CYBER MATURITY IN THE ASIA–PACIFIC REGION 2014

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

CREATING A REGIONAL CYBER MATURITY METRIC

ACKNOWLEDGEMENTS

The authors would like to thank a number of colleagues who generously contributed their time and comments to this report. Mr Peter Jennings was integral to the initial design of this project and his ongoing input, insights and guidance were invaluable. Without the help of Dr Andrew Davies, this report would not have been possible. His efforts on the mathematical elements of the country ranking system were indispensable. Thanks are also extended to Dr Ben Schreer, who provided helpful and honest comments during the final editing stages. To all of our expert panel members who participated in our methodology workshops and contributed to the category weighting process, we thank you and express regret if we could not capture all of your thoughts in our reporting.

Finally a special thanks should be reserved for Liam who contributed a significant amount of knowledge and expertise to the report. We greatly valued your insight, impartial recommendations and good humour throughout the writing process.

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. We are 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 (ICPC)

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

The Centre 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 would like to thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various funders, but special mention should go to IBM and the Commonwealth Bank who have been such strong advocates and supporters of our work.

First published April 2014

Published in Australia by the Australian Strategic Policy Institute

ASPI

Level 2,
40 Macquarie Street
Barton ACT 2600
Australia

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

CONTENTS

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

INTRODUCTION

In recent years, the Asia–Pacific region has undergone tremendous economic growth, political transformation and social change. The development of cyberspace and the information and communications technology (ICT) that powers it has proven to be an integral part of the region's socioeconomic growth. The online environment is also rapidly growing in importance as an avenue for political and social expression in Asian societies.

But technological development in the region varies dramatically. It's home to some of the world's least networked countries, such as Myanmar (1.1% internet penetration) and Cambodia (4.9%) plus some of the most networked, including South Korea (84.1%) and Japan (79.1%). It also encompasses burgeoning ICT markets such as China and India.

Although increasing connectivity has generated undeniable benefits, it has also created new vulnerabilities for governments and the private sector in the areas of national security and online crime. These tensions have manifested differently according to each state's domestic context.

As connectivity grows, so does the need for cyber-focused policies, legislation and regulatory frameworks. Governments in increasing numbers are starting to address shortfalls in their domestic arrangements, but there are many states that lag behind in either the formation or implementation of cybercentric mechanisms, frameworks and policy.

GAUGING NATIONAL CYBER MATURITY

Sitting above state-based cyber issues is a continually evolving international strategic landscape. The Asia–Pacific region is an increasing focus for major and middle powers. In an environment such as cyberspace where gains are high, the probability of capture is low and deniability rules, many different economic and political confrontations are playing out simultaneously. A by-product of this tension has been a rise in the number of countries that have acquired or are seeking offensive cyber capabilities.

To make considered, evidence-based cyber policy judgements in this regional context, there's a need for better tools and information to assess the 'cyber maturity' of nations in the region. The methodology proposed in this report uses a 'cyber maturity metric' to assess the various facets of nations' cyber capabilities.

This report analyses the 'cyber maturity' of 14 countries across the Asia–Pacific region, which represent a wide geographical and economic cross-section of the region. Australia's closest allies, the United States and the United Kingdom, have been included to provide an additional benchmark for overall national cyber maturity. 'Maturity' in this context is exhibited 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, 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 and as such this report's conclusions are based solely on open-source material.

Using the data from the metric we have also developed a separate 'cyber engagement scale' for government and industry. The scale aims to be a reference tool for use in identifying opportunities for the sharing of best practice, capacity building, development and business opportunities. With this additional layer of analysis, governments and the private sector should be able to tailor engagement strategies to best fit existing levels of maturity in each policy area in each country.

The report is the inaugural edition of what will be an annual report examining cyber maturity trends across the Asia–Pacific region. In future iterations, this report will seek to assess the maturity of an expanded range of countries and deepen the dialogue surrounding the best means to achieve this assessment.

2013–14 MATURITY TRENDS

Cyber awareness among governments, businesses and wider societies gained significant momentum throughout 2013–14. While the Asia–Pacific is home to countries along the full spectrum of cyber maturity, it's clear that each country surveyed is increasingly cognisant of cyberspace as a critical area. India, Japan and Singapore have all updated or launched new national cybersecurity policies, Papua New Guinea and Cambodia are developing new cybercrime laws, and Australia has announced the creation of the Australian Cyber Security Centre (ACSC), all of which are positive steps for the region.

Despite this increased awareness, capacity and implementation are likely to remain major hurdles for many countries in the region. For nations such as Myanmar, Papua New Guinea and Cambodia, lack of infrastructure severely impedes growth in cyber maturity. The urban–rural internet penetration gap in those countries, which can also be seen across the region to varying extents, continues to be an obstacle to full cyber maturity. Lack of resources or weak supporting legislation restrict efforts to strengthen cyber resilience in the Philippines, Malaysia, Indonesia, Cambodia and Thailand. In India, a lack of enforcement capacity hinders an otherwise fairly well-developed policy framework.

Comparatively mature cyber actors also face major challenges. China possesses strong cyber surveillance and technical capabilities but lacks solid cybercrime and cybersecurity policy, legislation and coordination. Domestic content control remains unremitting in China and is also an issue in Thailand and highly cyber mature Singapore. South Korea, one of the most wired countries in the world, faces serious external cyber threats across the border, leading to a focus on the defensive dimensions of cyberspace, while Japan's renewed efforts in cyber remain marred by issues with internal government cooperation. Australia's own cyber policy developments have largely stagnated since the announcement of ACSC in 2013.

