing a suitable policy and legal framework may be holding back further growth. Cambodia's positive developments are weakened by sustained lack of attention and resources for CERT activities, international engagement and financial cybercrime enforcement.

WEIGHTED SCORE **30.0**

1 GOVERNANCE

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

Cambodia's score for this category has increased this year to reflect work by the Cambodian Government on strengthening national telecommunications legislation. Cambodia's approach to cyber policy and strategy has been criticised as a 'paper trail' that hasn't been successfully implemented. The approval of the 2015 Telecommunications Law indicates that Cambodia is taking steps to address the shortfall in suitable legal frameworks for cyber issues. Cambodia's score for this category would improve further if other policy and legislative instruments were finalised, including the National ICT policy and e-commerce and cybercrime legislation.

SCORE: 4

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

In late 2015, Cambodia's legislature passed a new national Telecommunications Law, and it's considering several other pieces of legislation to regulate e-commerce and cybercrime. Previously, Cambodia relied on outdated legislation better suited to postal communications. The Telecommunications Law has been criticised for the wide-reaching surveillance powers it provides to government and a lack of transparency and accountability. Cambodia is receiving assistance from the US to develop new cybercrime legislation. Previous drafts of the legislation, shelved in 2014 but now apparently revived, have included heavy penalties for content that's critical of the government. The US's involvement should ensure that freedom of expression isn't harmed by the new legislation.

SCORE: 4

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

Cambodia's international cyber engagement is limited to engagement with ASEAN's cyber discussions and some bilateral engagement with Japan, South Korea and the US. This engagement is largely focused on technical capacity building and legislative and policy development assistance.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Cambodia's national CERT, CamCERT, issues regular monthly security alerts and maintains an online incident reporting portal. In the past year, it has also organised a cybersecurity challenge and conducted some limited international engagement, including a Japanese information-sharing study and a return to Asia–Pacific Telecommunity activity after a three-year hiatus. However, it isn't a member of APCERT. While it's difficult to assess CamCERT's capacity and capability, its regular activity and some international engagements in the past are promising signs that it's focused on becoming a more active and capable organisation.

SCORE: 3

2 CYBERCRIME

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

Cambodia's score for this category has increased, as there's clear evidence of cooperation between the police and the Ministry of Posts and Telecommunications to address cybercrime, including the arrests of two South Korean cybercrime groups in Phnom Penh. The passage of new cybercrime legislation and the establishment of a police cybercrime unit would increase Cambodia's score for this category.

SCORE: 2

3 MILITARY

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

Cambodia's military doesn't exhibit any obvious awareness or concern about cyber threats. The country's low reliance on networked military capability and computer networks for other critical infrastructure means that its vulnerability to cyber threats is also low.

SCORE: 1

4 BUSINESS

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

The elimination of political appointees to the ICT Federation's board is a positive step for public–private dialogue on digital business in Cambodia. The change in the federation's board means that industry leaders will now lead the organisation. Beyond the ICT Federation and some engagement between the government and international companies to secure an additional submarine cable, there's limited evidence of strong two-way engagement between government and the private sector on cyber issues.

SCORE: 3

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

Cambodia's significantly increased score for this category reflects the surge in e-commerce outlets in the country. Local media have stated that Cambodia's digital economy is worth an estimated US$800 million. Online services include online shopping sites that also provide lending services, and business-to-customer (B2C) sites that link consumers to brick-and-mortar shops. B2C websites have proliferated in the past two years and now number about 20. One site has claimed in the media that it records average monthly sales growth of 10%, despite the increasingly crowded marketplace. However, the market appears to be driven from the bottom up, and further support from government is needed to enable further sustainable growth, particularly by providing a stronger legislative framework.

SCORE: 3

5 SOCIAL

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

Discussion and awareness of cyber issues in local media remain relatively constant and are focused on discussion of new legislation and its potential effect on freedom of expression and privacy. The Cambodian Government has embraced social media as a means to interact more closely with its citizens, and Prime Minister Hun Sen's Facebook page has become a key communication channel for the government. Opposition leaders such as Sam Rainsy also have a large social media presence.

SCORE: 4

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 5

Poor infrastructure and high costs remain impediments to greater fixed broadband penetration in Cambodia, and only 0.5/100 Cambodians have a fixed broadband connection. The Ministry of Posts and Telecommunications estimates that 6.3 million Cambodians used mobile devices to access the internet in December 2015. There's relatively vigorous competition among the 8–10 mobile operators in Cambodia, and mobile devices are likely to remain the preferred method for Cambodians to access the internet. The ITU estimates that 42.8/100 Cambodians have an active mobile broadband connection.

CHINA

Rank 2016: 8th

2015: 8th

—

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	9
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	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 e.g. a Computer Emergency Response Team (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, policy, and security?	8
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	6
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has fixed broadband internet connectivity?	2
c) What percentage of the population has mobile broadband internet connectivity?	6

OVERALL ASSESSMENT

China has further consolidated its centralised government control of cyberspace, in both its governance approach and its military structure. There have also been significant efforts to address national security concerns about cyberspace in a reform of China's cybersecurity legislation, which continues to be strongly enforced in combating cybercrime. The new and proposed laws make it increasingly challenging for foreign investors to operate in China and are expected to have a detrimental impact on China's otherwise thriving digital economy. Chinese citizens' social engagement with cyber issues continues to be hampered by strong government content control and associated self-censorship.

WEIGHTED SCORE 63.0

1 GOVERNANCE

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

China continues to develop strong cyber governance efforts. The Central Leading Group for Cyberspace Affairs, constituted by high-ranking officials and headed by the President, is the national decision-making body for cyber governance. The group directs the activities of the Cyberspace Administration of China, which is the national coordinating body for cyberspace regulation. The establishment of a new multistakeholder cyber governance organisation—the Cyber Security Association of China—and the announcement of a dedicated 300 million yuan fund suggest that cybersecurity continues to be a priority for the Chinese leadership. This is echoed in China's recent release of a new five-year plan outlining investment to support innovation in cybersecurity, quantum communication and big data applications. Continued efforts to advance the cyber legislative framework reflect China's commitment to the doctrine of cyber sovereignty and content control.

SCORE: 9

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

China has a robust collection of cybersecurity legislation and a strong focus on data localisation, technology regulation and content control in pursuit of a secure and controllable cyberspace. The new *Counter-Terrorism Law*, passed in January, has drawn international criticism for requiring telecommunications operators to take an active role in monitoring online content and to provide decryption assistance to Chinese law enforcement. The long-awaited *Cyber Security Law* is still tied up in review after the second of its three readings in July 2016. The draft legislation stipulates that companies must cooperate with state surveillance authorities and keep servers inside China. This law faces similar international scepticism, and its slow progress contributes to China's stagnant score for this indicator. China has bolstered its regulatory framework with the addition of new rules for online advertising, publishing news content, mobile applications and domain names. The recent changes reflect China's increasingly centralised legislative control over cyberspace. In order to increase its score, China must broaden its legislative scope to address cyber issues that aren't related to national security, such as consumer protection and privacy.

SCORE: 7

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

China actively participates in international cyber discussions, promoting the concept of cyber sovereignty in opposition to the US school of multistakeholder internet governance. It held its second annual World Internet Conference in Wuzhen in December 2015 and took the opportunity to assert the central role of states in cybersecurity issues. It attempts to propagate those views through international institutions such as the ITU and ASEAN. China has successfully established new bilateral cybersecurity agreements with the US, UK, India and Russia covering issues including intellectual property theft, cybercrime and norms. These relationships show a strong focus on high-level political engagement. China's score could be raised if it were to demonstrate more effective multilevel cooperation and Asia–Pacific capacity building.

SCORE: 9

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

CNCERT continues to address cyber incidents, hold international conferences and participate in APCERT and ASEAN incident drills. Increasing its bilateral CERT–CERT engagement and taking a stronger leadership role in Asia–Pacific CERT activity would increase China's score for this indicator, which remains consistent for the third year in a row.

SCORE: 6

2 CYBERCRIME

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

China's enforcement of cybersecurity legislation appears to have strengthened this year. There's been an expansion of law enforcement efforts, including the embedding of cybersecurity police units within large internet companies and large-scale arrests of 15,000 people in August last year as part of a 'cleaning the internet' policy. These moves reflect China's ongoing focus on censorship instead of financial cybercrime. China's score has risen to reflect a notable improvement in its engagement with foreign law enforcement agencies. In September 2015, acting on a US request, China arrested hackers for the theft of intellectual property, and in February 2016, in cooperation with the FBI, apprehended 17 people for online child exploitation. China is also helping to develop Asia–Pacific capacity to combat cybercrime through its establishment of the China–ASEAN Law Enforcement Academy in March 2016. Through this facility, China has committed to training more than 2,000 officers over the next four years. Questions continue to arise about government-sanctioned cybercrime emanating from China; despite the September agreement with the US, incident rates and suspicions remain high.

SCORE: 6

3 MILITARY

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

The People's Liberation Army (PLA) has initiated significant restructuring with the establishment of the Strategic Support Force, a new centralised command responsible for high-tech warfare that reports directly to the Central Military Commission. This move elevates the position of cyber units within the PLA to that of the independent services and facilitates more sophisticated military coordination in cyberspace. The change builds upon the articulation of the PLA's cyber posture in *China's military strategy* in 2015, putting China in a good position to see its score increase upon the successful implementation of these organisational changes.

SCORE: 8

4 BUSINESS

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

The Cyber Security Association of China was established in May 2016 to engage the private sector, academia and government in the development of China's cyber policy. This industry association, which is led by the Chinese Communist Party and features Chinese tech giants Alibaba, Baidu and Tencent, is a positive development in China's cyber maturity. However, it remains to be seen whether the new organisation will result in real multistakeholder dialogue and influence or simply be an additional arm of top-down government control. China demonstrates minor receptiveness to international concerns over its cyber legislation, most recently by removing unpopular requirements for backdoors in the new *Counter-Terrorism Law*. The score for this indicator could be increased if China were to consult proactively with stakeholders before putting forward new legislation or policy, such as the pending *Cyber Security Law*. In general, dialogue remains one-directional in China, with a focus on compliance.

SCORE: 5

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

The digital economy plays a significant role in China and has been championed from the top with the implementation of the government's 2014 'Internet Plus' strategy. China is now the world's biggest e-commerce market, experiencing growth in online retail sales, fintech developments and thriving social networks. However, its legislative and regulatory system is posing increasing obstacles to the operation of foreign companies, such as mandated data localisation and decryption assistance. Local companies have a strong home-ground advantage, and this dynamic is expected to choke foreign investment in China's digital economy, as evidenced by the recent ousting of Uber in favour of domestic ride-share company, Didi.

SCORE: 6

5 SOCIAL

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

China now has the largest online population, which is highly engaged in social networks such as WeChat and RenRen. The recent legislative changes sparked some public debate over the social and economic implications, while the rise of microblogs has facilitated greater digital activism. Unfortunately, strong government censorship efforts, including 'cleaning the internet' crackdowns and tougher restrictions on news content providers, limit the discussion of cyber issues in China. Self-censorship also continues to inhibit open public discussion.

SCORE: 5

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 2

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 6

For the first time, more than half of China's population is online. Its more than 688 million internet users make up the world's largest online population. Smartphones are the device of choice and are used by two-thirds of its netizens to connect. There continues to be a significant rural–urban digital divide, as more than 70% of internet users are based in cities. In October 2015, the government announced plans to combat this deficiency through an investment of 140 billion yuan in rural internet infrastructure.

FIJI

Rank 2016: 19th
2015: 15th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	2
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	3
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	3
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	5

OVERALL ASSESSMENT

Fiji lacks specific governance structures, strategy and legislation to address cyber matters; however these are reportedly now under development through the Cyber Security Working Group. Fiji's police cyber crime unit has a minimal response capacity and its regional engagement is limited despite membership in multilateral initiatives. The paucity of supporting policy and infrastructure continues to hamper the development of Fiji's digital economy and social debate on cyber issues.

WEIGHTED SCORE 25.3

1 GOVERNANCE

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

The Fijian government announced in September 2015 that it will be working with the Commonwealth Telecommunications Organisation (CTO) to develop a national cyber security strategy. The document is yet to materialise, but is intended to act as a model for other Pacific island countries when completed. The Cybersecurity Working Group, a public-private partnership body established in 2011, is reportedly contributing to its development, alongside a cyber security policy and cyber legislation. Currently, Fiji has an underdeveloped organisational structure for cyber matters, with most of its capacity concentrated within police efforts. Hopefully the publication of the cyber strategy and policy documents will help Fiji improve in this area.

SCORE: 2

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

The Fijian government is reportedly in the process of drafting a Cyber Crime Bill and Cyber Security Bill, to address malicious online behaviour including pornography and online child exploitation. Fiji does not currently have legislation specifically addressing cyber security, but these laws will build upon existing relevant legislation such as the 1999 Telecommunications Act, 2004 Financial Transactions Reporting Act and 2009 Crimes Decree, which covers computer offences, and the *Telecommunications Licensing Regulation Act* of 2012. Successfully passing this foreshadowed cyber legislation will raise Fiji's score in this area.

SCORE: 4

c) How does the country engage in international discussions on cyberspace, including in bilateral, multi-lateral and other fora?

Fiji engages in bilateral and multilateral cybersecurity initiatives on a relatively narrow range of issues. It is a member of the Pacific Islands Telecommunications Association and ITU IMPACT. This year, Fiji became the Second Vice Chair of the Commonwealth Telecommunications Organisation (CTO) and will host the CTO Forum and Council meeting in September 2016. It has also hosted technical workshops for Asia-Pacific neighbours. Greater participation in Asia-Pacific forums would increase Fiji's score for this category.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (CERT)?

Fiji no longer has a national CERT capacity. PacCERT was previously based at the University of the South Pacific in Suva ceased operations in 2014.

SCORE: 0

2 CYBERCRIME

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

Combatting cybercrime has received public attention in Fiji this year, with the Attorney General and Minister for Communications promoting its role in securing a prosperous economy in June. The occurrence of ATM and credit card scams are on the rise in Fiji, along with social media fraud schemes. The manipulation of electronic payment methods has resulted in the diversion of private sector money transfers away from the intended recipient, costing two Fijian companies US$13,000 and US$14,000 in 2015. The Fijian Police Force's Cyber Crime Unit enforces the 2009 Crimes Decree, and 2004 Financial Transactions Reporting Act, and works with the Financial Intelligence Unit to address financial cybercrime. The unit handles cybercrime reported by the community, but there appears to be limited capacity to investigate and prosecute incidents. Fiji Police has had some engagement on cybercrime with Australian Federal Police, the Indonesian National Police and the Chinese Ministry of Public Security. Further evidence of strengthened capability to police cybercrime, and deeper international collaboration to address cybercrime would improve Fiji's score.

SCORE: 4

3 MILITARY

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

Other than the military's role in forming a cybersecurity working group in 2011, there is no evidence to indicate that the Fijian military has significant awareness of cyber threats, or the capability to defend itself from them. Defence collaborates with the Police Force's Cyber Crime Unit but does not appear to be working toward the development of a cyber strategy or military cyber capabilities.

SCORE: 1

4 BUSINESS

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

The Government of Fiji has indicated that it sees the value in private sector consultation in regards to the digital economy. In 2011 the country established a Cybersecurity Working Group, based on a public private partnership model, with representatives from the Ministry of Defence, Cybercrimes Unit, Financial Intelligence Crimes Unit, licensed operators, network service providers and banks. The group continues to operate, currently developing the national cyber security strategy, policy and legislation. Broader dialogue beyond this initiative is limited, and the facilitation of more frequent, widespread public-private collaboration is required to improve Fiji's score.

SCORE: 2

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

There is little indication that Fiji has engaged with the digital economy. While infrastructure has been a significant issue, the continuing rollout of wireless internet and 3G/EDGE mobile connectivity has not seen a corresponding take up of ecommerce or other digital services beyond an increase in mobile banking. Fiji requires a clear strategy from the government and closer dialogue with the private sector to fulfil the significant potential of Fiji's digital economy, and the country's future development.

SCORE: 3

5 SOCIAL

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

Public awareness, debate and media coverage of cyber matters is limited by government censorship and a lack of infrastructure. The minimal discussion that does take place tends to focus on incidents of cyber crime. Greater access to information would help raise the profile of cyber issues in Fiji.

SCORE: 3

b) What percentage of the population has fixed line broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 5

Fixed broadband connectivity is limited by cost and access, but take up of mobile broadband means that now nearly half of Fijians have internet access through a mobile device. This has provided more Fijians with access to banking services that were previously unavailable, and online bill and salary payments are becoming more common.

INDIA

Rank 2016: 10th

2015: 11th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	7
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	5
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	7
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	3
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	7
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	7
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	2

OVERALL ASSESSMENT

India's approach to cyber issues and the digital economy has taken some promising steps in 2016. The Prime Minister has focused on obtaining the maximum possible benefit from digital connectivity for government service delivery and the economy. However, India continues to struggle with other issues that prevent it making significant gains in this area, including bureaucratic delays in the implementation of policy, low connectivity outside urban areas and high levels of illiteracy. Regardless, India's enormous population means that it has a significant effect on the world's digital ecosystem. It also has the world's second-largest national group of app users.

WEIGHTED SCORE 48.4

1 GOVERNANCE

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

India is notable for its extensive, complex and probably redundant cyber policy and security governance architecture. Implementation of the 2013 National Cyber Security Policy is still not complete, and the legislative framework underpinning cybersecurity is underdeveloped. A centralised agency to manage cyber policy and security issues was referred to in the 2013 policy, but no action on this is apparent. Policies such as Digital India and Startup India are positive developments and reflect a good awareness in some areas of government of the benefits of greater digital connectivity and the obstacles that must be overcome, including low levels of internet penetration and poor literacy. Clearer, streamlined policy and legal frameworks that are strongly implemented are required for India to improve its score for this category.

SCORE: 7

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

India's score for this category remains steady, reflecting continued inaction to improve outdated legislation and simplify the legal and regulatory framework for cybersecurity, cybercrime, e-commerce and privacy. Requirements for local product and equipment certifications and mandated use of particular technology are impeding the development of India's digital economy and raising costs for consumers. There's been some action to address this, including lifting some local content requirements that have allowed Apple to open its first store in the country. However, further action to improve the legal framework for cyber issues is necessary to build a stable basis for secure digital growth.