However, increased awareness, often driven by international engagement, is leading to positive cyber outcomes. For example, Japan's increasing engagement with the US is helping to shape its cyber capabilities, and its efforts to help regional partners develop their own cyber capacities offer a strong model for regional engagement. Robust existing regional policing and cooperation between national computer emergency response teams (CERTs) lay the foundation for higher level cyber policy engagement, particularly at the multilateral level. With the ASEAN Regional Forum expanding their efforts in 2014, the Asia–Pacific has every potential to see improved dialogue across both technical and policy realms and increasing levels of cyber maturity across the board.

REGIONAL CYBER MATURITY: A GOVERNMENT PERSPECTIVE

Most governments across the region are now beginning to understand and prioritise cyber issues as a core tenet of policymaking. While the urgency and thoroughness of how nations respond to the issue varies significantly, all countries examined in this study are grappling with 'cyber' as a component of state power.

Governance growth

In the past year, there has been a rapid expansion in many nations' cyber policies and governance frameworks. At the forefront of these policy developments have been India, Japan and Singapore, all of which have introduced impressive-looking policy documents that link together the various departments and agencies with responsibilities for cyber issues. However, implementing the policy recommendations found in these documents won't be an easy task.

At the opposite end of the scale are those nations that lack an adequate focus on their cyber policies, this list includes Cambodia, Myanmar, the Philippines, Thailand, Papua New Guinea, and Indonesia. There's an opportunity for nations that have sophisticated mechanisms in place to help build policy capacity in those nations that are in need of support.

Military use of cyber

There are no surprises about which nations are leading the way in military aspects of cyber capabilities: the US, China, UK, Australia, Singapore and South Korea. However, the increased utilisation of cyber capabilities by the North Korean regime over the past year is a concern. This has put the South Korean Government under pressure to respond to cyber incidents as they arise without an escalation between the two countries, creating another challenge for strategic planners. The onus is on Seoul to develop an ever more sophisticated and mature cyber policy architecture and resilience framework so that it can remain clearheaded in its responses, preventing incidents from turning into large-scale military action in the face of extreme provocation. There's no doubt that we'll see increased military cyber developments in the region.

International engagement

Inevitably the Snowden 'cloud' has hung over the Asia–Pacific region as much as it has over the rest of the world, and this has increasingly had a bearing on the international dialogue on cyberspace. However, a great deal of discussion continues in the region about confidence building measures, capacity building and transparency in the cyber domain, mainly through the ASEAN Political and Security Community. These discussions present an opportunity for nations to increase their cooperation and mutual assistance in cyberspace. Australia had been at the forefront of international efforts chairing the UN Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2013, pushing for a strong practical agenda through ASEAN Regional Forum Workshops, and working hard on practical policing capacity building. China has also been utilising similar avenues, albeit with different agendas, and its energetic efforts in the international arena cannot go unnoticed. There is a need for nations in the region to coordinate more proactively on cyber issues especially given the wider, sometimes tense, geopolitical strategic backdrop. This environment could potentially see small miscalculations in cyberspace or misperceptions of cyber actions result in extremely damaging consequences.

REGIONAL CYBER MATURITY: A BUSINESS PERSPECTIVE

With prospects for the world economy on the rise in 2014, investors and businesses continue to turn to the Asia–Pacific region as a driving force for growth. As home to some of the world's largest and most dynamic economies as well as some of the most impoverished, the region offers a diverse range of opportunities and challenges in the digital realm.

Digital standard-bearers

Australia, Japan, Singapore and South Korea are some of the most digitally savvy economies. With their highly developed infrastructure, highly digitised business communities, large populations of 'digital natives' and engaged governments, they offer many opportunities for investment as well as the capacity to incubate cutting-edge innovations. While these economies aren't generally expected to experience any rapid growth in the near term, they're all highly stable, advanced and diversified.

Economic engines

China and India are giants in the region and Indonesia is on the cusp, with clear potential. All have been marked as key emerging markets to varying degrees and have large populations to match their economic dynamism. While they offer huge opportunities, there are many critical challenges to their cyber maturity. They'll continue to struggle to manage major structural shifts as they attempt to move from more export oriented to more balanced economies. Each country can be characterised as having limited and inconsistent engagement between government and businesses on cyber issues, limited legal and/or technical capacity to combat cybercrime, and little evidence of a strategy to foster a domestic digital economy.

A strategic leveraging of ICT offers great potential to cultivate a vibrant digital economy, but limited infrastructure and unequal accessibility, especially between urban and rural areas, limit the role of the internet in the larger economy. China has for many

years had strict controls on internet content and restrictive access to certain websites, and India and Indonesia have toyed with content control to varying degrees. This may become more attractive to their governments because of real or perceived threats from political unrest and used as a means to control discontent surrounding inequality. Despite these limiting factors, ICT technology usage has been growing quickly in each country and e-commerce and social media adoption is on the rise.

Growth in mobile markets

With technological adoption driven by social media and mobile devices, Malaysia, the Philippines, and Thailand boast growing populations of young 'digital natives'. Each government recognises the potential of domestic digital economies and has adopted strategies or agendas to reflect this, but the ability to realise those ambitions remains questionable. Their government–business interactions are mainly limited and one-way, and their cybercrime and cybersecurity legislation is generally less mature. Each country is a high-potential market with vibrant ICT growth, but political and social issues remain a potential threat to current positive economic trends. The digital economy is certainly a growth area in these nations, with strong investment potential, particularly in digital infrastructure.