SCORE: 5

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

India remains engaged in bilateral and multilateral cyber discussions. In the past year, this has included new bilateral meetings or agreements with Australia, Kenya, the US, the UK, Germany, the European Union, France, South Korea, Russia and Japan. India is also pursuing membership in the Shanghai Cooperation Organisation, which has a strong cyber policy and norms agenda. It has made several conflicting statements about its approach to key internet governance issues, particularly the debate about multistakeholder versus multilateral approaches. The statement issued after a trilateral Russia–China–India foreign ministers meeting in May 2016 supported multilateralism. However, in June 2016, Prime Minister Modi signed a new Framework for US–India Cyber Relationship agreement that notes that both countries are committed to a multistakeholder model of internet governance. Greater consistency in India's approach to key issues is necessary for India's score for this category to improve.

SCORE: 7

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

India's national CERT, CERT-IN, appears to have increased its domestic threat response and information raising activities and engaged more broadly with international partners, raising India's score for this category. CERT-IN reported in the APERT annual report that it responded to 49,455 security incidents in 2015, most of which were website defacements. CERT-IN has also assisted with the establishment of a CERT in Mauritius and signed MoUs with CERTs in Australia, Malaysia, Singapore and Japan.

SCORE: 5

2 CYBERCRIME

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

Cybercrime remains a significant problem in India, where registered cybercrimes have increased by 40% since 2014. The Home Ministry has committed to the establishment of a new cybercrime centre, the Indian Cyber Crime Coordination Centre (IC4). However, while the IC4 will address all types of cybercrime, a spokesperson for the Home Ministry has noted that its priority will be dealing with child pornography and online trolling, rather than financial cybercrime. The ministry has also committed to training for a further 90,000 police personnel and 15,000 judicial staff in cybercrime in order to strengthen enforcement. Evidence that these initiatives have been implemented may lead to an increase in India's score in future years.

SCORE: 4

3 MILITARY

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

India's score for this category has been reduced due to sustained inaction by its armed forces to address cyber threats. Cyber incident response teams have been established in the Navy and Army, as well as the Department of Defence Production. The strength of Defence Information Assurance and Research Agency oversight of triservice and Defence Ministry cyber efforts is not clear. The Army has also reportedly established two units within its Intelligence Corps to counter foreign cyber espionage attempts targeting Army networks and personnel. However, the armed forces have taken little action to engage in a cooperative approach to cybersecurity and operations capability development, and the long delay in authorisation of a tri-service cyber command indicates that this won't occur anytime soon.

SCORE: 3

4 BUSINESS

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

Startup India is a flagship policy of Prime Minister Modi. It aims to enhance the take-up of digital economic opportunities by Indians through a range of measures for digital start-ups, including tax exemptions, reduced compliance measures, a lower bar for government tenders and alterations to insolvency regulations. New research parks and technology incubators are also planned to enhance digital economic opportunities. Government and industry have also come together to cooperate on internet governance discussion in ICANN, and co-investment in new research and innovation centres is being encouraged by the Department of Electronics and IT. India's actions to enable digital business are positive, but improved two-way dialogue is needed to improve its 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?)

India's digital economy has continued to grow strongly, supported by strong engagement by foreign firms in India, an active homegrown start-up industry and sustained growth in the IT services sector. IT services make up 25% of India's exports and employ about 12.5 million people. India is emerging as the second-largest user of apps, and by 2017–18 is expected to have the largest number of app developers in the world, prompting Google to fund training for a further 2 million Android developers in India out to 2019. However, while the sheer numbers for this industry are impressive, they make up only a small part of India's overall national workforce of nearly half a billion people. Poor connectivity outside major urban conglomerations and high levels of illiteracy prevent India benefiting to an even greater extent from the digital economy.

SCORE: 7

5 SOCIAL

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

There's significant media, academic and social coverage of cyber-related policy and security issues in India, and an active approach by major policy and security think tanks. In 2016, this has addressed such issues as net neutrality and the proposed introduction and subsequent blocking of Facebook's 'Free Basics' program, and the government's response to cyber threats. There's also been media coverage of broader issues, including multistakeholder internet governance and developments in the digital economy and technology sectors. Social media are increasingly used by politicians, commentators and the public to discuss policy and social issues, although these exchanges often become heated.

SCORE: 7

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 2

India's Communication Minister, Ravi Shakar Prasad, has stated in the media that he's hopeful that India will have 500 million internet users by the end of 2016. While internet connectivity in India is affordable, the World Economic Forum's *Global information technology report* notes that infrastructure and a lack of skills among the population are key obstacles to greater internet penetration, coupled with a high level of illiteracy (currently about one-third of the population). Unlike in other countries, mobile connectivity hasn't overcome some of the infrastructure barriers present in India. Smartphones remain in the hands of only a few, which is reflected in mobile broadband connectivity of only 9.36/100 people. Regardless, that's still an enormous number of people, and is reflected in the high rates of app usage in India in the global context.

INDONESIA

Rank 2016: 12th
2015: 14th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	5
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	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 e.g. a Computer Emergency Response Team (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, policy, and security?	6
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	5
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	5

OVERALL ASSESSMENT

Indonesia has wrestled with cyber governance and legislation reforms this year, but has neither delivered the anticipated National Cyber Agency nor updated its central cybersecurity law. It continues to cooperate in Asia–Pacific multilateral forums and cybercrime efforts, and the new Defence White Paper has made Indonesia's military posture in cyberspace clearer. Strong government efforts to fulfil Indonesia's digital economic potential are expected to bear fruit in the coming years, but relaxing state control of online content will be necessary to further increase Indonesia's maturity.

WEIGHTED SCORE 47.4

1 GOVERNANCE

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

There have been no tangible changes to Indonesia's cyber governance structure, despite rhetoric about the establishment of a National Cyber Agency over the past year. It appears that the development may have been cancelled due to a lack of funding, but expectations remain that the agency will still be established, possibly by presidential decree. In the meantime, the National Cyber Information Defense and Security Desk at the Coordinating Ministry for Political, Legal and Security Affairs continues to play a central role in the organisation of cyber policy. Indonesia's score for this indicator has been reduced because of its inability to implement the proposed structural reform and establish a more centralised approach to cybersecurity. There are still no accessible strategies or policies that articulate Indonesia's governance approach to cyberspace.

SCORE: 5

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

Indonesia continues to rely on the *Electronic Information and Transactions Act 2008* (the ITE Law) as its central cybersecurity legislation. The law underwent a review, resulting in a draft revision that reduced the prison sentence for online defamation from six to three years. However, this reform has been abandoned and the controversial article remains unchanged. The *Computer Crimes Act* promised last year is nowhere to be seen, but a draft Personal Data Protection Bill is being discussed. If passed, this law will govern the collection and handling of personal data and will be the first to address the privacy of Indonesians. Delivery of the discussed reforms and new legislation will help raise Indonesia's score for this indicator.

SCORE: 5

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

Indonesia has maintained its bilateral engagements with Australia, Japan, the US and China. It continues to cooperate in the Asia–Pacific through APCERT, ITU-IMPACT and ASEAN, and initiated and hosted the first ASEAN Cyber Security Competition in November 2015. Indonesia's international efforts remain mostly technical and policing focused, and expanding its engagement in both scale and scope would raise its score in this area.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

The Indonesia Security Incident Response Team of the Internet Infrastructure Coordination Centre (ID-SIRTII/CC), within the Ministry of ICT, is Indonesia's national CERT. Domestically, it runs a substantial training and education program for public- and private-sector participants on topics such as secure programming, digital forensics and DNS security. Internationally, ID-SERTII/CC is a member of APCERT, FIRST and OIC-CERT and participates in Asia–Pacific drills. There appears to have been little change in its operations, so Indonesia's score remains consistent.

SCORE: 6

2 CYBERCRIME

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

The Indonesian National Police (INP) has an active cybercrime unit in the Sub-Directorate of Information Technology and Cybercrime. The police prosecute criminals under Articles 27–37 of the central ITE Law pertaining to pornography, gambling, defamation and hacking. There's evidence of strong implementation and frequent arrests, most often for cases of cyber fraud. The INP cooperates with international partners through its partnership with the Australian Federal Police, engagement with INTERPOL and recent hosting of the ASEANPOL Police Training Cooperation Conference in October 2015. However, Indonesia remains the largest source of malicious cyber activity in the world, indicating that greater law enforcement efforts are required.

SCORE: 4

3 MILITARY

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

Indonesia established a Cyber Defence Operations Centre in 2013, and Japan's NEC Corporation recently agreed to set up a new Security Operations Centre to train Indonesia's officials and combat national cyber threats. The release of Indonesia's Defence White Paper in November 2015 has shed light on its military approach in cyberspace. The White Paper depicts cyberspace as an asymmetric weapon for non-linear warfare and as an integrated support for military operations. The document is a timely addition, providing a narrative for Indonesia's organisational structure and raising its score in this area. Indonesia has also expanded its international military cooperation in cyberspace by planning joint cyberwar simulation exercises with China.

SCORE: 6

4 BUSINESS

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

The Indonesian Government has identified the importance of private-sector innovation for economic growth and has released a new policy to support it. The e-Commerce Roadmap sets out regulations for the digital economy, proposes tax breaks for tech start-ups, and plans infrastructure improvements and boosts to human resources. Indonesia has removed e-commerce from its negative investment list and established the National Payment Gateway in order to help achieve President Widodo's vision of a US$130 billion digital economy by 2020. A new regulation requiring foreign over-the-top internet companies to pay local taxes is intended to improve the odds for Indonesian competitors. However, this change took place without stakeholder consultation and created private-sector frustration and confusion, indicating that the discussion remains predominantly one-directional. There are efforts towards interaction, such as the Indonesia Cyber Security Summit and Asia Internet Symposium, but the delivery of the promised National Cyber Agency will help generate truly collaborative public–private partnerships.

SCORE: 5

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

The internet economy currently accounts for only 1% of Indonesia's GDP, but Indonesia is expected to become the biggest e-commerce market in Southeast Asia by 2018. The telecommunications market is liberalised and includes eight mobile companies and 35 infrastructure-owning ISPs, and 4G connectivity is now available nationwide. There's strong bottom-up development, exemplified by the growth in local start-ups, mobile tech take-up and online shopping. Capitalising on the untapped elements of Indonesia's large, youthful population will boost digital development. However, achieving this potential will require several obstacles to be overcome. Indonesia's historically weak and chaotic regulation of the digital economy has left underdeveloped telecommunications infrastructure, skills shortages and insufficient online payment capabilities. Strong implementation of the e-Commerce Roadmap will help address these issues and further strengthen Indonesia's digital maturity.

SCORE: 5

5 SOCIAL

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

There's been a slight increase in public debate about cyber issues among Indonesians. Indonesia has increased its efforts to engage youth in cybersecurity through events such as the Indonesia Cyber Army, Cyber Jawara and Cyberkids Camp. Significantly, the failed reform of the ITE Law sparked high-profile discussions about freedom of expression online and concerns about government censorship. The occurrence of this debate is a positive step, but the root issues persist and Indonesia's internet freedom remains limited.

SCORE: 5

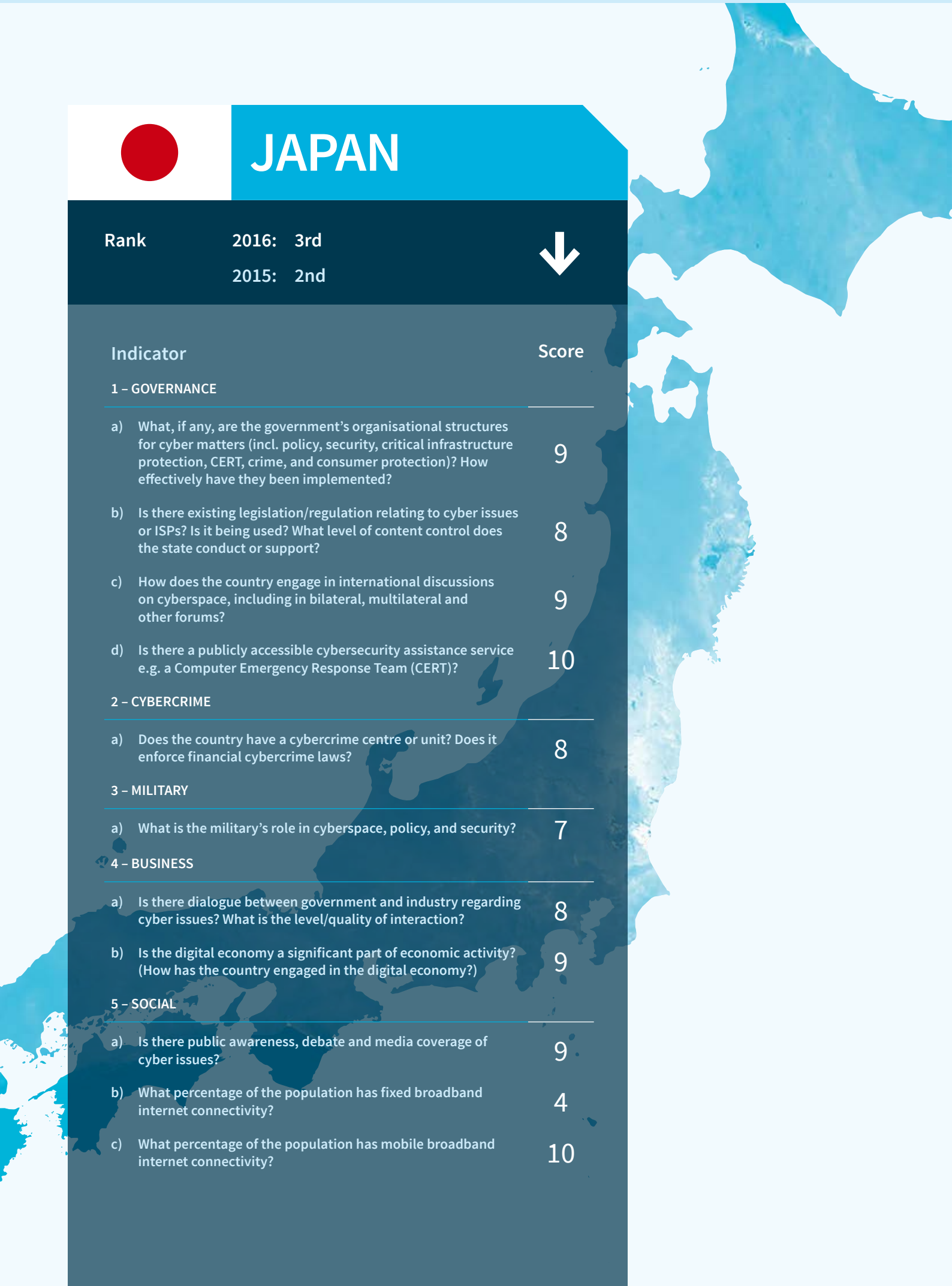
b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 5

Indonesia's archipelagic geography remains an obstacle to fixed-line internet penetration, which currently reaches only 1% of the population. However, the take-up of smartphones is bringing the internet to more Indonesians. Mobile connectivity now sits at 42% of the population.



JAPAN

Rank 2016: 3rd
2015: 2nd

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	9
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	7
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	9
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has fixed broadband internet connectivity?	4
c) What percentage of the population has mobile broadband internet connectivity?	10

OVERALL ASSESSMENT

In 2015–16, Japan launched its new Cybersecurity Strategy and amended the *Cybersecurity Basic Act*, and a continuing increase in public awareness about cyber issues. It bolstered its already impressive international engagement efforts with the creation of the 'cyber office for national security policy' in the Ministry of Foreign Affairs. JPCERT/CC maintained its position as an Asia–Pacific leader in CERT/CSIRT best practice with an impressive domestic and international engagement program, new alert and notification initiatives, an expanding geographical capacity-building remit and the 'Cyber Green' initiative. Whole-of-government efforts will continue to build in the lead-up to the Tokyo Olympic and Paralympic Games in 2020.

WEIGHTED SCORE: **82.9**

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?

In Japan, the Cybersecurity Strategic Headquarters functions as the control point for government coordination and the implementation of Japan's new national cyber strategy, primarily through its secretariat, the National Information Security Center (NISC). Approved by cabinet in September 2015, the Japanese Cybersecurity Strategy takes a more holistic approach to cyber matters than previous strategies by coherently addressing threats and benefits and outlining Japan's basic principles for cyberspace and policy approaches to attain them. It highlights the role of industry and civil society in maintaining Japan's cybersecurity and the centrality of two-way information sharing as a practical manifestation of this. Following the high-profile Japan Pension Service hack, the new strategy also includes plans to allow NISC to monitor government-affiliated agencies for the first time; this will be crucial in maintaining the public's trust in e-government initiatives such as the My Number social security program.

SCORE: 9

b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?

The Japanese Government adopted the *Cybersecurity Basic Act* in November 2014. The Act outlined the roles and responsibilities of government in protecting Japan online, including uniform standards for government and measures at local and national levels. It also solidified the legal standing of NISC, granting it the legal authority and power to implement standards and policies on other government ministries and agencies and formulating a whole-of-nation approach to cyberspace. The *Cybersecurity Basic Act* was amended in April 2016 in response to the Japan Pension Service hack to give NISC new power to monitor and audit the security of entities created by direct government approval or laws. In the light of NISC's expanded role, the new law also allows it to delegate some of its audit responsibilities to the Information-technology Promotion Agency.

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 program of multidimensional cyber engagement that stretches across policy, technical and legislative realms. This agenda is backed up by the Cyber Security Strategy and the stand-alone International Strategy on Cybersecurity. This work is supported by an ambassador in charge of cyber policy and a newly established 'cyber office for national security policy' in the Ministry of Foreign Affairs. Japan is a member of the Global Forum on Cyber Expertise and has been a member of two UNGGEs. It often discusses whole-of-government cyber issues at high-level international political dialogues, both multilateral and bilateral, and at cyber-specific dialogues with subject matter experts. The Japanese Government has a strong Asia–Pacific engagement program, working closely with ASEAN countries to lift internal and Asia–Pacific cybersecurity capacity.