Nations with unfulfilled potential

Lack of infrastructure is the largest challenge to the development of a strong digital economy in Cambodia, Myanmar, North Korea and Papua New Guinea. That lack is exacerbated by continued limited investment and by political concerns, limiting the potential for near-term growth in the digital economy. In Papua New Guinea, the recent opening up of the telecommunications sector offers potential for increased connectivity. Myanmar suffers from a stark absence of infrastructure, but increased foreign investment in recent years, matched by ambitious government efforts to promote ICT, show clear potential. While North Korea has the technical capacity to develop a strong digital sector, its current political and social profile limits its allure and potential.

Each of these economies is limited primarily by government and infrastructure deficiencies, but mobile technologies offer the most promising route to increase internet penetration into society and business. With sufficient long-term investment directed at the development of such assets, they have the potential to build niches in the digital marketplace.

METHODOLOGY

RESEARCH QUESTIONS

For this report, research questions were oriented around four key topics: Governance; Military Application; Digital Economy and Business; and Social Engagement. A full scoring breakdown for each question is in Appendix A.

1 Governance

Political considerations and mechanisms influence the organisational approach of a state to cyber issues. This includes the composition of government agencies engaged with cyber matters, legislative intent and ability, and views on international cyber policy issues such as internet governance, the application of international law and the development of norms and principles.

The following indicators provide guidance for diplomatic, government, development, law enforcement and private-sector engagement in regional states.

a) **What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?**

   The existence of a strong organisational structure within government suggests an awareness of cyber issues. The effectiveness and breadth of the organisational structure is an indicator of the sophistication of a government's awareness and ability to engage on cyber issues.

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

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

State views on ISP regulation are suggestive of the state's perspective on the regulation of content, governance and the involvement of the private sector in cyberspace.

The level of content control (censorship) that the state conducts or supports isn't necessarily a measure of cyber maturity, but an understanding of the state's views on content control is important to all other stakeholders when engaging with it.

Because some of the most serious threats from cyberattacks are to critical national infrastructure (CNI), one measure of cyber maturity is the presence of a government CNI protection policy, the implementation of that policy, and an awareness of the threat on the part of both the infrastructure owners (usually the private sector) and the regulators (the government).

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

This indicator provides an understanding of the state's preferred engagement style and views on international security aspects of the cybersphere, such as internet governance, international law, norms, principles and confidence building measures.

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

The existence of a service to help business recover from and prevent cybersecurity incidents indicates an awareness of the risk to business and the economy of such incidents.

2 Military application

Military considerations include the military organisational structure (if any) relating to cyber issues and known state views on the use of cyberspace by the military. Military uses of cyberspace, particularly national capabilities, are a sensitive topic for all regional states, and this area requires careful consideration before engagement is sought or agreed to.

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

A specialised organisational cyber structure within the military indicates some awareness of cyber issues in the armed forces, and possibly the military's perspectives on the use of cyber operations capabilities. This helps to identify states with which military-to-military engagement may be beneficial and the relevant organisational stakeholders.

3 Digital economy and business

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

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

High-quality public–private dialogue on cyber issues demonstrates a mature understanding within government and a good awareness of cyber risks in the private sector. This presents an opportunity either to engage in capacity building or 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?**

The state's level of engagement with the digital economy indicates its ability to harness the digital sector for economic growth. This indicator can guide engagement by governments (to build capacity or develop trade) and businesses.

4 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, indicates the maturity of discourse within the state.

b) **What percentage of the population has internet connectivity?**

This is an indicator of the nature of business and personal engagement with cyberspace, the quality of infrastructure and trust in digital commerce. This can guide engagement by development agencies seeking to build regional economies and by businesses seeking to further develop business in the region.

COMPONENTS OF THE METHODOLOGY

The questions used to assess each nation's cyber maturity were arrived at in a three-step process.

Stage 1

An initial set of questions was formed through expert internal discussion in the ASPI International Cyber Policy Centre. Qualitative data collected from open-source literature was used to make a provisional assessment of each of the questions.

Stage 2

The initial 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 this discussion, the research team developed a set of nine questions that together provide a reliable representation of a nation's overall cyber maturity.

Stage 3

The third step was to weight the indicators in order of their relative importance to a nation'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, with 1 being 'least important' and 10 'most important'. The nine factors were:

- organisational structures
- existing legislation/regulation
- international engagement
- CERTs
- military application
- government–business dialogue
- digital economy
- public awareness
- internet penetration.

The ratings for each category were then averaged to produce a weighting factor that could be used in the calculation of an overall score (Table 1). There was notable agreement among the group about the weightings. The few outlier ratings had little effect on the resulting scores and no effect on the relative rankings of the countries analysed.

By consensus, the most important factors are 1a) Organisational structures and 1b) Existing legislation/regulation, which had average scores of 8.4 and 8.3 out of 10, respectively. The least important—although still moderately important with a score of 4.9—was 4a) Public awareness.

The final step was to rate each country against the nine factors, again on a scale of 1 to 10, with 10 being the highest level of maturity that could be awarded. These assessments were based on an extensive qualitative and quantitative open-source research package.

The overall score for each country is then simply the sum of the scores against each factor weighted by the average importance calculated earlier (Table 2). For ease of interpretation, the overall scores were converted to a percentage of the highest possible score. A score of 100 would reflect perfect policy formulation and implementation, as judged by the expert group.