SCORE: 9

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Established in 1996, JPCERT/CC is Japan's national CERT and the coordinating centre for all other CSIRTs in Japan. It works with government agencies, critical infrastructure operators, security vendors and broader civil society. Since its inception, JPCERT/CC has been a steering committee member of APCERT and played host to its secretariat, also acting as chair of the body from 2011 to 2015. It's also a member of FIRST's board of directors and offers sponsorship for other CSIRTs that wish to join. JPCERT/CC also created the TSUBAME packet traffic monitoring system, which now promotes collaboration across the Asia–Pacific and enhances the sharing of threat information. In addition, JPCERT/CC offers an impressive range of weekly and monthly security alerts, advisories and updates in Japanese and English. It undertakes extensive capacity building across and outside the Asia–Pacific, lending expertise and technical training to other CERTS/CSIRTS, and engages with higher level policy and confidence-building efforts. JPCERT/CC is also working with global partners on a 'Cyber Green Initiative' to help create a 'healthy' cyberspace based upon internationally gathered and shared metrics and statistics.

SCORE: 10

2 CYBERCRIME

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

The 9th (Cybercrime) Division of the Criminal Investigation Bureau and the Hi-Tech Crime Technology Division of Japan's National Police Agency are responsible for investigating and prosecuting cybercrimes. The Cybercrime Division houses cyber experts who speak English, Chinese, Korean and Russian, who are also utilised in the defence of government organisations, defence contractors and critical national infrastructure operators. The National Police Agency is also active internationally, engaging in bilateral dialogues and exchanges with other Asia–Pacific police forces on high-tech crime issues.

SCORE: 8

3 MILITARY

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

The Japanese Ministry of Defense Cyber Defence Unit, which currently numbers around 90 individuals, is tasked with the protection of military installations, the ministry and critical infrastructure. The ministry and the Japan Self-Defense Forces have leaned strongly on traditional partners to help expand and upskill the forces, in particular by working quite closely with the US through the US–Japan Cyber Defense Policy Working Group, joint military exercises and other ad hoc and high-level discussions. To improve its score, Japan would benefit from a more defined doctrine or strategy outlining how cyberspace is used in warfare and a more developed approach to protecting its defence industry.

SCORE: 7

4 BUSINESS

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

Japan's Cybersecurity Strategy has made strong moves to pull down the cultural 'veil of silence' surrounding cybersecurity issues that can often exist in the private sector. The new strategy includes provisions for the direct hiring of private-sector experts into NISC (of NISC's 40 new staff, 18 are to be recruited from the private sector). The Japanese Business Federation has also established a cybersecurity working group of more than 30 of Japan's most important companies. The group has already sent the government a set of recommendations on improving Japan's cybersecurity, including on improving critical national infrastructure protection, information sharing, skills training, R&D and increased international cooperation. The calls seem to have resonated with the government: at a conference in 2016, Chief Cabinet Secretary Yoshihide Suga highlighted many of the recommendations as key focus areas for the government over the next 12 months.

SCORE: 8

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

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

SCORE: 9

5 SOCIAL

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

Public, business and government focus on cyber issues remains very high following the Japan Pension Service hack and subsequent alterations to Japan's *Cybersecurity Basic Act*, cyber concerns in the lead-up to the Tokyo Olympic Games and the rollout of the My Number social security program. Japan has a well-developed culture of academic research into cyber issues, and many universities also partner with government and the private sector to develop skills programs to help fill the country's growing skills gap. Media reporting on new government policies (local to national), organisational changes, cyber threats and infiltrations remains plentiful.

SCORE: 9

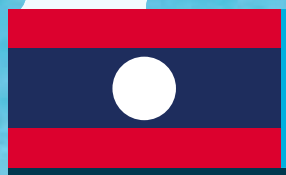
b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 4

c) What percentage of the population has fixed broadband internet connectivity?

SCORE: 10

The number of mobile data connections in Japan is equal to 126% of the population, while 30% have a fixed broadband connection.



LAOS

Rank 2016: 20th
2015: 17th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	4
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	3
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	2
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	2
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	2

OVERALL ASSESSMENT

The National Assembly of Laos recently passed new cybercrime legislation, and the government has ambitious plans to introduce a raft of new policy and legislative proposals for further ICT development and cybersecurity. LaoCERT leads the way in driving the country's international cyber engagement, but efforts to counter cybercrime, build military cyber capability and foster broader international engagement remain quite underdeveloped. In response to the creation of the ASEAN Economic Community, there are burgeoning grassroots efforts to create new online marketplaces to sell local Lao goods.

WEIGHTED SCORE 21.3

1 GOVERNANCE

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

In Laos, the Ministry of Posts and Telecommunications has responsibility for ICT policy formation and regulation and increasing awareness about cyber strategies. The National Assembly recently passed a new cybercrime law and will soon be considering an additional Law on ICT. According to the ministry, Laos is also drafting an ambitious set of policies, including the National ICT Development Strategy for 2016–2025, the National ICT Master Plan for 2016–2020, and national policies covering broadband, ICT and information security.

SCORE: 4

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

Laos's new cybercrime law defines online crime based on definitions in the European Convention on Cybercrime. It includes provisions to enable international cooperation on cybercrime issues and outlines penalties and fines for people convicted of offences. It also discusses strategies and programs to help prevent online crime. Other legislation that law enforcement can draw upon includes the *Telecommunications Law* and the *Broadcasting Law*, which were reportedly drafted with the support of China.

SCORE: 3

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

Laos's international engagement is strongly oriented towards discussions with immediate neighbours, particularly China. In 2016, the Ministry of Posts and Telecommunications signed an MoU with the Cyberspace Administration of China. This augments previous collaboration conducted with other ASEAN countries in 2015 in the creation of the China–ASEAN ICT Work Plan. Laos is a member of ITU-IMPACT and APCERT, and in 2015 took part in dialogues with Japan and Korea on public key infrastructure issues.

SCORE: 2

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

LaoCERT was created in 2012 and is the national CERT point of contact within Laos and internationally. It works domestically to handle incidents affecting government, industry and the public while increasing end-user education on good cyber hygiene. LaoCERT is an active participant in international training sessions organised by other Asia–Pacific CERTs and APCERT and within ASEAN. It has signed several recent MoUs with neighbouring CERTS and has been a participant at larger cross-cutting information security and cybersecurity conferences around the world.

SCORE: 3

2 CYBERCRIME

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

There's no evidence to show that Laos maintains a dedicated cybercrime component in its police force or has the capacity to enforce financial cybercrime laws. In 2015, the Vietnamese Ministry of Public Security donated 50 computers to the Lao Ministry of Public Security and the Vietnam Investors Association in Laos donated an additional US$100,000 to help the ministry purchase IT equipment.

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 devoted limited thinking to cybersecurity threats. Older national documents stipulate that the military has been assigned responsibility to coordinate responses to information security incidents that threaten 'national stability', but there's no evidence that this has been acted upon organisationally.

SCORE: 1

4 BUSINESS

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

Laos appears to have an emerging level of dialogue with ISPs and telecommunications companies. The Lao National Internet Centre has reportedly consulted with those sectors when formulating its development plans. The Lao ICT Commerce Association and the Lao National Chamber of Commerce and Industry are working to boost public–private partnerships in areas of ICT.

SCORE: 2

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

In 2012, the National Assembly passed e-commerce legislation after receiving assistance to draft the laws from the UN Economic and Social Commission for Asia and the Pacific (UNESCAP), the UN Conference on Trade and Development and the US Agency for International Development. Lack of infrastructure continues to be a barrier to the expansion of Laos's digital economy. Several industrious companies and individuals have begun to set up 'e-commerce platforms', which are essentially online marketplaces selling local Lao products, leveraging new economic links resulting from the creation of the ASEAN Economic Community.

SCORE: 2

5 SOCIAL

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

The Ministry of Posts and Telecommunications is working to roll out internet access in schools throughout the country and works with partners to try to raise IT security awareness. The ministry provides training to government officials in cooperation with partners including UNESCAP / Asian and Pacific Training Centre for ICT for Development and the Asia–Pacific Network Information Centre, and via the ASEAN–Japan Information Security Awareness Program. The ministry also produces a tri-monthly Lao ICT magazine that focuses on IT security issues. The Lao Revolutionary Youth Union is working in schools and universities to 'raise awareness on social media best practice'. There's been some media coverage of the passage of Laos's cybercrime law, but most commentary has been restricted to foreign media. Due to Laos's low internet penetration levels, wide public discussion of cyber issues remains absent.

SCORE: 2

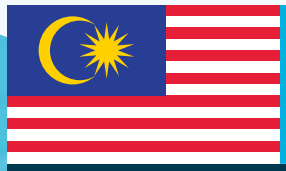
b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 2

Laos still struggles to provide basic internet infrastructure to a large part of its population. Mobile internet growth, the main driver of internet penetration in neighbouring Southeast Asian countries, has stagnated to some extent because of government over-regulation and anticompetitive practices, along with poor maintenance of existing telecommunications infrastructure by operators.



MALAYSIA

Rank 2016: 7th

2015: 7th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	7
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	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 e.g. a Computer Emergency Response Team (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, policy, and security?	6
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	7
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	8
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	10

OVERALL ASSESSMENT

Malaysia has continued to implement a comprehensive approach to cyber policy and security issues domestically and to engage on technical and policy issues with international partners. Cyber Security Malaysia operates a range of services to assist the Malaysian public and business communities with technical cybersecurity advice and incident response. A lack of overarching government cyber policy or strategy and a lack of evidence of increased international cooperation on financial cybercrime enforcement are key areas that need to be addressed to further increase the maturity of Malaysia's cyber policy and security framework.

WEIGHTED SCORE 67.7

1 GOVERNANCE

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

Malaysia's score for this category remains steady in 2016, reflecting steady progress by the Malaysian Government in the development and implementation of cyber policy. Cyber Security Malaysia, an agency of the Ministry of Science, Technology and Innovation, remains at the centre of the government's approach to cyber policy and security issues and oversees several other related functions, including cybersecurity awareness, incident response and education. In 2015, the government announced that Malaysia will review its suite of cyber policies but, other than the new Internet of Things Roadmap, the review hasn't been finalised. Malaysia would benefit from an overarching whole-of-government cyber strategy to comprehensively underpin its work on cyber issues.

SCORE: 7

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

Malaysia hasn't made any significant changes to its cyber-related legislation in 2016, and implementation appears to be steady. The country's cyber legislation is fairly comprehensive and includes the *Computer Crimes Act 1997,* the *Electronic Commerce Act 2006*, the *Communication and Multimedia Act 1998*, the *Financial Services Act 2013* and the *Personal Data Protection Act 2010*. Malaysia has been criticised for blocking online news services that have been critical of the government and for pursuing criminal investigations against online commentators. This has included an unsuccessful application for an INTERPOL red notice against a London-based blogger who first reported on the corruption scandal involving Prime Minister Razak and the Saudi royal family.

SCORE: 7

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

Malaysia has maintained a steady program of international cyber engagements in bilateral and multilateral forums. It has made new bilateral agreements with the European Union, Oman and India in the past year and had discussions with China on the sidelines of the ASEAN Regional Forum. It retained its active role in the forum and co-hosted a workshop with the European Union in March 2016. Malaysia's score for this category would improve if there were further evidence of Malaysian leadership in Asia–Pacific capacity building.

SCORE: 8

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

MyCERT, an agency of the Ministry of Science, Technology and Innovation, plays an active role in cybersecurity response and education in Malaysia. MyCERT maintains a range of cybersecurity advice and incident response services, including the Cyber 999 Help Centre, a vulnerability assessment service and the Malaysia Common Criteria Certification Body. It's also highly active in Asia–Pacific CERT/CSIRT forums such as APCERT and in broader international CERT organisations and plays a notable leadership role in OIC-CERT.

SCORE: 8

2 CYBERCRIME

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

The Cybercrime and Multimedia Investigation branch of the Royal Malaysian Police's Commercial Crime Division is responsible for investigating and prosecuting financial cybercrime in Malaysia. The police have also partnered with the University of Creative Technology to deliver the 'Be Smart' online crime prevention and awareness campaign, which has been running since 2013. Further evidence of an increased Malaysian role in leading Asia–Pacific responses to cybercrime and information sharing would be likely to increase Malaysia's score for this category.

SCORE: 6

3 MILITARY

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

Malaysia's score for this category has increased to reflect an improvement in the Malaysian Armed Forces' awareness of cyber threats and some evidence of action to mitigate them. The National Defence Policy notes that cyber capabilities, both defensive and offensive, are necessary to 'counterbalance' other Asia–Pacific countries. This is framed in the context of 'information dominance', in which superior acquisition, analysis and dissemination of information will improve the quality of commanders' decision-making during combat, enhancing Malaysia's combat power. Further evidence of the Malaysian Armed Forces acting on this guidance and enhancing their cyber operations capability is required for Malaysia's score for this category to increase further.

SCORE: 6

4 BUSINESS

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

Public–private dialogue on cyber issues remains relatively strong in Malaysia. There's a good level of engagement between Cyber Security Malaysia, universities and foreign and domestic cybersecurity firms. The government recognises the need to engage with the private sector and academic institutions but it appears to be focused on leveraging their research capacity to support technical cybersecurity measures. Further evidence of a two-way dialogue on broader policy issues is required for Malaysia to score higher in this category.

SCORE: 7

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

The Malaysian Government recognised the significant potential offered by the digital economy early on. The Department of Statistics has estimated that the digital economy produced 17% of GDP in 2015. The government established the Malaysian Digital Economy Corporation in 1996 and supports other organisations committed to enhancing digital business, including the Malaysian Innovation Agency and MSC Malaysia, which is a national initiative to attract international organisations and foster local industry. The World Economic Forum has noted that the Malaysian Government is fully committed to enabling digital business, and the private sector is increasingly agile in its adoption of new technology and organisational adaptations to meet new market conditions. Continued growth and sustained government attention to enabling digital growth would see Malaysia's score for this category continue to improve.

SCORE: 8

5 SOCIAL

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

Malaysians remain concerned about cyber threats, and several programs have been organised by Cyber Security Malaysia or the Royal Malaysian Police to raise awareness of cybersecurity issues. Malaysians are frequent users of social media sites and are increasingly adopting over-the-top messaging services. While there's some discussion in the media of cybersecurity incidents and cybercrime, there seems to be limited coverage of broader cyber policy and internet governance.

SCORE: 6

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 10

The *Global information technology report* notes that Malaysia's fixed broadband infrastructure suffers from low bandwidth by world standards, and affordability remains an issue. The ITU estimates that about 9/100 Malaysians have a fixed broadband subscription, and that about 90/100 have a mobile broadband subscription. Mobile take-up has accelerated in recent years, supporting Malaysians' increased engagement with social media and the digital economy.

MYANMAR

Rank 2016: 17th
2015: 16th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	5
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	1
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	2
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	4

OVERALL ASSESSMENT

Myanmar shows some awareness of cybersecurity issues but is limited by a policy and governance focus on controlling content. Its international engagement on cyber issues is also narrowly focused on the receipt of capacity-building training from other Asia–Pacific countries in technical aspects of cybersecurity and ICT infrastructure development. While Myanmar's military retains a strong cyber surveillance capability, the ability of law enforcement authorities to respond to cybercrime is limited. Low levels of internet penetration limit the reach of the digital economy and social engagement on cyber related issues. A focus on engaging more of the population in cyberspace within a strong policy and legislative framework is required for Myanmar to improve its cyber maturity.

WEIGHTED SCORE 28.1

1 GOVERNANCE

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

Myanmar's organisational structure for cyber matters is centred on the Ministry of Communications and Technology, which houses the Post and Telecommunications Department and Myanmar's mmCERT. The ministry also houses the Computer Science Development Council and Computer Federation, which develop ICT policy in the country. It drafted a new Telecommunications Masterplan in 2015, but it's not apparent whether the plan's been approved or whether implementation has begun. While these agencies and the draft plan indicate an awareness of the need for national cyber governance structures, the government's inaction on implementing existing policies or developing new ones means that Myanmar's score for this category remains low.

SCORE: 3

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

Myanmar's legislation to regulate cyber issues is largely focused on content control. It includes the 1996 *Computer Science Development Law*, the 2013 *Telecommunications Act* and the 2014 *Electronic Transactions Law*. Myanmar's score for this category would be improved by greater evidence of effective implementation and a broader focus of legislation to address cybercrime.

SCORE: 4

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

Myanmar participates in some international discussions on cyberspace as a member of ASEAN, ITU-IMPACT, APCERT and the TSUBAME program. It has a relationship with Singapore to develop its military cyber capabilities and receives training through the Myanmar–Singapore Training Compendium. Myanmar also works with South Korea to develop its cyber policy and has recently established a partnership with India to create the India–Myanmar Centre for Enhancement of Information Technology Skills. Broader international engagement beyond the receipt of capacity-building assistance would increase the country's score for this category.

SCORE: 4

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Myanmar's mmCERT works to increase private and public awareness of cybersecurity threats and provides technical assistance to affected stakeholders. While mmCERT publishes regular security alerts, the lack of evidence of an effective response capacity limits Myanmar's score for this category.

SCORE: 3

2 CYBERCRIME

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

The Myanmar Police Force's Criminal Investigation Department and Department of Transnational Crimes are responsible for the enforcement of cybercrime law in Myanmar. In 2015, the police announced plans to establish a cybercrime unit, but it's unclear whether that was achieved. The police have a 'Cybercrime Police' Facebook page and receive training from Australia, Japan and Singapore. Myanmar's score for this category would increase with further evidence of cybercrime response capacity and greater two-way international engagement.

SCORE: 2

3 MILITARY

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

Myanmar's military is reported to have a strong cyber surveillance capability that enables it to monitor online content, opposition to the government, and dissidents in exile. It's believed that Myanmar developed this capability with assistance from Asia–Pacific partners, specifically Singapore and China. While the Myanmar Armed Forces show an understanding of potential cyber threats and the development of capabilities to respond, the country's score for this category would be improved if there were greater transparency about the measures they have adopted.