TABLE 1: WEIGHTINGS ASSIGNED TO EACH CATEGORY

Weighting		Category
8.4	1a)	Organisational structures
8.3	1b)	Existing legislation/regulation
6.9	1c)	International engagement
6.3	1d)	CERTs
7.0	2a)	Military application
7.3	3a)	Government–business dialogue
7.4	3b)	Digital economy
4.9	4a)	Public awareness
6.1	4b)	Internet penetration

TABLE 2: WEIGHTED SCORES

	Country	Weighted score
1	United States	86.3
2	United Kingdom	81.2
3	Australia	75.8
4	South Korea	75.5
5	Japan	75.3
6	Singapore	74.7
7	China	58.4
8	Malaysia	57.9
9	India	45.9
10	Philippines	43.4
11	Indonesia	42.4
12	Thailand	41.6
13	Myanmar	29.7
14	Papua New Guinea	23.0
15	North Korea	20.7
16	Cambodia	20.1

TABLE 3: COUNTRY SCORES, BY CATEGORY

	1. Governance				2. Military	3. Digital economy & business		4. Social engagement		Weighted score
	a) Organisational structure	b) Legislation / regulation	c) International engagement	d) CERTs	a) Military role in cyberspace	a) Govt–business dialogue	b) Digital economy	a) Public awareness	b) Internet connectivity	
Australia	7	9	8	8	7	6	8	7	8	75.8
Cambodia	2	3	3	3	2	1	1	2	1	20.1
China	6	5	9	6	8	3	7	4	4	58.4
India	7	5	5	5	4	3	4	6	2	45.9
Indonesia	5	4	6	6	4	3	4	4	2	42.4
Japan	7	7	8	9	6	8	8	7	8	75.3
Malaysia	7	5	7	7	4	5	6	5	6	57.9
Myanmar	4	4	4	3	5	2	1	2	1	29.7
North Korea	3	1	2	0	7	1	2	1	1	20.7
Papua New Guinea	3	3	3	2	2	1	1	4	2	23.0
Philippines	5	4	5	4	5	2	6	5	3	43.4
Singapore	8	6	7	8	7	8	7	9	8	74.7
South Korea	7	6	7	8	7	8	8	9	9	75.5
Thailand	5	5	4	5	4	2	5	4	3	41.6
UK	9	8	9	6	8	8	8	9	8	81.2
US	9	7	10	9	9	8	9	9	8	86.3

LIMITATIONS OF THE RESEARCH

Some limitations in this research should be noted. First, there are clear limitations to the use of numerical scoring of each nation. The numbers arrived at aren't intended to be absolute, but are meant to provide a guideline for the quick assessment of the level of cyber maturity for the indicator. Beyond that, they're open to the reader's interpretation.

Second, because a great deal of information in this area is necessarily bound in government secrecy, there are clear limits on the material available for analysis. Therefore, this report is based solely on information in the public domain.

This report is intended to initiate open dialogue on issues of cyber maturity that will inform subsequent iterations of the report. The methodology will be refined and sharpened from the feedback that's received.

ENGAGEMENT OPPORTUNITIES

A key aim of this research has been to try to provide a rapid assessment tool for public and private sector readers to make considered, evidence-based, cyber policy judgements when engaging with the countries assessed. Therefore, in each of the nine questions examined, we assessed the potential for engagement and the provision of capacity support from government or the private sector. A colour-coded system (shown in Figure 1) illustrates that potential in Figure 2. Appendix C explains the indicators used to measure engagement potential in each category.

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. This mature level of understanding, capability, or both suggests a clear avenue for engagement and potential collaboration and cooperation.