SCORE: 5

4 BUSINESS

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

The minimal development of Myanmar's ICT industry indicates that there's little dialogue between government and industry on cyber issues. mmCERT provides some contact for the private sector on technical issues, but both government and industry will need to become more active in this space to improve Myanmar's score for this category.

SCORE: 1

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

Scarce infrastructure and low internet penetration inhibit the development of a digital economy in Myanmar. State-owned ISPs continue to skew diversity in the telecommunications sector, while state regulation restricts opportunities for private investment, preventing digital economic development.

SCORE: 2

5 SOCIAL

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

Restricted internet access, limited ICT infrastructure and strong state regulation reduce public awareness, debate and media coverage of cyber matters in Myanmar. Discussion is largely focused on the development of ICT infrastructure and the digital economy and is led by external groups.

SCORE: 2

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 4

Mobile broadband access in Myanmar, at 29/100 people, significantly outpaces fixed broadband penetration rates of 0.35/100, reflecting the dearth of legacy telecommunications infrastructure. Myanmar's national Telecommunications Masterplan hasn't been implemented sufficiently to have a significant effect on connectivity. Additional effort is needed to enable the growth of mobile connectivity in Myanmar to produce benefits.

NEW ZEALAND

Rank 2016: 6th

2015: 6th

—

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	8
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	6
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	6
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	9
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has fixed broadband internet connectivity?	4
c) What percentage of the population has mobile broadband internet connectivity?	10

OVERALL ASSESSMENT

New Zealand has been highly active this year, improving its score in several areas. It has published a new Cyber Security Strategy and passed new cyberbullying legislation to support its already strong cyber governance approach. The recent release of the National Plan to Address Cybercrime and a Defence White Paper will provide structure and improve its capacity to address the different types of threats that emanate from cyberspace. New Zealand's greatest improvement has been in its digital economy, an increasingly mature two-way collaboration between industry and government, and extensive government initiatives to boost digital development. New Zealand has also announced plans to establish a national CERT capability and a NZ$2 billion investment to improve internet infrastructure.

WEIGHTED SCORE 74.6

1 GOVERNANCE

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

New Zealand has a strong governance model for cyber issues and significantly updated its national strategies this year. The National Cyber Policy Office, within the Department of the Prime Minister and Cabinet, remains the key focal point for cyber policy development and coordination. The Government Communications Security Bureau houses the National Cyber Security Centre, which is responsible for securing the networks of the government and New Zealand more broadly. The Ministry of Business, Innovation and Employment continues to play an active role in implementing domestic cyber policy. The Cyber Security Strategy 2015 and its associated action plan were released in December 2015, alongside the new National Plan to Address Cybercrime. New Zealand also updated the Government ICT Strategy and the *New Zealand information security manual*. These changes put New Zealand in a great position to increase its score upon the successful implementation of the new strategies.

SCORE: 8

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

This year, New Zealand has updated its already robust collection of cybersecurity legislation. Parliament passed the *Harmful Digital Communications Act 2015*, which criminalises cyberbullying and online incitement to commit suicide, as well as authorising fines and take-down notices for harmful content. The National Plan to Address Cybercrime refers to an ongoing legislative reform process, including a review of the *Privacy Act 1993*, the *Extradition Act 1999*, the *Mutual Assistance in Criminal Matters Act 1992* and the *Customs and Excise Act 1996*. These are promising updates to New Zealand's legal framework in response to the contemporary challenges of cybersecurity. The establishment and effective operation of the complaints agency and new civil court processes outlined in the Harmful Digital Communications Act and further evidence of the legislative review will cement the reforms and help raise New Zealand's score.

SCORE: 8

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

New Zealand continues to cooperate with international partners on cyber issues in bilateral and multilateral forums. Most of its efforts are focused on the Five Eyes community and NATO, and it has especially strong multilevel ties with Australia. New Zealand undertakes limited Asia–Pacific engagement through the ASEAN – New Zealand Dialogue and is co-chair of the ADMM-Plus Cyber Security Working Group this year. The new Cyber Security Strategy outlines plans to improve New Zealand's international cyber engagement 'with a particular focus on the Asia–Pacific'. Making good on this promise by increasing New Zealand's Asia–Pacific relationships and capacity building is necessary to increase its maturity.

SCORE: 6

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

New Zealand announced plans to establish a national CERT in its Cyber Security Strategy Action Plan. The government has committed to having an official CERT operational from the first quarter of 2017, replacing the efforts of the National Cyber Security Centre. In May 2016, the government approved a budget of NZ$2.2 million to set up the new organisation within the Ministry of Business, Innovation and Employment. Relocating the CERT function away from the impenetrable intelligence environment of the Government Communications Security Bureau is a favourable decision and is likely to facilitate greater engagement with the country's private sector. The execution of these plans and the opening of CERT-NZ's doors in 2017 will raise New Zealand's score in this area.

SCORE: 7

2 CYBERCRIME

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

The cybercrime and high-tech crime units within the New Zealand Police work to prevent and punish online crime. Based on a comprehensive legislative framework, there are law enforcement efforts to tackle financial crime, online child exploitation, identity theft and internet scams. Reporting cybercrime in New Zealand has become easier through the establishment of 'The Orb', a secure online platform through which to notify the government of any online incident. The new National Plan to Address Cybercrime outlines plans to enhance New Zealand's police training, undertake legislative reform and bolster international cooperation on cybercrime. International cooperation is New Zealand's main shortcoming in this area, so delivering on the promise of greater Asia–Pacific engagement may help raise New Zealand's score.

SCORE: 7

3 MILITARY

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

The release of New Zealand's Defence White Paper in June 2016 has provided insight into the military's role in cyberspace. It identifies the strategic benefits and vulnerabilities created by connectivity and outlines the New Zealand Defence Force's intent to defend its networks and retain operability through a new 'cyber support capability'. The White Paper describes cyber capability development as the modernisation of existing roles and responsibilities within the military, rather than the creation of new ones. This contrasts with the Defence Minister's description of cyber capabilities as 'a significant weapon', and ambiguity remains about the funding, scale and authorities of any new initiative. Improving the coherence of the narrative and establishing detailed plans will further improve New Zealand's performance in this area.

SCORE: 6

4 BUSINESS

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

New Zealand has demonstrated significant growth in the maturity of the dialogue between its government and industry on cyber issues. In May 2016, it held its inaugural Cyber Security Summit, which was run by Connect Smart and hosted by the Minister for Communications. The event brought together CEOs and public officials to strengthen cross-sector dialogue and inspire greater prioritisation of cybersecurity issues in the private sector. There's also evidence of strong collaboration in the establishment of the CERT in the form of a public–private advisory board to help inform the process and drive policy choices. Similarly, the recent update of the *New Zealand information security manual* involved a process of private-sector stakeholder consultation. These initiatives indicate a mature two-way dialogue, the importance of which is articulated in the new Cyber Security Strategy. New Zealand's pleasing new efforts in this area have caused its score to increase significantly.

SCORE: 8

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

The digital economy plays a strong and growing role in the nation's economy. In 2015, the tech sector employed 5% of the workforce and produced 9% of the country's exports. The government's awareness that New Zealand's digital economy has the potential to add an extra NZ$34 billion to the economy has driven an uptick in supportive policies. A comprehensive new Digital Economy Work Plan, released in January 2016, outlines eight agenda areas for government effort and investment, including digital business, digital government and digital skills. A tax reform that came into force in October 2015 exposes foreign digital services to the same GST rates as local companies. The change, which includes fines for the use of virtual private networks, is an effort to create a level playing field and enable New Zealand corporations to remain competitive. The government has also proposed a new cyber credentials scheme—a cybersecurity rating system that companies can use to guarantee certain security standards and boost consumer confidence in digital services. These initiatives represent an elevation of the role of the digital economy in New Zealand.

SCORE: 9

5 SOCIAL

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

New Zealand's media, academic and social networks continue to engage in a healthy public debate about cyber issues. Connect Smart, a cyber awareness platform led by the National Cyber Policy Office, promotes October as Cyber Security Awareness Month in partnership with the Five Eyes community. An independent not-for-profit, NetSafe, continues to develop digital citizens, engaging with initiatives such as Safer Internet Day. Internet NZ also works to advocate for cyber issues through avenues such as the NetHui conference, a debate and sharing of best practice. There's been little change in New Zealand's already strong cybersecurity discussions, so its score remains the same.

SCORE: 9

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 4

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 10

This year, the government has made a NZ$2 billion investment in upgrading national telecommunications infrastructure. The Ultrafast Broadband Initiative and the Rural Broadband Initiative are intended to improve national connectivity over the coming decade.

NORTH KOREA

Rank 2016: 22nd
2015: 20th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	1
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	8
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	0
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	1
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	1
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	1

OVERALL ASSESSMENT

Despite a lack of transparency on cyber governance structure and policy, it's clear that North Korea's cyber operations are highly organised and that the leadership deems cyberspace to be of great strategic value. North Korea's strong top-down control and military focus have stifled the potential benefits of cyberspace, such as the development of a digital economy or social networks. Instead, access to the internet is highly restricted and the government uses cyberspace as a tool of state power against its conventionally superior international adversaries. For this reason, North Korea doesn't participate in international debates on cybersecurity or engage in multilateral conflict-prevention measures.

WEIGHTED SCORE 16.7

1 GOVERNANCE

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

North Korea maintains centralised control over cyberspace, mostly concentrated in the hands of the military. The Reconnaissance General Bureau (RGB), specifically Bureau 121, is the main organisational body responsible for governing peacetime cyber issues. It's infamous for spying, conducting network disruptions and other clandestine operations. The RGB reports directly to Kim Jong Un, indicating the high significance placed on cybersecurity by the leadership. The bureau appears to have undergone recent restructuring, absorbing additional units and bureaus associated with cyberwarfare and espionage. This represents further centralisation, but governance efforts seem limited to the military. Expanding to a broader whole-of-government approach and articulating a clear national strategy would raise North Korea's score.

SCORE: 3

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

The existence of strong national cyber regulations is implied by the government's effective implementation of nationwide internet access control. The Ministry of Posts and Telecommunications manages public use of communication technologies, while the Central Scientific and Technological Information Agency is responsible for managing North Korea's Kwangmyong intranet. Regulation appears limited to issues of access and content control, and the lack of accessible legislation that articulates these measures reduces North Korea's score in this area.

SCORE: 1

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

North Korea doesn't regularly participate in multilateral discussions on international cyber issues, but it does engage bilaterally with selected international partners. China provides significant technical support, including internet infrastructure and staff training, and hosts personnel to complete national cyber operations outside the restrictions of North Korea's networks. Russia also offers assistance by training North Korean hackers, both in Russia and in North Korea. In 2012, Iran and North Korea signed a technology treaty that encourages bilateral IT information sharing in their efforts against 'common enemies'. In general, North Korea is a passive recipient of technical capacity-building support.

SCORE: 3

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

There's no evidence of a CERT in North Korea. There's little need for this capability, given the country's low level of connectivity and low vulnerability to exploitation in cyberspace.

SCORE: 0

2 CYBERCRIME

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

North Korea shows no sign of possessing a cybercrime police unit, probably because of its limited exposure due to low connectivity rates. On the contrary, it's thought to run a department, referred to as Office 39, specifically tasked with generating state revenue through cybercrime campaigns against foreign targets. Questions have been raised about North Korea's involvement in this year's hacking of SWIFT, the international bank messaging software.

SCORE: 0

3 MILITARY

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

North Korea's military boasts sophisticated cyber capabilities and appears to favour cyberspace as an avenue for asymmetrical confrontation with its enemies. While the RGB conducts covert cyber operations during peacetime, the General Staff Department of the Korean People's Army is responsible for cyber operations in support of conventional military efforts during conflict. In this sense, North Korea conceives cyber operations both as an independent force projection and as a supporting element of military activity. There appears to be a complex organisational structure and division of responsibilities, supported by significant manpower of around 6,000 cyber officers. These offensive capabilities are often used to create a 'second front' against South Korea, targeting its government, infrastructure and private-sector networks. North Korea exhibits a very coherent and consistent approach to cyberspace; however, there's no published strategy or accessible doctrine to support that approach. This shortcoming, and the absence of mature international military engagement, have limited North Korea's score for this indicator.

SCORE: 8

4 BUSINESS

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

There's no evidence of dialogue within North Korea, where most companies are owned by the state. One of the few cases of foreign investment is North Korea's single ISP, which is a joint venture between the Ministry of Post and Telecommunications and a Thai company called Loxley Pacific. Another is that of Orascom, an Egyptian mobile provider, which successfully gained 3 million North Korean customers through 'Koryolink', a joint venture with the government. However, this year it was challenged by a government-supported local competitor, experienced difficulty repatriating profits and officially lost control of its operation, despite owning a majority stake. This poor track record of relations between government and industry is likely to discourage foreign investment in the digital economy and leave North Korea's government–business dialogue non-existent.

SCORE: 0

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

The digital economy doesn't form a significant part of North Korea's economy. However, given that foreign computers are forbidden, there's some limited activity in the form of a domestic computer industry. The Pyongyang Informatics Centre develops software, while the Korea Computer Centre manufactures hardware devices. The Korea Computer Centre operates a small overseas trading company, Shinheung, selling tablet PCs and North Korea's Red Star operating system in Germany, China and Syria. The ousting of Orascom, which brought 3G cellular networks to the Hermit Kingdom, bodes poorly for the future of North Korea's digital infrastructure, and the quality of service may regress as a result.

SCORE: 1

5 SOCIAL

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

Because of the widespread lack of connectivity, there's little awareness of cyber issues outside government-mandated operations. Unfortunately, any public dialogue that did exist would be likely to be stifled by strong government regulation and censorship. However, cyber skill recruitment campaigns are run through the Korea Computer Centre and various universities in order to absorb talented young hackers into the regime's cyber operations.

SCORE: 1

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 1

North Korea restricts domestic access to the internet and, while its domestic intranet is freely available, low income levels and poor public services mean that only several thousand residents can access it. Access to the broader internet is limited to senior government officials, and accurate numbers are difficult to discern. Efforts to circumvent the state's content-control mechanisms are frequent but normally unsuccessful.

PAKISTAN

Rank 2016: 18th

2015: NA

—

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	3
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 e.g. a Computer Emergency Response Team (CERT)?	1
2 – CYBERCRIME	
a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	4
3 – MILITARY	
a) What is the military's role in cyberspace, policy, and security?	4
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	4
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	3
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	2

OVERALL ASSESSMENT

After many years in the making, the Prevention of Electronic Crime Bill has finally progressed through both houses of Pakistan's parliament, but the controversial bill now faces a challenge in the High Court. Looking beyond the legislative sphere, Pakistan's cyber maturity is uneven: it has some cybercrime and military capability but an underdeveloped CERT and international engagement program. Pakistan is beginning to harness the opportunities presented by the digital economy, but poor internet connectivity continues to be a limiting factor to its spread in the near term.

WEIGHTED SCORE 26.6

1 GOVERNANCE

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

Pakistan's Ministry of Information Technology and Telecommunication is the country's lead agency for the planning, coordination and implementation of policies and programs relating to IT. In 2004, the ministry launched Pakistan's national broadband policy, which aimed to facilitate the spread of high-speed internet across the country, develop the number and maturity of ISPs and encourage private investment in broadband service provision. The Pakistan Telecommunication Authority reports to the ministry and works to regulate and filter Pakistan's internet. It also provides policy and service delivery advice to government. In 2004, the government announced that it would create a National Cyber Strategy, but that document has failed to eventuate, as has the promised *National Cyber Security Council Act* (also from 2004), which was proposed to help create a national public–private cybersecurity advisory body.

SCORE: 3

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

In August 2016, the Prevention of Electronic Crime Bill passed both the upper and lower houses of Pakistan's parliament. The Bill includes provisions related to information security and, controversially, information control. It's is now facing a legal challenge in the High Court, led by the opposition party Pakistan Awami Tehreek, which argues that the law is unconstitutional, is against basic human rights and could be used to target political dissidents. Pakistan has theoretically enshrined several privacy provisions in its Constitution and via international conventions such as the International Convention on Civil and Political Rights. State surveillance is enabled by the *Investigation for Fair Trial Act 2013*, which permits access to any form of computer- or mobile-based communications, including emails and data. The *Telecommunication Act 1996*, amended in 2006, facilitates federal government regulation of the internet. Pakistan has enacted cybercrime legislation through the *Cyber Crime Act 2007,* but implementation is said to be very poor.

SCORE: 3

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

Pakistan engages in a limited range of international cyber-oriented discussions. Much of its current international outreach is tied to work with the ITUhosting workshops and receiving aid for training programs. Pakistan also probably leans on traditional allies such as China for assistance with cyber issues. The government has applied for membership of the Shanghai Cooperation Organisation, which could boost Pakistan's international engagement on cyber issues if it's admitted.

SCORE: 2

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

PakCERT is Pakistan's national CERT but reportedly its activities have traditionally been limited to raising public awareness. In the past, PakCERT provided more extensive training programs and public advisory updates, but they seem to have ceased in 2009.

SCORE: 1

2 CYBERCRIME

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

The National Response Centre for Cyber Crime (NR3C) in the Federal Investigation Agency is the national-level body responsible for combating high-tech crime in Pakistan. It's responsible for fighting online crime in Pakistan and has the ability to carry out digital forensics, IT system security audits and penetration testing. The NR3C works with other law-enforcement and judicial bodies to investigate online crime and raise awareness and resilience. It also performs its awareness-raining role in the broader community and has established the Cyber Scouts program to train students in IT skills. The NR3C also maintains an SMS-based cyber alert service and 24/7 cyber rescue hotline for the public to report cybercrimes.

SCORE: 4

3 MILITARY

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

Pakistan is said to possess both defensive and offensive cyber capabilities, although their extent is largely unknown. Most often deployed against neighbouring India during periods of increased geopolitical tension, this capacity is most probably housed within the Directorate General for Inter-Services Intelligence. The intelligence service has reportedly been attempting to acquire the technology to allow the tapping and surveillance of international undersea communications cables making landfall in Karachi.