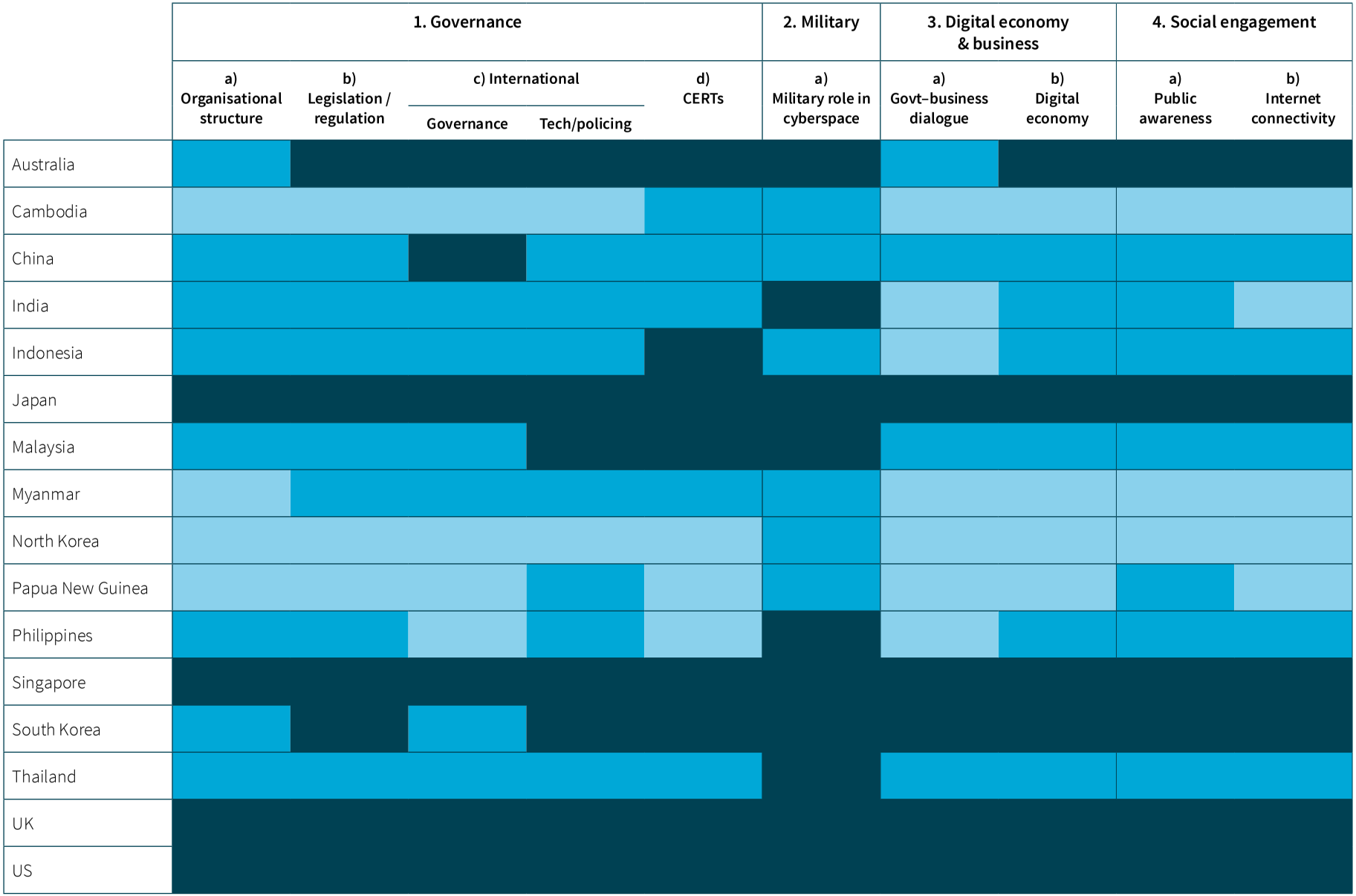
ENGAGEMENT & DEVELOPMENT

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

DEVELOPMENT

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

FIGURE 2: REGIONAL CYBER ENGAGEMENT OPPORTUNITIES



AUSTRALIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	7
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	9
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	8
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	8
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	7
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	6
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	8
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	7
b) What percentage of the population has internet connectivity?	8

OVERALL ASSESSMENT

While the fundamentals of Australia's cyber organisation are strong, they clearly lack a whole-of-government policy perspective. The last Cybersecurity White Paper was released five years ago and there's been significant ambiguity surrounding the country's cyber leadership since the abolition of the Deputy National Security Adviser position in 2013. On the international level, Australia is active in both bilateral and multilateral forums, actively pushing to improve the cyber maturity of other countries in the region. There's generally a strong public understanding of cyber issues and an adequate level of business–government interaction, which should improve with the opening of the Australian Cyber Security Centre in 2014. The Australian Defence Force (ADF) possesses strong cyber capabilities, but is lacking a policy position to guide its and the wider Defence Department's approach to cyber threats.

WEIGHTED SCORE: 75.8

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

Australian Government agencies with responsibility for cyber issues are highly engaged and active in their respective policy and operational areas. However, Australia's score was reduced due to a lack of action by government in updating key policy documents. CNI protection efforts also require invigoration by government and industry stakeholders. Additionally, there's uncertainty about the leadership of cyber policy within government since the dissolution of the Deputy National Security Adviser / Cyber Policy Coordinator role by the current government. Australia's score would improve with greater clarity on policy leadership, and with the effective implementation of the Australian Cyber Security Centre expected in 2014.

SCORE: 7

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

Australia scores highly for its effective development of a range of cyber-related legislation, in particular Division 477.1 of the *Criminal Code Act*. The government also worked closely with industry to create and implement a voluntary code of conduct for ISPs (the iCode). The iCode provides a consistent approach for ISPs when addressing cybersecurity issues and covers 90% of the Australian home internet market. Australia has also acceded to the Council of Europe Convention on Cybercrime, otherwise known as the Budapest Convention. The convention codifies what constitutes a criminal act in cyberspace and streamlines international cybercrime cooperation between signatory states.

Australia's internet censorship is limited, earning it a status of 'Free' in the Freedom House *Freedom on the net* report.[1]

SCORE: 9

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

Australia is actively involved in regional and international multilateral forums on international cyber policy issues. Australia chaired the most recent iteration of the UNGGE, which produced a consensus report confirming the applicability of international law to cyberspace. In March 2014, Australia co-chaired an ASEAN Regional Forum workshop with Malaysia on confidence building measures in cyberspace. The Australian Federal Police has also established strong cybercrime policing relationships across the region, particularly with Indonesia and South Korea. CERT Australia is on the steering committee of the Asia Pacific Computer Emergency Response Team (APCERT) and actively shares threat information with other CERTs across the world. Australia's score reflects its position as an active participant in international cyber engagement across the full spectrum of activities.

SCORE: 8

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

CERT Australia is an agency of the Attorney-General's Department that provides services to business and critical infrastructure operators. It is the single point of contact for cybersecurity issues affecting major Australian businesses and works closely with its government partners. CERT Australia is a founding member of APCERT and is active in several international CERT forums. AusCERT is a private fee-for-service CERT within the University of Queensland and is also an operational member of APCERT. Australia is home to six members of the Forum of Incident Response Security Teams (FIRST) and scores highly for its proactive approach to the introduction and effective operation of CERTs.