SCORE: 4

4 BUSINESS

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

Pakistan's government has established a national ICT R&D fund that seeks to boost government–industry collaboration in several ways, including industry–academia partnerships, building the domestic IT workforce with industry and working to appeal as a location for internationally outsourced IT jobs. Using the fund, in 2016 the government has established the National Incubation Center in Islamabad to foster 'economic growth through innovation'. The National University of Sciences and Technology has also established its own Technology Incubator of Pakistan, which replicates the government's incubation centre but in an academic environment.

SCORE: 4

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

For Pakistan's 2015–16 federal budget, the IT Ministry proposed the extension of the existing tax exemption on the export of IT services. It also proposed removing sales taxes on domestically purchased computers and laptops to help boost internet connectivity. Pakistan's e-commerce market has risen exponentially in recent years and, while cash-on-delivery online shopping still comprises 95% of online purchases, the expansion of branchless banking in Pakistan could see payment methods move online. The proliferation of cheap Chinese smartphones and more affordable data plans will boost the e-commerce sector further. The Pakistan Telecommunications Authority recently concluded a three-day conference in partnership with the Internet Society – Asia Pacific to discuss the current status of Pakistan's digital economy and opportunities for growth and sustainable development.

SCORE: 3

5 SOCIAL

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

Public awareness of cyber issues in Pakistan remains low, and coverage of cyber topics in the media is generally restricted to concerns related to overzealous information control provisions in cybercrime and cybersecurity legislation. The Pakistan Information Security Association, the membership of which comprises information security professionals, conducts events and prepares publications to boost the skills and awareness of its members. iPOP (the Internet Policy Observatory Pakistan) provides research and analysis on public-interest ICT policy and regulation in Pakistan to range of stakeholders, including governments, regulators, operators, community organisations and multilateral institutions.

SCORE: 2

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 2

Pakistan has a growing internet population, largely because of steady growth in mobile internet connectivity, which is currently used by around 13% of the population. This growth was largely initiated by the introduction of 3G/4G mobile networks to the country in 2014 and is helping to offset very low levels (0.9%) of fixed-line broadband penetration.

PAPUA NEW GUINEA

Rank 2016: 21st
2015: 19th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	4
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	3
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	2
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	1
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	1
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	1

OVERALL ASSESSMENT

Papua New Guinea (PNG) continues to take a limited approach to cyber governance despite recent efforts at legislative reform, including a Cybercrime Policy and a sim card registration initiative. PNG's policy implementation is patchy, while its international engagement is centred on financial and technical support. PNG recognises potential cyber threats to its armed forces, but it doesn't have the capability to defend against them. The government has sought out some private-sector partnerships to develop the country's ICT industry, which is currently impeded by limited infrastructure. While a large rural population restricts internet penetration, public awareness of cyber issues is evident. A more comprehensive cyber strategy and effective policy implementation would improve PNG's score.

WEIGHTED SCORE 18.7

1 GOVERNANCE

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

PNG's organisational structure for cybersecurity is limited and largely focused on the development of ICT infrastructure. The Department of Communication and Information and the National Information and Communications Technology Authority are the principal agencies responsible for addressing cyber matters. On 20 June 2016, the authority launched PNG's first National Cybercrime Policy. This was the first significant cybersecurity governance effort since the country's 2013 National Broadband Policy, boosting the PNG's score for this category.

SCORE: 4

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

PNG regulates online content and user access to telecommunications networks through the *Telecommunications Act 1996* and the *National Information and Communications Technology Act 2009*. Recent efforts at improving legislation in the Cybercrime Policy of 2016 and Regulation on Sim Card Registration of 2016 demonstrate a desire to crack down on cybercrime and improve the administration and management of information. In a promising sign, PNG's new Cybercrime Code Act was passed by the parliament in early August 2016. However, the Act has received some criticism for its potential to enable government censorship. Evidence of implementation coupled with a more comprehensive legislative framework would improve PNG's score.

SCORE: 3

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

PNG participates in cybersecurity discussions through its membership of APEC, IMPACT, the Pacific Islands Telecommunications Association, the Pacific IT Regulatory Centre and the Asia–Pacific Telecommunity, for which it hosted the 9th Policy and Regulation Forum. It also receives technical and financial support from various donors, including a US$53.3 million grant from the Chinese Government for an integrated government information system, through the Australia–PNG Cooperation Initiative and from the Asian Development Bank. Broader international engagement beyond technical support and greater use of bilateral relationships would improve PNG's score for this category.

SCORE: 2

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

PNG no longer has access to a CERT since the closure of PacCERT.

SCORE: 0

2 CYBERCRIME

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

The Royal Papua New Guinea Police Intelligence Unit is responsible for enforcing cybercrime law in PNG. In 2014, PNG police established a cybercrime taskforce, with plans to provide training for officers and increase the force's response capability, but effective implementation of this initiative remains to be seen. The effective implementation of the taskforce, new cybercrime legislation and the establishment of a specific unit dedicated to cybercrime would increase PNG's score for this category.

SCORE: 1

3 MILITARY

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

There's no evidence of a clear policy or strategy guiding the PNG Defence Force's approach to cyberspace. While PNG's 2013 Defence White Paper alluded to cyber threats, indicating some awareness, the PNG Defence Force doesn't appear to have any capability to defend against them.

SCORE: 1

4 BUSINESS

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

Dialogue between government and industry on cyber issues is limited, and no officially recognised national or sector-specific initiatives are apparent. The PNG Government recognises the value in public-private-sector partnerships to develop the country's ICT infrastructure.

SCORE: 2

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

A lack of ICT infrastructure and a large rural population restrict digital economic activity in PNG. While the government has expressed a desire to boost economic growth in its *PNG Vision 2050* report, further investment and diversification of the country's service providers is necessary.

SCORE: 1

5 SOCIAL

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

Although internet access is heavily restricted by PNG's rural population and lack of ICT infrastructure, public awareness, debate and media coverage of cyber issues are evident in the country's blogging community, which regularly comments on social and political issues. PNG media usually face little government censorship, as the Media Council of PNG serves as an advocate for media freedom.

SCORE: 5

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet

SCORE: 1

Fixed-line broadband connectivity in PNG is highly limited, reaching only 0.2/100 people. This reflects the challenges of providing this infrastructure in PNG's geography and reaching its highly rural population. Mobile broadband connectivity is higher at 6/100, but that's still significantly below connectivity in other Asia–Pacific countries.

PHILIPPINES

Rank 2016: 14th
2015: 13th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	5
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	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 e.g. a Computer Emergency Response Team (CERT)?	0
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, policy, and security?	3
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	4
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	5
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	5

OVERALL ASSESSMENT

The Philippines has delivered implementation plans for its 2012 Cybercrime and Data Privacy legislation, including the establishment of a new national coordinating department for cyber issues. However, from a military perspective, developments appear to have stagnated. While the Philippines engages in multiple international forums, there is room for the nation to take on a greater leadership role in this space. The Philippines' burgeoning digital economy requires less government regulation, greater public-private partnership and an updated digital strategy in order to fulfil its potential.

WEIGHTED SCORE 41.6

1 GOVERNANCE

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

The Philippines has updated its governance structure in an effort to streamline its national cyber policy. Recent legislation established a new Department of Information and Communication Technology, the first overarching entity to oversee the planning, implementation and coordination of national cyber policy. The Philippines already possessed a variety of bodies responsible for cyber issues. This reform prescribes the absorption of certain agencies, such as the Information and Communications Technology Off ice and National Computer Centre, under the operation of the DICT, while other agencies, such as the National Privacy Commission and Cybercrime Investigation and Coordination Centre, will continue to operate under DICT guidance. There is an expected six-month transition period to fully implement these changes to the Philippines' cyber governance structure. Tangible delivery of the legislated changes and evidence of efficient policy coordination under the DICT will raise the Philippines' score.

SCORE: 5

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

Former President Aquino signed the Republic Act 10844 in May, establishing the Department of Information and Communication Technology (DICT). The legislation, also known as the DICT Act, outlines the responsibilities and powers of the DICT as well as provisions relating to ICT sector regulation and consumer protection. In addition, the Philippines finally issued the 'Implementation Rules and Regulations' for the 2012 Cybercrime Prevention Act last August. The regulations define a spectrum of cybercrimes and penalties, and lay out the relevant governmental roles and responsibilities. Similarly, pursuant to the provisions of the 2012 Data Privacy Act, the Philippines established the long-awaited National Privacy Commission in March and published a draft of the 'Implementing Rules and Regulations' for the Act in June. These proposed regulations outline standards for data management, transfer and breach notification requirements. These are positive steps towards improving the Philippines' historically weak legislative implementation and its score for this indicator has risen to reflect that.

SCORE: 6

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

The Philippines participates in cyber security discussions as a member of APEC, IMPACT and APCERT. Under ASEAN, the Philippines partnered with Japan on a Joint Information and Security Awareness raising initiative. A proposal put forward by the Philippines to create a cyber security working group within the ASEAN Defense Ministers Meeting was adopted in May, and will be co-chaired with New Zealand. The Philippines maintains special relationships with the United States, Japan, and Australia through the Philippines Comprehensive Partnership agreements. These efforts would be bolstered by the Philippines taking a greater leadership role in regional cyber discussions.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

The Philippines no longer has a CERT capacity, after PHCERT was disbanded in June 2016.

SCORE: 0

2 CYBERCRIME

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

The Philippines has consolidated its national approach to cybercrime in accordance with the 'Implementation Rules and Regulations' of the 2012 Cybercrime Prevention Act, released in August. The regulations define various cybercrimes, such as illegal access, data interference and cyber fraud, and outline their associated punishments. It also cements the law enforcement responsibilities of the National Bureau of Investigation and the Philippine National Police, and the prosecution role of the Department of Justice's Office of Cybercrime that was created under the Act. More broadly, the Philippines' cybercrime policy efforts are coordinated by an inter-agency body, the Cybercrime Investigation and Coordinating Centre, under the Office of the President. Improving cooperation with international partners to combat regional cybercrime issues will help improve this score.

SCORE: 6

3 MILITARY

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

The Armed Forces of the Philippines demonstrate an awareness of the potential use of cyberspace to achieve strategic goals but it is unclear the extent to which they have developed capabilities to do so. Despite announcements at the end of 2012 of plans to establish a cybersecurity operations centre, no evidence of its implementation has materialised. Establishing clear cyber responsibilities within the military and articulating a national military cyberspace posture will raise the Philippines score.

SCORE: 3

4 BUSINESS

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

The Philippines have indicated an understanding of the importance of the digital economy to the development of the broader economy; however there is limited activity to back this up in practise. The Department of Science and Technology continues to implement the Digital Strategy 2011-2016, with a current focus on free Wi-Fi in public places, eGovernment initiatives and developing the ICT sector. Microsoft Philippines is still driving force behind Filipino digital development, releasing an 'ICT Manifesto' for the Philippines and partnering with local telecommunication company to address digital skills shortages. However, collaborative cross-sector dialogue remains limited. In fact, Philippine telecommunication companies have explicitly cited overbearing government regulation as a barrier to digital development. The Philippines needs to expand its public-private dialogue in this space to raise its score for this category. The development of an updated national strategy for the digital economy will also be important to sustain the Philippines' advances in this area.

SCORE: 4

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

The Philippines' digital economy comprises a significant proportion of its economic activity. The electronics industry, focused on semiconductors, continues to grow and is expected to reach an export value of US$30 billion by the end of 2016. Having said that, it is the services sector that dominates the economy in general, representing 60% of GDP in 2015. Specifically, the Philippines has risen to the 34th largest commercial services exporter in the world, up from 47th in 2005. The continued dynamism of these sectors reflects the country's digital development. Unfortunately, the low level of bank account and credit card ownership continues to inhibit the Philippines' digital economic growth. However, promising innovation in mobile finance technology may help overcome this issue. A bigger problem remains the Philippines' incredibly low internet speeds and over regulation by government. Until this is resolved through infrastructure improvements, government deregulation and industry diversification, the digital economic potential of this country will remain unrealised, and the Philippines score has been reduced to reflect this.

SCORE: 5

5 SOCIAL

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

Public awareness and debate of cyber issues in the Philippines is evident in the country's active blogging community. In fact, Filipinos spend the most time online out of all countries in the Asia-Pacific, at more than 5 hours a day. Official media coverage of cyber matters is represented in reporting through local and international outlets. Cyber issues gained a higher profile in public discussion when the Commission on Elections suffered a severe data breach in April and the hacking of several government websites in July. However, violence against critical journalists remains a problem. Improved freedom of speech and greater academic engagement on cyber issues would improve the Philippines' score for this category.

SCORE: 6

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 5

Like many countries in the region, the majority of internet users in the Philippines are connecting via mobile rather than fixed line broadband. Mobile broadband reaches 42% of the population, compared to only 3% using fixed line connections. Internet speed remains a perennial obstacle for the Philippines, with the second slowest download speed in Asia.

SINGAPORE

Rank 2016: 5th
2015: 4th

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

OVERALL ASSESSMENT

Singapore again rates highly in this year's report, maintaining its place as the most mature cyber nation in Southeast Asia and in the top five for the Asia–Pacific region. This score is based on a solid legislative and organisational foundation spearheaded by Singapore's Cyber Security Agency (CSA), which has wasted no time in implementing an impressive agenda of programs and initiatives following its creation in 2015. Singapore's dialogue with the private sector is a best practice example for the region and will ensure that the country is well positioned to continue to harness economic opportunities created by the internet. Singapore's international engagement, particularly in the area of capacity building, is one of the few areas where it falls slightly behind the maturity of its neighbours.

WEIGHTED SCORE 80.2

1 GOVERNANCE

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

Singapore's CSA, created last year under the Singaporean Government's National Cyber Security Masterplan 2018, has worked hard to establish itself as one of the region's leading central government cybersecurity bodies. It has implemented a strong agenda of programs that reach out across government, the private sector and civil society. Examples include the holding of Exercise Cyber Star (a multisector national cyber incident management exercise), the creation of a cyber forensics laboratory to provide forensic support to critical information infrastructure sectors and the establishment of programs with industry to build skills. Communications and Information Minister Yaacob Ibrahim has also committed to spending up to 10% of Singapore's IT budget on boosting cybersecurity.

SCORE: 9

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

Singapore is said to be drafting a new cybersecurity bill intended to provide the CSA with expanded powers to assist in the protection of Singapore's critical information infrastructure. Details of the new law are thin, but it may include provisions for mandatory breach reporting. The Bill will be tabled in parliament in 2017 and will complement Singapore's existing primary cybersecurity legislation, the *Computer Misuse and Cybersecurity Act*, which was last amended in 2013. Beyond cybersecurity, Singapore has a strong set of legislation relating to cybercrime, ISP licensing and regulation, electronic transactions, spam and copyright infringement.

SCORE: 8

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

Singapore engages in a strong international program that features ministerial and other high-level discussions on cyber issues alongside official-level meetings, particularly under the auspices of ASEAN. The CSA has signed several MoUs with other cyber and coordinating ministries inside and outside the region. Multilaterally, Singapore is active in forums such as the East Asia Summit, ASEAN cybercrime meetings and the ASEAN Regional Forum, where in October 2015 it co-chaired a workshop with the US on cyber confidence-building measures. Singapore also serves as the 'voluntary lead shepherd' of the ASEAN Senior Officials Meeting on Transnational Crime / ASEAN Ministerial Meeting on Transnational Crime.

SCORE: 7

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

SingCERT, created in 1997 and housed in the CSA since 2015, works to detect, resolve and prevent security-related incidents on the internet affecting Singaporean companies and users. In October 2015, Singapore hosted the ASEAN CERTs Incident Drill, and has agreed to facilitate the drill again in 2016. SingCERT signed an MoU with CERT-In to enable information sharing and incident response collaboration. Singapore's score is reduced in this category because other CERTs with comparable capabilities engage in a much wider program of capacity building in the region.

SCORE: 7

2 CYBERCRIME

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

The Financial and Securities Offences Directorate in the Singapore Police Force is home to the Technology Crime Unit, which investigates cybercrime and technology-enabled crime and participates in reviews of crimes and policies related to cybercrime. Singaporean Home Affairs Minister K Shanmugam has announced the National Cybercrime Action Plan and accompanying legislation to be introduced in 2017. The plan has four key priorities: boosting end-user education; enhancing government capacity to fight cybercrime; strengthening law and criminal justice frameworks; and improving international partnerships and engagement.

SCORE: 8

3 MILITARY

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

Singapore's military capabilities in cyberspace are reported to be among the best developed in Asia. It has publicly stated its interest in developing both offensive and defensive cyber capabilities as far back as the its 2000 Defence White Paper. The Defence Technology Group, the Defence Sciences and Technology Agency and the Defence Science Organisation all contribute to Singapore's military technical developments. The Singapore Armed Forces also maintain the Cyber Defence Operations Hub, which protects Singapore's military networks, and it was recently announced that the number of personnel assigned to the hub would double by 2020. Despite Singapore's deep technical capabilities, the military's strategic discussions on the use of cyberspace appear to be underdeveloped.

SCORE: 8

4 BUSINESS

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

Singapore has a very high level of substantive two-way dialogue between its public and private sectors. These relationships are encouraged by high-level policy documents such as the National Cyber Security Masterplan 2018 and practically enacted in a swathe of tailored programs. Among them are Exercise Cyber Star, the Cyber Security Associates and Technologists Programme, Capabilities Development Grants, the Cyber Security Awareness Alliance, the International Advisory Panel for the National Cybersecurity R&D Programme, and the iSPRINT program for small and medium-sized enterprise ICT productivity and growth. These exist alongside an expansive CSA – private sector MoU program and a strong culture of consultation when forming key national documents and strategies.

SCORE: 10

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

Singapore's digital economy is a model for best practice for the region and the world. Singapore was the highest ranking country in the 2016 World Economic Forum Networked Readiness Index—the second year it has finished in top position. Late in 2015, the government unveiled the new 30-member Committee on the Future Economy, which includes government and industry leaders, to help solidify Singapore's position as a best practice leader in this area and to enable its continuous repositioning to best harness new technologies and opportunities for growth. Singapore's e-commerce market was valued at US$1 billion in 2015 and is expected to make up 6.7% of all retail sales by 2025. Singapore has also been identified as the most active country in Southeast Asia for venture capital and start-up markets, with the largest deal quantity and deal value of any of its neighbours.