SCORE: 8

2 | MILITARY

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

The Department of Defence maintains sophisticated cybersecurity capabilities. The Australian Signals Directorate (ASD) is responsible for the development of the nation's signals intelligence capability. ASD is the Commonwealth Information Security Authority and maintains the *Information security manual* for Australian Government agencies. It also runs the Cyber Security Operations Centre, which is responsible for defending against threats to Australian interests in cyberspace and coordinates operational responses to cyber events of 'national importance'. Defence maintains the Network Operations Centre to protect and manage the security of its own networks. However, Australia's score for this indicator is reduced because there's no publicly available strategy or policy position to guide Defence and the ADF's approach to cyber threats.

SCORE: 7

3 | BUSINESS

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

The Australian National Digital Economy Strategy was launched in 2012 and updated in 2013 from the remnants of the failed Cyber White Paper. The Australian Government has engaged with the private sector on private issues through several different dialogues and programs, including the Prime Minister's Digital Economy Forum in 2012. There are several excellent government–industry services, such as the StaySmartOnline Alert Service, but most of those initiatives appear to be one-way, not two-way dialogues. The development of the iCode is a notable two-way success for public–private engagement. Australia would score higher if two-way engagement programs, such as the Digital Economy Forum, were implemented in a coordinated and sustained manner.

SCORE: 6

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

The digital economy is an important part of Australia's total economic activity: knowledge-intensive jobs account for 42.9% of the workforce[2] and the internet economy accounted for 3.3% of 2010 GDP.[3] Australians are increasingly using the internet for e-commerce transactions, both domestically and internationally. In 2010, the Australian Communications and Media Authority reported that 88% of households made at least one e-commerce transaction in the six months to November 2009; 62% had made four different types of digital transaction in that period.

SCORE: 8

4 | SOCIAL

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

There's significant public awareness of cybersecurity issues, particularly regarding the compromising of Australian Government networks and corporate information and about wider cybercrime. There's also a growing level of discussion in the think-tank and academic domain. Australia's score would be higher if there were greater awareness of broader international cyber policy issues, including the internet governance debate.

SCORE: 7

b) What percentage of the population has internet connectivity?

The Australian individual internet usage rate is at 82.3%[4]. The country had 12.4 million internet subscribers at the end of June 2013, and 19.6 million Australians have mobile phones connected to the internet.

SCORE: 8

CAMBODIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	2
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	3
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	3
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	2
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	1
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	1
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of the population has internet connectivity?	1

OVERALL ASSESSMENT

Cambodia's treatment of cyber issues is largely ad hoc, and it currently has little organisational structure in place. Cambodia has stated that it intends to develop cybercrime legislation based on the model of the Budapest Convention, but there are concerns that the framework may be manipulated and imposed in such a way as to limit free speech online. The government has denied this, stating that there are no plans to use the law to crack down on opposition voices. With very limited internet connectivity, the country's digital economy is fairly constrained. Most of Cambodia's cyber efforts are directed towards capacity and capability building, rather than governance.

WEIGHTED SCORE: 20.1

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

Cambodia doesn't appear to have any sort of governance structure for the management of cyber issues, beyond the development of ICT infrastructure in accordance with its National ICT Policy. Without a concerted whole-of-government effort in this area, Cambodia's digital capacity as well as policy development is likely to be hampered.

SCORE: 2

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

Cambodia's cyber-related legislation is generally undeveloped. Most regulations are implemented through ad hoc and non-binding internal circulars and enforced inconsistently. Cambodia is working to develop cybercrime legislation modelled on the Budapest Convention, but there are fears that this law may perpetuate existing limits on free speech. Cambodia has a *Freedom on the net* status of 'Partly Free'.[5]

SCORE: 3

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

Cambodia is a member of the International Multilateral Partnership Against Cyber Threats (IMPACT) program of the International Telecommunication Union (ITU) and has actively engaged regional partners such as Japan, India and South Korea for ICT capacity-building. However, there's little additional evidence of proactive Cambodian international engagement on cyber issues beyond limited, development-based partnerships.

SCORE: 3

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

CamCERT was established in 2008 within the National ICT Development Authority. CamCERT is charged with developing IT security standards and norms, developing a cybersecurity platform, acting as a national point of contact and investigating and responding to all cybercrime attacks, but there's little data available on its effectiveness. It's not an operational member of APCERT, but participates in the Internet Traffic Monitoring Data Visualisation Project (TSUBAME) Working Group.

SCORE: 3

2 MILITARY

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

While it appears that the Cambodian Armed Forces have at least a superficial involvement with cyber policy and security, the extent and detail of that involvement remain unclear in open-source material. Regardless of the level of defence force involvement, it's understood that Cambodia has a 'very limited' capability to defend against cyberattacks.

SCORE: 2

3 BUSINESS

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

There's little evidence of dialogue between the government and private sector on cyber issues. The government has yet to build a level of internal cyber maturity that would allow it to reach out to external cyber stakeholders. In the past, it has pressured ISPs to block access to certain domains or sites, but that seems to be the extent of its interaction with the private sector.

SCORE: 1

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

With low levels of internet penetration (4.9%) and only 2.5% of the workforce employed in knowledge-intensive jobs, Cambodia's engagement with the digital economy is minimal.[6] Because of insufficient infrastructure and limited investment at this time, there's little short-term prospect of Cambodia's digital economy growing significantly.

SCORE: 1

4 SOCIAL

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

There's some reporting of cybersecurity incidents in the Cambodian media, but little evidence of public debate on cyber policy and security issues. However, high social media adoption has provided an avenue for increased civil engagement on various social and political issues.

SCORE: 2

b) What percentage of the population has internet connectivity?

Only 4.9% of Cambodians are connected to the internet[7], and that proportion is growing only slowly. Physical infrastructure and cost are the largest barriers to expanding access, and mobile technologies provide the most promising avenue for short-term improvement.