SCORE: 9

5 SOCIAL

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

The Infocomm Development Authority of Singapore conducts an impressive suite of awareness-raising events, training workshops and programs and delivers many educational IT scholarship opportunities. Singapore's media and public commentary on cybersecurity issues is at a very developed level, and the public's understanding of IT issues is among the most developed in the region.

SCORE: 9

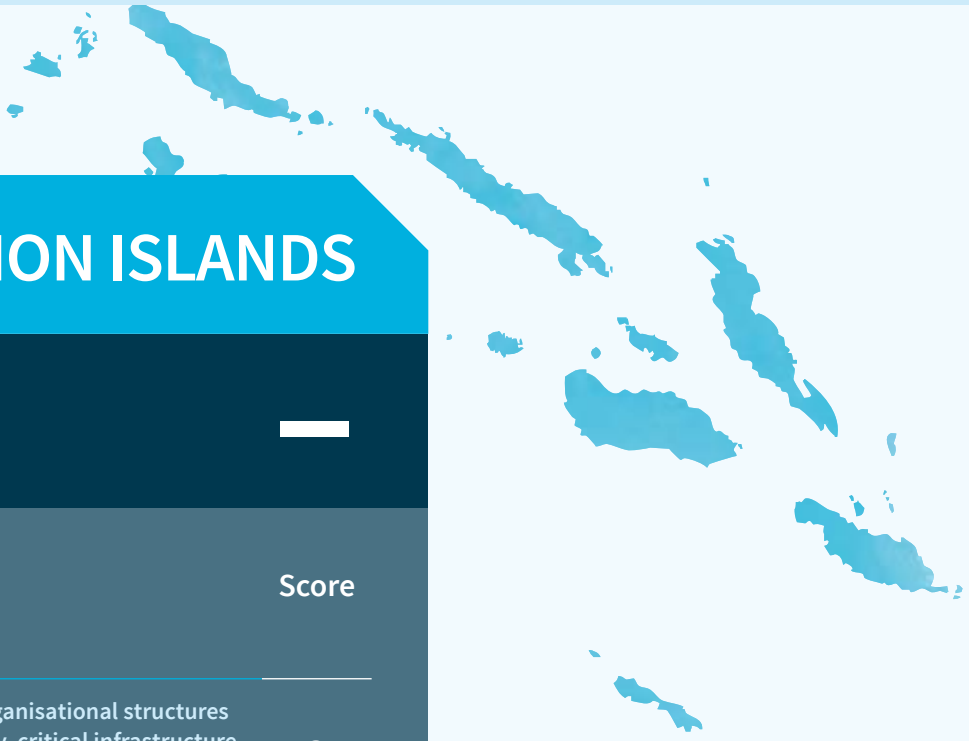
b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 3

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 10

Singapore's mobile internet connectivity sits at 142%, the largest number in this year's maturity metric and reflective of Singapore's highly networked society. Fixed-line broadband connectivity is comparatively low: only 26% of the population use it to get online.



SOLOMON ISLANDS

Rank 2016: 23rd

2015: NA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	3
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	0
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	2
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	0
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	1
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	1
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	2

OVERALL ASSESSMENT

Solomon Islands has only basic organisational structures and policies relating to the telecommunications sector. Given its relatively underdeveloped economy, the government's focus remains on issues of sector liberalisation, infrastructure development and improving internet access. Due to low connectivity, Solomon Islands is yet to confront the risks of cyberspace and has no CERT, cybercrime or cyberwarfare capabilities. At this stage, it's a passive aid recipient, but it does participate in some multilateral cooperation efforts in its near region. The government also shows a promising willingness to partner with industry, which will serve both of them well as the digital economy develops.

WEIGHTED SCORE 11.9

1 GOVERNANCE

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

Solomon Islands has basic organisational structures through which to govern telecommunications. The Ministry of Communications and Aviation is the central body responsible for the development and coordination of ICT policy, while the Telecommunications Commission of Solomon Islands (TCSI) is responsible for industry regulation. Given its nascent development, Solomon Islands lacks policies or strategies specific to cybersecurity. Instead it possesses several that encompass concepts of infrastructure improvement and ICT sector development, such as the National Development Strategy (2011–2020) and the 2013 National Infrastructure Investment Plan. The ministry is working towards increasing competition in the telecommunications sector, bolstering regulation and improving internet access. Meanwhile, the Ministry of Finance has an ICT Support Unit responsible for the procurement and management of government computer networks.

SCORE: 3

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

There are no specific cybersecurity or cybercrime laws in Solomon Islands; however, the *Telecommunications Act 2009* established the TCSI. This is an independent regulatory agency for the ICT industry, encouraging sector liberalisation, service affordability and infrastructure development. The Royal Solomon Islands Police Force (RSIPF) acknowledges the lack of cyber provisions in its legislative framework and has committed to a legal review process once cybercrime poses a tangible threat to Solomon Islands.

SCORE: 0

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

Solomon Islands' international engagement involves the passive acceptance of capacity-building assistance and involvement in Asia–Pacific multilateral cooperation. The Asian Development Bank provides significant aid to the country, most importantly for funding a new submarine cable slated to come into operation by the end of 2017. However, Solomon Islands has also actively participated in Asia–Pacific cyber initiatives such as the Pacific ICT Ministerial Meeting and Cyber Safety Pasifika. It's currently the chair of the Melanesian Spearhead Group, an intergovernment organisation that also addresses emerging cyber issues in the region.

SCORE: 2

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

As Solomon Islands has low connectivity and limited exposure to cyber threats, it has no CERT.

SCORE: 0

2 CYBERCRIME

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

There's no dedicated cybercrime unit in the RSIPF, but there's an indication of minor engagement with the issue in Asia–Pacific forums. Solomon Islands was one of 10 Pacific countries to attend an Asia–Pacific cybercrime training workshop in Tonga in February 2016 to identify common challenges and share best practice. It agreed to participate in the Melanesian Spearhead Group's audit of the members' national cybercrime legislation in order to improve Asia–Pacific standards, and has also applied for an INTERPOL membership. Despite this outward-facing engagement on cybercrime, there's no evidence of domestic activity.

SCORE: 1

3 MILITARY

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

Solomon Islands lacks an official military force.

SCORE: 0

4 BUSINESS

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

There's evidence of some dialogue between the Solomon Islands Government and the private sector on cyber issues. The development of the 2013 National Infrastructure Investment Plan reportedly involved extensive consultations with key stakeholders, including the private sector, civil society and development partners. The plan also advocates for close industry involvement in Solomon Islands' future infrastructure development efforts. Similarly, the TCSI has consulted with Solomon Telekom over the process of internet domain name management. At this stage, the dialogue is limited to infrastructure issues; expanding the scope and scale of the partnership will increase Solomon Islands' score.

SCORE: 2

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

The economy of Solomon Islands is still heavily reliant on agriculture and forestry. Under the TCSI, the telecommunications sector has been liberalised in an effort to increase the quality and affordability of digital services through competition. Within Melanesia, Solomon Islands is leading in the take-up of mobile technology, which is expected to reach 57% of the population by 2020. However, ICT makes a very low contribution to GDP and poor internet penetration continues to stifle the country's digital economic development.

SCORE: 1

5 SOCIAL

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

There's a very low level of public discussion of cyber issues in Solomon Islands. The high illiteracy rate tends towards a reliance on radio for news and a low engagement with online media. Awareness campaigns such as Cyber Safety Pasifika, championed by the RSIPF, and One Laptop per Child, supported by the Ministry of Education and Human Resources Development, are run to boost youth engagement with cyber issues.

SCORE: 1

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 2

Currently, less than 1% of the population have access to a fixed internet connection due to the high cost of establishing infrastructure across many islands to a poor population that can't afford the services. Instead, 11% of Solomon Islanders are getting online via their mobile devices. The completion of the new submarine cable at the end of next year, thanks to the Asian Development Bank, is expected to improve connectivity and trigger a significant drop in service costs.

SOUTH KOREA

Rank 2016: 2nd
2015: 3rd

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

OVERALL ASSESSMENT

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

WEIGHTED SCORE 83.6

1 GOVERNANCE

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

South Korea has strong cyber governance structures and maintains a centralised approach to cyber issues. The National Security Office oversees the country's cybersecurity governance, while strong incident management and response capability is held within the National Cyber Security Centre of the National Intelligence Service. The Korea Internet and Security Agency plays a prominent role in the promotion of cyber-centred innovation, releasing an annual Internet White Paper. Government policy is still informed by the 2011 National Cyber Security Masterplan, and South Korea's score for this indicator may increase with an upgrading of its current strategy.

SCORE: 8

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

South Korea has taken several steps this year to update its already comprehensive cyber legislation framework. The controversial new *Anti-Terrorism Act,* ostensibly designed to combat the online threat from North Korea, expands the surveillance powers of the National Intelligence Service and has sparked significant privacy concerns about the collection of public data. Ironically, the *Personal Information Protection Act* and the *Promotion of IT Network Use and Information Protection Act* have both been amended to enforce harsher punishments on corporations that breach the privacy rights of South Korean citizens. South Korea is highly regulated, particularly in relation to government control of online content. The Korean Communications Standards Committee monitors and removes inappropriate content, while the police enforce penalties for 'cyber defamation'. This sustained focus on cyber issues, the expansion of legislation and strong implementation have raised South Korea's score for this indicator.

SCORE: 9

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

South Korea has successfully diversified its international engagement, stepping into a greater leadership role and more mature cyber discussions. It has continued to deepen its bilateral and trilateral cooperation with key partners, including the US, Australia, China and Japan. Importantly, it has also founded two new multilateral forums: the Global Cybersecurity Centre for Development and the Cybersecurity Alliance for Mutual Progress. South Korea has improved its score in this area because these initiatives represent not only its growing Asia–Pacific leadership but also its broadened discussions on norms, internet governance and capacity building.

SCORE: 8

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

South Korea has maintained its sophisticated CERT capability during the year. KNCERT oversees the security of government networks, while KrCERT is the front-facing incident response unit for broader private-sector cybersecurity and is a member of APCERT. This year, KrCERT conducted public awareness campaigns and delivered international capacity-building in countries including Mongolia, Vietnam, Peru and Costa Rica. It has implemented a 'bug bounty' program to incentivise the reporting of network vulnerabilities and established a user notification system to alert individuals when they fall victim to malicious online exploits. Further developing its international cooperation and elevating its activities from CERT engagement to leadership would increase KrCERT's score.

SCORE: 8

2 CYBERCRIME

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

South Korea continues to address rising levels of cybercrime through the Cyber Bureau within the Korean National Police Agency (KNPA). The bureau possesses sophisticated response capability in its Cyber Safety Division, Cybercrime Response Division and Digital Forensics Centre. There's evidence that the KNPA strongly enforces South Korea's extensive suite of cyber legislation. Its annual International Symposium on Cybercrime Response in June 2016 gathered global law enforcement experts to share best practice, and was held in parallel with the INTERPOL Eurasian Working Group Meeting for Heads of Units. South Korea appears to have broadened its international capacity-building efforts. The export of 'K Cop' training to foreign law enforcement agencies has received a fivefold budget increase. The KNPA is also reportedly working with companies to combat the spread of malware.

SCORE: 8

3 MILITARY

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

South Korea's military service remains very cognisant of cyberspace policy and security in the light of the high-profile online threat posed by North Korea. This year alone, South Korea suffered hacking efforts against the country's train system, the phones of senior government officials, online banking systems, a naval shipbuilding firm and the Ministry of National Defense. Not only is cybersecurity clearly prioritised through the National Cyber Command, but it's also well coordinated across the services by the Defense Cyber Security Council, which comprises Cyber Command, Defense Security Command and the Joint Chiefs of Staff, and which met in March 2016. There have been significant efforts to boost the human capital behind South Korea's national cyber defences. Since 2009, Cyber Command has doubled in size and received an increase in funding of almost 50%. This year, President Park Geun Hye introduced a new initiative offering full university scholarships to talented young hackers in exchange for seven years of military service. The first student cohort of professional cyber officers also graduated from Korea University's Cyber National Defense Department in February 2015, after the department's establishment in 2012. The military has a significant and clearly defined role in cyberspace, but its focus remains narrowly on defending against the North Korean threat. Broadening its military narrative to a more comprehensive posture in cyberspace would indicate greater cyber maturity.

SCORE: 9

4 BUSINESS

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

There's a strong two-way dialogue between the government and private sector in South Korea. The Ministry of Science, ICT and Future Planning's Future Wealth Business Plan 2016 outlines an increased investment in the Internet of Things, big data and cloud computing development. South Korea supports the growth of the start-up community, providing funding to the most innovative initiatives through the K-Start Up Grand Challenge. The government also seeks input from industry by offering the most visited websites US$90,000 to develop more sophisticated technology standards that can then be used more widely. The opening of the new Microsoft Cybersecurity Centre by the Korea Internet and Security Agency President and the President of Microsoft Asia Pacific further exemplifies the high level of mature public–private partnership.

SCORE: 9

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

South Korea boasts one of the most flourishing digital economies, and the ICT sector produces almost 10% of GDP. President Park's vision of South Korea as a 'creative economy' and 'Asia's Silicon Valley' has provided strong top-down support for digital growth. Consistent infrastructure improvements have supported these developments, and the digital economy now forms an essential component of South Korean success. The start-up ecosystem will require ongoing support in order to compete with the entrenched *chaebols*, and more agile regulatory frameworks would facilitate even greater innovation.

SCORE: 9

5 SOCIAL

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

There's an active debate among the South Korean public about cyber issues across media, academic and social platforms, despite the attentive regulation of internet content by the Korean Communications Standards Committee. Freedom House categorises South Korea as 'partly free' based on concerns about the use of 'cyber defamation' charges to discourage anti-government sentiment and the resulting risk of self-censorship. The Korea Internet and Security Agency and KrCERT run campaigns to raise the public's already high awareness of cybersecurity issues. In fact, public exposure to technology is so high that the government has identified 'internet addiction' as a national health crisis and has established 'digital detox boot camps' in order to combat the problem among South Korean youth.

SCORE: 9

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 5

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 10

While only 40% of South Koreans have fixed-line internet access, there's prolific mobile phone connectivity—all at the fastest speeds in the world. Telecommunication infrastructure developments mean that South Korea will also attain another GHz of bandwidth by 2023 in order to support its growing Internet of Things.

THAILAND

Rank 2016: 9th

2015: 12th

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

OVERALL ASSESSMENT

Thailand's National Legislative Assembly is currently considering a set of legislation that would dramatically overhaul the country's legal, policy and organisational structures. Some of this reorganisation has already taken place with the creation of the new Ministry of Digital Economy and Society. While debate swirls around the more controversial elements of the new Bill, ThaiCERT and the Royal Thai Police remain active in the remediation and crimefighting spheres. The jewel in the crown of Thailand's cyber policy is its well-developed approach to supporting the growth of the digital economy, using a multipronged strategy that focuses on short-term infrastructure and supply issues in addition to longer term problems such as skills shortages and e-government service infrastructure.

WEIGHTED SCORE 52.7

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?

This year, Thailand's National Legislative Assembly approved the creation of the Ministry of Digital Economy and Society. The new ministry will subsume the responsibilities of existing ministries and agencies, including the Ministry of Information and Communication Technology, the Software Industry Promotion Agency and the Electronic Transactions Development Agency, which currently take on much of Thailand's current policy formation. The ministry will be officially established in September this year. The Ministry of Information and Communication Technology has proposed seven other pieces of legislation related to cyber and digital issues under the Thailand Digital Economy policy. These pieces of legislation have been approved by the cabinet and are now moving through the Legislative Assembly. One of them, the Cybersecurity Bill, would create two new organisational bodies: the National Cybersecurity Committee, which would act as a high-level control tower on cyber response and coordination issues, and the Office of the National Cybersecurity Committee, which would be the committee's implementation arm. These new bodies will work to create a new national cyber strategy.

SCORE: 6

b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?

The tranche of legislation included in the Thailand Digital Economy policy will expand the powers of the government to investigate and prosecute online crime. Concerns have been raised that the new legislation fails to differentiate between 'content' and 'computer crimes'. Under the new legislation, it appears that punishment for computer crimes will be dealt out by the executive branch via a ministerially appointed committee. The committee will have the power to hand down fines and a maximum two-year prison sentence. Existing legislation includes the vaguely worded *Computer Crimes Act 2007* and the *Electronic Transaction Act 2001*.

SCORE: 6

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

A significant amount Thailand's international engagement on cyber issues takes place within ASEAN-related forums. Thailand is also member of ITU-IMPACT, and Bangkok hosts the ITU's Asia–Pacific office. It's also engaging in bilateral discussions with international partners, including Israel, on how to best form its new cybersecurity strategy and on the creation of its new cyber frameworks and agencies. Thailand's score would improve with an increased participation in capacity building and discussions about international security issues tied to cyberspace.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

ThaiCERT is a non-profit government-supported organisation that will soon be administratively housed in the new Ministry for Digital Economy and Information Technology. As Thailand's national CERT, ThaiCERT is a point of contact for government, the private sector and civil society, as well as the incident coordination body for international cyber incidents originating in Thailand. It organises local training workshops and digital forensic training courses and participates in international drills, workshops and conferences.

SCORE: 5

2 CYBERCRIME

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

Technology Crime Suppression Division of the Royal Thai Police is responsible for implementing Thailand's cyber laws. The division is quite active in enforcing the *Computer Crimes Law*, which it uses to detain individuals for the infiltration of networks and distributed denial-of-service attacks and for social commentary that's disparaging of the military or other institutional bodies. The Thai police also have a hotline for reporting incidents and activities such as 'illegal and harmful content on the internet'.

SCORE: 5

3 MILITARY

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

Thailand's Defence Minister announced in late 2015 that the Royal Thai Armed Forces would be creating a cyberwarfare unit. The unit will comprise members from the three branches of the armed forces and the police force. Its creation was outlined as a priority implementation measure in the armed forces' 2015 five-year plan. Reports vary as to the capability in the unit, but at the very least it seems to possess the ability to block websites deemed offensive and to remediate defacements and distributed denial-of-service attacks fuelled by internal and international political tension.