SCORE: 1

CHINA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	6
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	5
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	6
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	8
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	3
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	7
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has internet connectivity?	4

OVERALL ASSESSMENT

China's cyber-espionage capabilities are well established, but what's less well understood is the lack of internal cyber coordination within the government and the People's Liberation Army (PLA). This is reflective of a wider domestic disinterest in establishing solid cybercrime or cybersecurity legislation or working constructively with businesses. Attention is instead diverted to bolstering domestic surveillance laws and promoting the primacy of the state in internet governance within international forums.

WEIGHTED SCORE: 58.4

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

China has an array of government organs involved in cyber issues, including the Ministry of Information Industry, the Department of Information Security Coordination, the Bureau of Communications Security, the Ministry of State Security and the National Administration for the Protection of State Secrets, to name a few. China's score reflects the uncoordinated way these organisations operate and the seeming lack of overarching, comprehensible, national cyber policy goals or strategy. The Chinese score also reflects the focus of government bodies on domestic surveillance at the expense of other issues, such as consumer protection, cybercrime and critical infrastructure protection.

In February 2014, China established the Central Internet Security and Information Leading Group, a high-level committee charged with addressing increased cyberattacks, guiding public opinion and turning China into a global internet power. Headed by President Xi Jinping and including Premier Li Keqiang, the group has great clout, but it's unclear what impact, if any, it will have on Chinese cyber policymaking.

SCORE: 6

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

China's cyber-related legislation is generally focused on domestic surveillance and information control—specifically, the Law of Guarding State Secrets and the Security Management Procedures in Internet Accessing. China has some of the strongest internet censorship in the world, earning it a *Freedom on the net* status of 'Not Free'.[8] China's score would be higher if legislation addressed cyber issues comprehensively.

SCORE: 5

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

China's high score reflects the systematic approach of the Chinese to engagement in bilateral and multilateral international forums across the full spectrum of international cyber policy and security issues, including the UNGGE. In 2011, China joined Russia, Tajikistan and Uzbekistan in proposing to the UN an international code of conduct for information security, followed by a multistate proposal in 2012 to give the ITU greater control over the internet. Chinese views on internet governance and international law in cyberspace are in conflict with those of Western states such as Australia, the US and the UK, but its strategic and consistent approach means that China scores highly for this indicator.

SCORE: 9

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

China's CERT (CNCERT) is a national body that coordinates other CERTs within China, but it's difficult to rate its effectiveness using open sources. CNCERT's role in national monitoring also contributes to a lower score for this indicator. CNCERT, along with China Education and Research Network Emergency Response Team (CCERT), is an operational member of APCERT. China also hosts four members of FIRST.

SCORE: 6

2 MILITARY

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

Open-source reporting indicates that the PLA has several bureaus that actively conduct cyber-espionage operations. The PLA has also published several doctrinal information and development articles and monographs on information warfare and the role of cyber capabilities in military operations. China's score is reduced by the apparent lack of coordination of these activities within the PLA.

SCORE: 8

3 BUSINESS

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

Engagement between the business community and the government on cyber issues is often confused by a lack of clarity in areas of responsibilities within government, complex regulatory regimes and inconsistent implementation of policy. The Chinese Government has recognised the threat of cyberattacks to Chinese business, but comprehensive action on the issue is not widely evident.

SCORE: 3

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

The digital economy is a fast-growing part of China's economy: 85% of firms use email to interact with clients and suppliers and 66.1% have websites.[9] However, this activity continues to make up only a small portion of China's total economy, in which knowledge-intensive jobs account for only 7.4% of the workforce[10] and the internet economy accounted for only 5.5% of 2010 GDP.[11] While nearly 142 million Chinese shopped online in 2010, China's score for this indicator is reduced because it has no clear policy to further develop the digital economy. The significance of the digital economy was raised in high-level policy agendas as early as in 2003, and the potential for China's huge population to engage in the digital economy is enormous. However, if infrastructure issues, particularly in rural areas, aren't addressed, those high aspirations might result only in a missed opportunity for China to boost consumption and build a robust digital economy.

SCORE: 7

4 SOCIAL

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

The Chinese media are generally quick to report on cyber issues whenever China is accused of cyber-espionage and have been similarly active as the Snowden revelations continue. Beyond that, there's little discussion of cyber issues in traditional Chinese media. There are signs of limited public awareness in non-traditional media and social networks, but strict government controls limit continued and widespread engagement on cyber issues.

SCORE: 4

b) What percentage of the population has internet connectivity?

China has about 618 million internet users.[12] However, while urban areas are well served, poor infrastructure in the rural areas of China means that only about 42.3% of individuals use the internet[13], reducing China's score for this indicator. Mobile internet is becoming an increasingly important means of connectivity in the country, but over-reliance on state-owned enterprises and lack of infrastructure in rural areas have slowed growth in internet accessibility in recent years.

SCORE: 4

INDIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	7
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	5
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	5
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	5
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	4
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	3
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	4
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	6
b) What percentage of the population has internet connectivity?	2

OVERALL ASSESSMENT

The Indian Government is generally aware of cybersecurity risks, as evidenced by its National Cyber Security Policy, Cyber Command and Domestic Cyber legislation, but it lacks follow-through with implementation and enforcement. India's international engagement is generally limited to bilateral discussions with traditional allies, and dialogue with businesses is also underdeveloped. Internet penetration is low, resulting in a weak digital economy and low public awareness of cyber issues.