SCORE: 5

4 BUSINESS

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

Thailand's government is taking strong steps to build its IT infrastructure, and a key slice of its dialogue with private-sector companies relates to achieving that goal. Older cyber policy frameworks make reference to establishing public–private partnerships, but detail as to how those connections should be made is lacking. The new cybersecurity legislation includes vaguely worded provisions compelling private-sector cooperation in the government's 'collection of information on cyber threats and other information concerning the maintenance of Cybersecurity'.

SCORE: 4

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

The Thai Government has developed several strategies to help enable the growth of the country's digital economy. They include the Thailand 4.0 Plan, which contains practical implementation measures such as the establishment of technology parks for small and medium-sized digital enterprises, and the National Broadband Policy, which aims to expand physical internet infrastructure to remote areas. The National Digital Economy Master Plan has a six-pillar plan for development that includes plans for the development of digital service infrastructure, a digital workforce and soft infrastructure in addition to hard infrastructure. The Digital Government Development Plan (2016–2018) aims to boost the provision of online government services. In 2016, the ICT Ministry also approved plans to boost Thailand's 'international internet gateway' to at least 4,000 Gbps to help promote the country's reputation as a digital hub.

SCORE: 6

5 SOCIAL

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

Public discussion of cyber issues has traditionally been tied to concerns about content control and online censorship. The proposed Cybersecurity Act has garnered significant local and international media attention, particularly from human rights organisations. Campaigns led by such groups have had some success in pressuring the government to wind back the more controversial proposals in its latest tranche of legislation. The short-lived 'single internet gateway' proposal also drew the attention of international media. Several small private think tanks are also beginning to provide more in-depth commentary on cyber issues. But beyond these pockets of knowledge, widespread public awareness of cyber issues is still in the development phase.

SCORE: 6

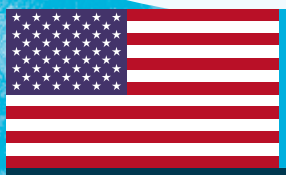
b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 2

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 8

Thailand's burgeoning middle class is driving increased internet penetration, as are government programs to expand digital infrastructure to rural and regional areas. Mobile internet penetration sits at a respectable 75% of the population, while fixed-line broadband services are used by 9%.



UNITED STATES OF AMERICA

Rank 2016: 1st

2015: 1st

—

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	10
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	10
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	9
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	9
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	10
b) What percentage of the population has fixed broadband internet connectivity?	4
c) What percentage of the population has mobile broadband internet connectivity?	10

OVERALL ASSESSMENT

The US has retained its leading position in the Asia–Pacific and globally in 2016. In the wake of several embarrassing breaches in 2015, the government has taken strong action to enhance national cybersecurity through a deeper partnership with the private sector. The US provides significant assistance to international partners to fight financial cybercrime, and its business sector incorporates titans of the digital economy that are changing the way the world uses cyberspace. In 2016, the US has for the first time publicly disclosed that its military is targeting an adversary through cyberspace, indicating significant confidence in its capabilities. However, US cyber legislation has been delayed for several years in Congress, and emerging issues such as encryption, which has caused tensions between the government and the private sector, continue without legislative action. Public attention on cyber issues has again been focussed by major incidents including the encryption debate and the hacking of the Democratic National Committee.

WEIGHTED SCORE 88.1

1 GOVERNANCE

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

The US Government has continued efforts to both refine its governance of cyber issues and more carefully clarify the roles and responsibilities of its agencies in cybersecurity incident responses for the public and private sectors. Major new initiatives in the past 12 months include the 30-day Cybersecurity Sprint, the *Cybersecurity Act of 2015*, the Cybersecurity National Action Plan, the Federal Cybersecurity Research and Development Strategic Plan, and Presidential Policy Directive 41 on cyber incident coordination. In totality, these initiatives are intended to make short- and long-term changes to strengthen the cybersecurity of the government, private sector and society. The White House has also requested significant additional funding of US$19 billion for the 2017 budget to support the implementation of new cyber initiatives. There's a strong focus on increasing and improving public–private cooperation on cybersecurity, along with new legislation and funding to support information sharing, education, R&D and digital economic growth. Notably, there's been a specific effort to provide better information to the public on how to report cybersecurity incidents and on the framework that guides the government's response. This is set out in Presidential Policy Directive 41, which details the principles governing US Government responses to cybersecurity incidents affecting public or private-sector entities and requires the departments of Justice and Homeland Security to maintain updated publicly accessible contact information to assist public- and private-sector agencies to report incidents to the proper authorities.

SCORE: 10

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

There's significant legislative activity in the US on cyber-related issues, notably about encryption and privacy, and close to 30 Bills are under consideration by both houses. However, these matters are making very slow progress, and many key issues continue to carry on without legislative guidance. The major legislative development in the past 12 months was the passage of the *Cybersecurity Act of 2015*. The Act is an amended version of the Cybersecurity Information Sharing Act, and there's been a four-year debate about information-sharing and data-breach requirements. It creates a voluntary cybersecurity information-sharing process to facilitate better exchanges of cybersecurity information and provides some legal protection from privacy and anti-trust violations for entities that share information with the government. However, these protections are more limited than those included in the original Cyber Intelligence Sharing and Protection Bill. The Act also includes initiatives and funding for new research, workforce training and scholarships. The debate about cyber-related issues in legislation indicates a good awareness of cyber matters among US legislators, but the significant delays in enacting the legislation mean that the US's score for this category hasn't increased.

SCORE: 8

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

The US continues to lead the global counter-narrative to the Chinese- and Russian-led conception of international cyber policy and governance, promoting an open, collaborative multistakeholder model of cyberspace. In the past year, the US has led agreements in major multilateral forums on norms and confidence-building measures in cyberspace, including the G20, ASEAN and the Organization for Security and Co-operation in Europe. It's also had some significant breakthroughs in bilateral discussions. A major achievement was the US–China bilateral agreement in September 2015 to improve cooperation on cybercrime, including through a new high-level dialogue, and an agreement that neither government would 'conduct or knowingly support cyber-enabled economic espionage for commercial gain'. The G20 issued a statement in November 2015 that also committed states to refrain from intellectual property theft through cyberspace and to respect the principles of freedom from interference in privacy. While US leadership on policy issues is strong, greater presence and visibility of US capacity-building efforts, particularly in the Asia–Pacific, is needed to increase its score for this category.

SCORE: 9

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

The Department of Homeland Security's National Cybersecurity and Communications Integration Center houses both US CERT and the Industrial Control System CERT (ICS-CERT). There's also a strong private-sector CERT community in the US, including 72 US members of FIRST. US CERT provides a range of information to the public and private sectors to manage cyber threats, including vulnerability bulletins, alerts and cybersecurity tips, which collectively make up the National Cyber Awareness System. ICS-CERT provides similar information specifically tailored to operators of critical infrastructure control systems and has also assisted in investigating the hacking of parts of the Ukrainian power grid. The US has a well-developed CERT community with strong response capabilities, but could improve its score for this category with further evidence of international engagement and capacity building in the CERT sector.

SCORE: 8

2 CYBERCRIME

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

The US retains its role as an international leader in the pursuit and prosecution of financial cybercriminals. The FBI's Cyber Division has specially trained agents and analysts in its 56 field offices to investigate cybercrime, new cyber action teams that work with international partners to collect intelligence, and 93 computer crimes taskforces across the US. The FBI has also worked to engage the private sector through the National Cyber Forensics and Training Alliance and its iGuardian cyber intrusion reporting portal. Statistics from the FBI's Internet Crime Complaint Center show that in 2015 there was US$1 billion in losses from reported cybercrime, at an average of US$8,421 per incident where a loss was reported. The US Secret Service and US Immigration and Customs Enforcement Cyber Crimes Center also investigate cybercrime in the US. The US supplies extensive expertise and capability to its overseas partners and has continued to support the investigation and prosecution of cybercrime in the region.

SCORE: 10

3 MILITARY

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

In 2016, the US has taken further steps to enhance the capability of its armed forces to defend themselves and the country from cyber threats and engage its adversaries though cyberspace. It has had difficulty in recruiting the 6,200 troops for 133 new cyber teams within Cyber Command, but has discussed publicly for the first time the employment of offensive cyber capability against Islamic State. It isn't possible at this time to assess the effectiveness of those operations, but media reporting has indicated that they haven't yet met the expectations of senior military and political leaders. In 2016, the US also outlined its policy on cyber deterrence, which notes that it will use all instruments of national power to deter cyberattacks and other malicious acts in cyberspace that threaten the US and its interests, including its military command and control systems. The US is the most forward-leaning nation in discussing the development and employment of its military cyber capabilities, indicating a significant level of confidence in its capability and the frameworks that guide and govern its use. The Department of Defense has requested funding of US$6.2 billion in the 2017 budget and US$34.6 billion for projects requiring funding over the period from 2017 to 2021, but details of how the money will be spent are scarce.

SCORE: 10

4 BUSINESS

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

The US Government has a clear focus on improving the quality of its engagement with the private sector on cyber issues. While there's been some tension between the government and major technology firms about encryption in the past year, the relationship is generally cooperative. New policy and legislative initiatives, including the Cyber Security National Action Plan, the Cybersecurity Act, Presidential Policy Directive 41 and measures to strengthen cooperation, clearly delineate responsibilities and enable better information sharing between the government and the private sector. The Commission on Enhancing National Cybersecurity, an element of the Cyber Security National Action Plan, has been assembled from key private-sector leaders to recommend actions by both government and the private sector to improve national cybersecurity by December 2016. The government has also provided funding to facilitate cybersecurity training for small and medium-sized enterprises throughout the country. There's clear intent from both the public and the private sector to engage constructively to address cybersecurity issues in the US.

SCORE: 9

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

The US digital economy stands out globally for the breadth and influence of its digital products and services. Major US technology firms have led the way in the development of new products that have a significant influence on the global digital economy, including social media, transportation, commerce and entertainment. The World Economic Forum notes that the US is an extremely favourable environment for business and innovation. This is supported by affordable access to broadband internet and high levels of connectivity. The US Government has also sought to assist start-ups with funding for impact investing and seed finance through the Startup America initiative. Pew Research Center surveys have found that about 72% of adults in the US have used at least one of 11 different online services surveyed, 50% of which were to purchase used or second-hand goods online. However, the surveys also indicated that there's a deep divide between those who are engaged with the digital economy and those who aren't: a significant percentage (28%) had never used any major shared or on-demand online services. Tellingly, while 15% of Americans had used ride-sharing apps such as Uber, 30% didn't know what they were. The full economic potential of digital growth has been estimated to be worth about US$421 billion in 2020, but further work to fully engage the population in the digital economy is necessary to achieve that potential.

SCORE: 9

5 SOCIAL

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

Awareness of and debate about cyber matters in the US has continued to cover a broad range of issues in international and domestic cyber policy and security. There are strong academic and think tank communities that are highly active in researching and commenting on cyber issues. Cyber security has been an issue in the presidential election, particularly the theft and release of Democratic National Committee information. The dispute between the FBI and Apple about the decryption of an iPhone that belonged to San Bernadino gunman Syed Farook has focused significant public and media attention on encryption technology and its implications for security and privacy. Privacy was also an issue of public and media concern in the debate about the *Cybersecurity Act of 2015* and the preceding Cybersecurity Information Sharing Bill. International issues such as internet governance are also an area of significant engagement by the policy research community.

SCORE: 10

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 4

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 10

The ITU notes that 31/100 Americans have a fixed-line broadband connection. The price of broadband subscriptions in the US is low by world standards, starting from US$16 per month compared to a global average of US$52. Rural, poor, indigenous and non-white communities are disproportionately affected by a lack of access to broadband and, where there is connectivity, about 100 million Americans haven't connected. Presidential candidate Hillary Clinton has proposed a program to increase the reach of broadband internet through a US$25 billion infrastructure bank to encourage private investment. The growth of mobile connectivity has had significant effects on how Americans engage socially and commercially in cyberspace. US mobile broadband connectivity rates of 109/100 are similar to rates in other major advanced economies, such as South Korea, Australia and Japan. Smartphone ownership has increased from 35% in 2011 to 68% in 2015 according to the Pew Research Center, and that growth looks likely to continue.

VIETNAM

Rank 2016: 11th
2015: 9th

Indicator	Score
1 – GOVERNANCE	
a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?	6
b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?	7
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	5
d) Is there a publicly accessible cybersecurity assistance service e.g. a Computer Emergency Response Team (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, policy, and security?	3
4 – BUSINESS	
a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?	4
b) Is the digital economy a significant part of economic activity? (How has the country engaged in the digital economy?)	6
5 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has fixed broadband internet connectivity?	1
c) What percentage of the population has mobile broadband internet connectivity?	4

OVERALL ASSESSMENT

For Vietnam, the big movement this year was the passage though the National Assembly of the *Law on Cyber Information Security*. It will be interesting to see whether the new law works as intended to consolidate the proliferation of existing IT security-related laws into a single law. Many will also be watching closely to see how the law is practically implemented and whether concerns raised by national and international privacy and human rights experts relating to data protection and freedom of speech eventuate or were overcritical. On most other areas of cyber maturity, Vietnam has kept an even keel, continuing its CERT engagement, cybercrime fighting efforts and ASEAN-based international activities. Mobile data plans continue to drive internet penetration, which will continue to grow with the rollout of new infrastructure to regional areas. The establishment of the ASEAN Economic Community is also likely to increase thinking about how the country can harness the opportunities presented by cyberspace.

WEIGHTED SCORE 48.1

1 GOVERNANCE

a) What, if any, are the government's organisational structures for cyber matters (incl. policy, security, critical infrastructure protection, CERT, crime, and consumer protection)? How effectively have they been implemented?

Cyber matters in Vietnam are largely handled by Ministry of Information and Communications via its agencies and departments, including the Authority of Information Security, the Department of Information Technology, VNCERT, the National Electronic Authentication Centre and the IT Application Authority. Created in 2004, the Authority of Information Security carries out much of the heavy lifting involved in governance, policy and legislative formation and whole-of-government coordination for cyber issues. The authority also has organisational responsibility for international coordination, although much of that engagement still seems to be carried out by the Ministry of Foreign Affairs. Under the umbrella of the National Strategy on Transforming Vietnam into an Advanced ICT Country, the government has run courses on capacity building and IT take-up among the public and government agencies and launched several strategies to lift ICT skills.

SCORE: 6

b) Is there existing legislation/regulation relating to cyber issues or ISPs? Is it being used? What level of content control does the state conduct or support?

In November 2015, Vietnam's National Assembly passed the *Law on Cyber Information Security*, which came into force in July 2016. The new law seeks to consolidate the proliferation of existing IT security-related laws into a single law. It includes provisions for the protection of the safety of personal information, systems, infrastructure and data and for the prevention of the use of information for 'terrorism'. The law requires the express consent of the owners of personal information online before it can be 'processed', which includes collection and transferral.

Existing legislation includes the 2005 *Law on E-Transactions*, the 2006 *Law on Information Technology,* the 2001 Management and Use of Internet Services Decree, the 2009 *Telecommunication Law*, the *Criminal Law* (2009 amendment), and the *Law on Protection of Consumers' Rights*.

SCORE: 7

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

Vietnam participates in ASEAN-based discussions on cybersecurity and cybercrime and in dialogues among ASEAN and other nations, such as China and Japan. Bilaterally, Vietnam is also working to weave cyber issues into higher level political discussions; examples have included Minister of Public Security Tran Dai Quang's recent meeting with US Secretary of Homeland Security Jeh Johnson, which touched on cybersecurity collaboration. Vietnam is a member of ITU-IMPACT and INTERPOL. Its score would improve with a more active contribution to international cyber policy and conflict prevention discussions through apparatus such as the ASEAN Regional Forum.

SCORE: 5

d) Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Vietnam's national CERT was established in 2005 as VNCERT. It's administratively housed within the Ministry of Information and Communications. VNCERT is active in incident response and online security awareness-raising in Vietnam. It works closely with private-sector and international partners in combating botnets and phishing sites located in Vietnam. It works domestically to test websites and increase the visibility of cybersecurity risks within government agencies. VNCERT is a member of APCERT and regularly participates in international drills and conferences. In 2015, it hosted incident-response training courses for LaoCERT.

SCORE: 6

2 CYBERCRIME

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

The Police Department for High-tech Crime Prevention (C50) is located in the General Department of the Vietnam Police within the Ministry of Public Security. The department is split into several divisions that address different areas, including data recovery and evidence collection; cybercrime; traditional crimes that use cyberspace as an enabler; liaison offices; and coordinating arms. The division is relatively active in its enforcement of online criminal law and in international information-sharing and collaboration. Much of its engagement recently seems to be strongly connected to cracking down on illegal gambling rings.

SCORE: 6

3 MILITARY

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

Vietnam's 2004 Defence White Paper mentioned that the Vietnamese People's Army Technology General Department would build ICT capabilities through research, development and the application of new technologies. Cyber issues were largely absent from Vietnam's 2009 Defence White Paper, but cyber capability is expected to again feature in the 2016–17 White Paper in the wake of increased online skirmishes tied to the East Vietnam Sea / South China Sea dispute. In November 2015, the Vietnamese People's Army hosted members of South Korea's Defence Security Command, and cybersecurity training was delivered by South Korean experts. Cooperation on cyber issues is set to continue into 2016. Beyond moves from the Ministry of Public Security to establish a high command for cybersecurity and information security in 2011, there's been little movement to indicate higher level organisational structures or thinking for cyber issues. This may be because the Information Security Department established in 2015 at the Ministry of Information and Communications may be carrying out much of this responsibility.

SCORE: 3

4 BUSINESS

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

The Vietnamese Government continues to have well-established connections with large multinational companies on information security issues, albeit somewhat incidentally, as those conversations appear to concern the establishment of training centres or more general attempts to achieve foreign direct investment. VNCERT drives most private-sector engagement on end-user education and remediation efforts, but the level of substantive two-way dialogue on cyber issues beyond that is assumed to be minimal. There's been an increasing trend in which ministries partner with business in delivering conferences on cybersecurity, which is a positive move that could help build more established connections and discussions in the future.

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 is continuing to implement its Masterplan on Information Technology, which outlines targets for making Vietnam an 'advanced ICT country' by 2020. IT companies operating in Vietnam have been granted tax exemptions and streamlined administration policies under the policy. Rapid mobile internet take-up in major cities continues to bolster digital economic activity, and the restructuring of state-owned telecommunications companies could lead to improved delivery and expanded broadband internet coverage in rural areas.

SCORE: 6

5 SOCIAL

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

The Vietnam Information Security Association continues to be a linchpin in driving awareness of cyber issues and delivering initiatives in partnership with government and the private sector, including by hosting the annual Vietnam Information Security Day. In 2016, RMIT University in Ho Chi Minh City opened a new cybersecurity lab to train business students in ICT security, and the university has also run workshops on cybersecurity for the business community. Cyber issues continue to feature in the media, which has paid increased attention to them after several high-profile disruption and infiltration efforts tied to broader maritime disputes.

SCORE: 4

b) What percentage of the population has fixed broadband internet connectivity?

SCORE: 1

c) What percentage of the population has mobile broadband internet connectivity?

SCORE: 4

According to the ITU, 38% of Vietnamese are able to access the internet over a mobile connection. Only 8% have a fixed-line broadband connection. This number is well below the Asia–Pacific average and is tied to poor rural infrastructure rollout. In the near term, Vietnam will continue to bolster internet availability via mobile data plans and the expansion of mobile infrastructure into rural and regional areas.

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 the development of suitable legal frameworks. 3 = A few laws exist, but without adequate implementation measures. 4 = A few laws exist; some implementation measures undertaken. 5 = A legal framework exists, with moderate implementation; some regulation in specific areas. 6 = A legal framework exists, with moderate implementation; some regulation in critical areas. 7 = A strong legal framework exists; implementation is incomplete or stalled. 8 = A strong legal framework exists and is partially implemented. 9 = A strong legal framework exists and is effectively implemented. 10 = A comprehensive legal framework is strongly implemented.
1c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	0 = No international engagement. 1 = Some intent to engage internationally, as yet unrealised. 2 = Some passive international engagement. 3 = Minimal international engagement; technically focused. 4 = Minimal international engagement; aid-based or basic technical/policing. 5 = Some bilateral and multilateral engagement in technical/policing. 6 = Strong bilateral engagement and some multilateral engagement in technical, policing and policy. 7 = Strong bilateral and multilateral engagement in technical/policing and policy engagement. 8 = Very strong bilateral and multilateral engagement in technical/policing and policy engagement. 9 = Multilayered international engagement; bilateral and multilateral engagement, technical/policing and policy engagement, with leadership roles. 10 = A prominent leader in multilayered international engagement; bilateral and multilateral engagement, technical/policing and policy engagement.

Key indicators	Scoring breakdown
1d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0 = No. 1 = No; plans exist for establishment. 2 = Yes, but response capability is developing. 3 = Limited response capability; emerging international engagement. 4 = Uneven response capability; some international engagement. 5 = Structured and planned response capability; minimal international engagement. 6 = Structured and planned response capability; limited international engagement. 7 = Well-structured and planned response capability; some international engagement. 8 = Well-structured and planned response capability; strong international engagement. 9 = Strong response capability; strong international leadership. 10 = Very strong response capability; key international leader.
2a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?	0 = No. 1 = No; plans exist for establishment or some personnel are in training. 2 = Yes, but response capability is developing. 3 = Limited response capability; emerging international engagement. 4 = Uneven response capability; some international engagement. 5 = Structured and planned response capability; minimal international engagement. 6 = Structured and planned response capability; limited international engagement. 7 = Well-structured and planned response capability; some international engagement. 8 = Well-structured and planned response capability; strong international engagement. 9 = Strong response capability; strong international leadership. 10 = Very strong response capability; key international leader.
3a) What is the military's role in cyberspace, 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.

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

Key indicators	Scoring breakdown
5b) What percentage of the population has fixed broadband 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+%
5c) What percentage of the population has mobile broadband 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:
2016 OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

		1a	1b	1c	1d	2	3	4a	4b	5a	5b	5c	Total	Weighted score
Weighting		**8.0**	**7.8**	**7.0**	**8.0**	**7.8**	**6.8**	**7.8**	**7.7**	**6.0**	**7.0**	**7.0**		
Australia	Scores	8	8	9	8	9	8	8	9	9	3	10	89	
	Weighted scores	6.4	6.3	6.3	6.4	7.1	5.5	6.3	6.9	5.4	2.1	7	65.6	**80.9**
Bangladesh	Scores	4	3	2	2	3	1	4	4	5	1	2	31	
	Weighted scores	3.2	2.4	1.4	1.6	2.4	0.7	3.1	3.1	3	0.7	1.4	22.9	**28.3**
Brunei	Scores	6	6	4	6	5	4	5	5	3	1	1	46	
	Weighted scores	4.8	4.7	2.8	4.8	3.9	2.7	3.9	3.8	1.8	0.7	0.7	34.7	**42.8**
Cambodia	Scores	4	4	3	3	2	1	3	3	4	1	5	33	
	Weighted scores	3.2	3.1	2.1	2.4	1.6	0.7	2.4	2.3	2.4	0.7	3.5	24.3	**30.0**
China	Scores	9	7	9	6	6	8	5	6	5	2	6	69	
	Weighted scores	7.2	5.5	6.3	4.8	4.7	5.5	3.9	4.6	3	1.4	4.2	51.1	**63.0**
Fiji	Scores	2	4	3	0	4	1	2	3	3	1	5	28	
	Weighted scores	1.6	3.1	2.1	0	3.1	0.7	1.6	2.3	1.8	0.7	3.5	20.5	**25.3**
India	Scores	7	5	7	5	4	3	5	7	7	1	2	53	
	Weighted scores	5.6	3.9	4.9	4	3.1	2.1	3.9	5.4	4.2	0.7	1.4	39.2	**48.4**
Indonesia	Scores	5	5	5	6	4	6	5	5	5	1	5	52	
	Weighted scores	4	3.9	3.5	4.8	3.1	4.1	3.9	3.8	3	0.7	3.5	38.4	**47.4**
Japan	Scores	9	8	9	10	8	7	8	9	9	4	10	91	
	Weighted scores	7.2	6.3	6.3	8	6.3	4.8	6.3	6.9	5.4	2.8	7	67.2	**82.9**
Laos	Scores	4	3	2	3	1	1	2	2	2	1	2	23	
	Weighted scores	3.2	2.4	1.4	2.4	0.8	0.7	1.6	1.5	1.2	0.7	1.4	17.2	**21.3**
Malaysia	Scores	7	7	8	8	6	6	7	8	6	1	10	74	
	Weighted scores	5.6	5.5	5.6	6.4	4.7	4.1	5.5	6.1	3.6	0.7	7	54.8	**67.7**
Myanmar	Scores	3	4	4	3	2	5	1	2	2	1	4	31	
	Weighted scores	2.4	3.1	2.8	2.4	1.6	3.4	0.8	1.5	1.2	0.7	2.8	22.7	**28.0**

		1a	1b	1c	1d	2	3	4a	4b	5a	5b	5c	Total	Weighted score
Weighting		**8.0**	**7.8**	**7.0**	**8.0**	**7.8**	**6.8**	**7.8**	**7.7**	**6.0**	**7.0**	**7.0**		
New Zealand	Scores	8	8	6	7	7	6	8	9	9	4	10	82	
	Weighted scores	6.4	6.3	4.2	5.6	5.5	4.1	6.3	6.9	5.4	2.8	7	60.4	**74.6**
North Korea	Scores	3	1	3	0	0	8	0	1	1	1	1	19	
	Weighted scores	2.4	0.8	2.1	0	0	5.5	0	0.8	0.6	0.7	0.7	13.5	**16.7**
Pakistan	Scores	3	3	2	1	4	4	4	3	2	1	2	29	
	Weighted scores	2.4	2.4	1.4	0.8	3.1	2.7	3.1	2.3	1.2	0.7	1.4	21.6	**26.6**
Papua New Guinea	Scores	4	3	2	0	1	1	2	1	5	1	1	21	
	Weighted scores	3.2	2.4	1.4	0	0.8	0.7	1.6	0.8	3	0.7	0.7	15.2	**18.7**
Philippines	Scores	5	6	5	0	6	3	4	5	6	1	5	46	
	Weighted scores	4	4.7	3.5	0	4.7	2.1	3.1	3.8	3.6	0.7	3.5	33.7	**41.6**
Singapore	Scores	9	8	7	7	8	8	10	9	9	3	10	88	
	Weighted scores	7.2	6.3	4.9	5.6	6.3	5.5	7.8	6.9	5.4	2.1	7	64.9	**80.2**
Solomon Islands	Scores	3	0	2	0	1	0	2	1	1	1	2	13	
	Weighted scores	2.4	0	1.4	0	0.8	0	1.6	0.8	0.6	0.7	1.4	9.6	**11.9**
South Korea	Scores	8	9	8	8	8	9	9	9	9	5	10	92	
	Weighted scores	6.4	7.1	5.6	6.4	6.3	6.2	7.1	6.9	5.4	3.5	7	67.7	**83.6**
Thailand	Scores	6	6	5	5	5	5	4	6	6	2	8	58	
	Weighted scores	4.8	4.7	3.5	4	3.9	3.4	3.1	4.6	3.6	1.4	5.6	42.7	**52.7**
United States	Scores	10	8	9	8	10	10	9	9	10	4	10	97	
	Weighted scores	8	6.3	6.3	6.4	7.8	6.8	7.1	6.9	6	2.8	7	71.4	**88.1**
Vietnam	Scores	6	7	5	6	6	3	4	6	4	1	4	52	
	Weighted scores	4.8	5.5	3.5	4.8	4.7	2.1	3.1	4.6	2.4	0.7	2.8	39	**48.1**

APPENDIX 3:
2015 OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

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

		1a	1b	1c	1d	2a	3a	4a	4b	5a	5b	Total weighted scores
Weighting		**8**	**7.8**	**7**	**8**	**7.8**	**6.8**	**7.8**	**7.7**	**6**	**7**	
Myanmar	Scores	3	4	4	3	2	5	1	2	2	1	
	Weighted scores	2.4	3.1	2.8	2.4	1.6	3.4	0.8	1.5	1.2	0.7	**26.9**
New Zealand	Scores	8	8	6	7	7	5	6	8	9	9	
	Weighted scores	6.4	6.3	4.2	5.6	5.5	3.4	4.7	6.1	5.4	6.3	**72.8**
North Korea	Scores	3	1	2	0	0	8	0	1	1	1	
	Weighted scores	2.4	0.8	1.4	0	0	5.5	0	0.8	0.6	0.7	**16.4**
PNG	Scores	3	3	3	0	1	2	2	1	5	1	
	Weighted scores	2.4	2.4	2.1	0	0.8	1.4	1.6	0.8	3	0.7	**20.3**
Philippines	Scores	5	5	5	3	5	3	4	6	6	5	
	Weighted scores	4	3.9	3.5	2.4	3.9	2.1	3.1	4.6	3.6	3.5	**46.8**
Singapore	Scores	9	8	7	7	7	8	9	9	9	9	
	Weighted scores	7.2	6.3	4.9	5.6	5.5	5.5	7.1	6.9	5.4	6.3	**81.8**
South Korea	Scores	8	8	7	8	7	9	9	9	9	9	
	Weighted scores	6.4	6.3	4.9	6.4	5.5	6.2	7.1	6.9	5.4	6.3	**82.8**
Thailand	Scores	6	6	5	5	4	5	3	6	5	4	
	Weighted scores	4.8	4.7	3.5	4	3.1	3.4	2.4	4.6	3	2.8	**49.1**
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 4:
2014 OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

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 3.

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

APPENDIX 5:
KEY INDICATORS

Country	*Freedom on the net* report[a]	ITU statistics 2016[b]			FIRST membership[c]	World Economic Forum *2016 Global information technology report*: Knowledge-intensive jobs, % workforce (rank)[d]	APCERT operational member teams[e]
		Fixed broadband subscriptions/100 inhabitants	Active mobile-broadband subscriptions/100 inhabitants	Bandwidth (Mbit/s)			
Australia	Free	27.85	112.86	1,650,000	6	44.9 (13)	CERT Australia, AusCERT,
Bangladesh	Partly free	2.41	13.45	142,787	1	20.0 (71)	bdCERT
Brunei	n.a.	7.99	4.48	19,250	1	n.a.	BruCERT
Cambodia	Partly free	0.53	42.80	52,997	0	4.1 (104)	n.a.
China	Not free	18.56	56.03	4,603,904	4	n.a.	CCERT, CNCERT / CC
Fiji	n.a.	1.43	48.17	11,332	0	n.a.	n.a.
India	Partly free	1.34	9.36	1,908,736	1	n.a.	CERT-In
Indonesia	Partly free	1.09	42.05	370,000	1	8.9 (98)	ID-CERT, ID-SIRTII/CC
Japan	Free	30.49	126.44	7,411,391	27	24.4 (58)	JPCERT/CC
Laos	n.a.	0.52	14.16	21,457	0	n.a.	LaoCERT
Malaysia	Partly free	8.95	89.94	743,187	1	25.2 (53)	MyCERT
Myanmar	Partly free	0.35	29.54	43,404	0	n.a.	mmCERT
New Zealand	Free	31.55	114.22	440,000	2	42.9 (18)	New Zealand National Cyber Security Centre
North Korea	n.a.	n.a.	n.a.	n.a.	0	n.a.	n.a.
Pakistan	Not free	0.95	13.02	403,253	0	19.5 (73)	n.a.
Papua New Guinea	n.a.	0.20	6.07	5,500	0	n.a.	n.a.
Philippines	Free	3.40	41.58	1,550,000	0	23.5 (61)	n.a.
Singapore	Partly free	26.45	142.20	3,400,000	10	52.7 (2)	SingCERT
Solomon Islands	n.a.	0.24	11.41	250	0	n.a.	n.a.
South Korea	Partly free	40.25	109.67	2,091,476	8	21.4 (70)	KrCERT/CC
Thailand	Not free	9.24	75.28	1,720,000	1	13.8 (90)	ThaiCERT
United States	Free	31.53	109.23	24,000,000	72	38.0 (26)	n.a.
Vietnam	Not free	8.14	38.98	1,200,000	0	10.3 (95)	VNCERT

n.a. = not available.
a https://freedomhouse.org/report-types/freedom-net#.VdWySJfNx8E
b www.itu.int/pub/D-IND-WTID.OL-2016
c www.first.org/members/map
d www.weforum.org/reports/the-global-information-technology-report-2016/
e www.apcert.org/about/structure/members.html

ACRONYMS AND ABBREVIATIONS

ADF	Australian Defence Force
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia–Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
AusCERT	Australia CERT
B2C	business-to-customer
CamCERT	Cambodia CERT
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
CSA	Cyber Security Agency (Singapore)
CSIRT	computer security incident response team
FBI	Federal Bureau of Investigation (US)
FIRST	Forum of Incident Response and Security Teams
GCSIRT	Government Computer Security Incident Response Team (Philippines)
GDP	gross domestic product
ICPC	International Cyber Policy Centre (ASPI)
ICS-CERT	Industrial Control System CERT (US)
ICT	information and communications technology
ID-CERT	Indonesia CERT
ID-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center
IMPACT	International Multilateral Partnership Against Cyber Threats
INP	Indonesian National Police
IoT	Internet of Things
ISP	internet service provider
IT	information technology
ITE Law	*Electronic Information and Transactions Act 2008* (Indonesia)
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
KNPA	Korean National Police Agency (South Korea)
KrCERT/CC	Korea Internet Security Center (South Korea)
mmCERT	Myanmar CERT
MoU	memorandum of understanding
MyCERT	Malaysia CERT
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Center (South Korea)
NCSC	
NISC	National Information Security Center (Japan)
NR3C	National Response Centre for Cyber Crime (Pakistan)
OIC-CERT	Organisation of Islamic Cooperation CERT
PacCERT	Pacific CERT
PH-CERT	Philippines CERT
PLA	People's Liberation Army
PNG	Papua New Guinea
RGB	Reconnaissance General Bureau (North Korea)
RSIPF	Royal Solomon Islands Police Force
SingCERT	Singapore CERT
TCSI	Telecommunications Commission of Solomon Islands
ThaiCERT	Thailand CERT
TSUBAME	Internet Traffic Monitoring Data Visualisation Project
UK	United Kingdom
UN	United Nations
UNESCAP	UN Economic and Social Commission for Asia and the Pacific
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

AUTHORS

DR TOBIAS FEAKIN

Tobias Feakin joined ASPI in October 2012. He is Director of National Security Programs, coordinating all of the institute's work in this space. He examines issues relating to national security policy, cybersecurity, global counterterrorism, resilience and critical infrastructure protection. He established the International Cyber Policy Centre at ASPI in 2013 and is Head of the Centre. In this role, he researches how cyberspace is used for nefarious purposes by state and non-state actors, creating collaborative policy responses and national and international cooperation in cyberspace. His latest research examines Asia–Pacific cyber maturity and state responses to cyber incidents.

In 2014, Tobias was appointed by the Australian Prime Minister to be part of the Independent Panel of Experts to the Australian Cyber Security Review. He is an Oxford Martin Associate of the Devising Cyber Policy and Cyber Defence working group at the Oxford University Global Cyber Security Capacity Centre, and a research adviser for the Global Commission on Internet Governance run by Chatham House. He has previously acted as an expert adviser to Professor John Beddington, ex-UK Government Chief Scientific Adviser. He has also acted as a member of the Energy Security in a Multi-polar World Steering Committee, University of Exeter; and the Resilient Futures Project Steering Committee, Kings College London.

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, she 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 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. Before joining ASPI, Liam worked at the Department of Defence on strategic and international defence policy. 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.

ZOE HAWKINS

Zoe Hawkins joined ASPI in August 2015. She is currently working in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber policy. She is also working as a research assistant on the policy implications of quantum technology for the Centre for International Security Studies at the University of Sydney. Zoe previously interned with the Australian Institute of International Affairs NSW and holds a Bachelor of International and Global Studies, majoring in International Relations, from the University of Sydney. She has a special interest in cybersecurity, drone technology and the future of warfare.