WEIGHTED SCORE: 45.9

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

Gulshan Rai, head of CERT India (CERT-In), has been appointed as the first National Cyber Security Coordinator, with staff in the National Security Committee Secretariat. India released its National Cyber Security Policy in May 2013. On the surface, the plan is wide-reaching and ambitious and covers many areas of sound cyber policy, but it includes few details on solid implementation strategies and deadlines—a problem India has grappled with in the past. India's score in this category reflects the government's acknowledgement of the cyber issues facing the nation, but also the lack of urgency and irregular implementation of policy by the bureaucracy.

SCORE: 7

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

India has some cyber-specific and cyber-related legislation, but that legislation has been used haphazardly and in some cases has granted significant interception and censorship powers. India's Information Technology Act has been amended several times since 2000 but has been criticised for lacking adequate power to stop malicious activity in the cyber domain. Even though, according to Norton's Cyber Crime Report, 66% of adult Indians who are online were victims of cybercrime in 2012, the number of convictions under current legislation remains in single digits. The Information Technology Act also allows for the government to censor a wide variety of information, which the government has done by blocking Twitter handles and barring access to certain websites. This provision for censorship authority has earned India a *Freedom on the net* status of 'Partly Free'.[14]

SCORE: 5

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

India is actively engaged in bilateral dialogues with a narrow set of key partners, including the US, the UK and Japan, with the main aim of exchanging information on cyber threats. Australia and India are to hold their first bilateral cybersecurity forum in 2014. India was a member of the 2013 UNGGE, and the statement from the Indian-hosted 2013 ASEAN Asia–Europe Meeting of Foreign Ministers noted the work of the UNGGE and the need to ensure cybersecurity without harming freedom of speech. However, India's practical commitment to the statement is unclear. India's score reflects its concentration on mainly bilateral rather than both bilateral and multilateral engagement and the lack of clarity in the government's position on issues such as internet governance.

SCORE: 5

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

CERT-In was established in 2004 and has a range of functions. However, India scored less favourably than it might have done due to the additional role that CERT-In performs. It has a domestic function that includes targeting anti-government websites and commentators and has acted to block such websites. There's an argument that this function provides CERT-In with power beyond that which a CERT should have. CERT-In is an operational member of APCERT and is the only Indian member of FIRST.

SCORE: 5

2 MILITARY

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

The Indian military is aware of cyber threats and has established several organs to address them, including Defence CERT, the Army Cyber Security Establishment, the Defence Information Warfare Agency, the Cyber Security Laboratory and the Military College of Telecommunication Engineering. The establishment of a Cyber Command has also been announced, although it's unclear whether this has been implemented. India's score reflects the Indian Defence Force's awareness of cyber threats, but also its slow implementation and a lack of stated policy direction for military cyber capabilities.

SCORE: 4

3 BUSINESS

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

From scarce available information, it appears that the Indian Government doesn't engage regularly or systematically with the private sector on cyber issues, particularly legislative issues affecting businesses. The only existing mechanism is through the National Information Board, which mandated a dialogue between a range of stakeholders, including the private sector.

SCORE: 3

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

The Indian digital economy is estimated to be about 1.6% of the whole economy; the internet economy accounted for 4.1% of 2010 GDP.[15] India's low internet penetration and its small number of successful cybercrime prosecutions indicate that developing this sector will be challenging without a strategic approach from the Indian Government, which is currently lacking.

SCORE: 4

4 SOCIAL

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

There's been a growing debate on cybersecurity issues since about 2009–10, prompted by increased media coverage on this topic. Indian think tanks are debating and publishing on the topic more frequently, and there are indications that academia will begin to work on the issue more regularly. India will score higher in this category when the broader public are more engaged in the wider cyber debate, which is likely to happen with wider media coverage of more diverse topics.

SCORE: 6

b) What percentage of the population has internet connectivity?

India scores low in this category, as only about 12.6% of the population are connected to the internet.[16] The World Economic Forum ranks India's cyber infrastructure poorly for bandwidth and accessibility.

SCORE: 2

INDONESIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	5
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	6
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	6
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	4
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	3
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	4
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has internet connectivity?	2

OVERALL ASSESSMENT

Indonesia has achieved middle-of-the-range scores for governance structures, legislation and international engagement. For the most part, those scores are connected to positive work carried out in the CERT, cybercrime and policing spheres. Indonesia is developing higher level cyber policy frameworks and has plans to create a 'national cybersecurity body'. Despite strong potential, similar plans have yet to emerge for the Indonesian digital economy.

WEIGHTED SCORE: 42.4

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

Indonesia's score reflects the Indonesian Government's awareness of cyber threats, but also its so far scattered and ineffective response. Cyber policy and security are addressed jointly by the Ministry of Communications and Information and the Ministry of Defence. The Communications Ministry has plans to develop a national cybersecurity body that brings together all cyber stakeholders in the Indonesian Government, but it's unclear whether those plans have been implemented. Similarly, the Ministry of Defence has announced the creation of the Cyber Defence Operations Centre, which could potentially have future responsibility for national cybersecurity policy and network defence, but its status remains unclear.

SCORE: 5

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

Indonesia has enacted some cyber-specific and cyber-related legislation, including the 2010 TIPITI (cybercrime) Act, but it's not clear that those laws are systematically enforced. The government conducts targeted filtering of content, including pornography and Islamic extremist websites, but the filtering is often applied inconsistently by ISPs. Indonesia has a *Freedom on the net* status of 'Partly Free'.[17] Further evidence of implementation of cyber legislation would improve Indonesia's score.

SCORE: 4

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

Indonesia is active in bilateral and multilateral cyber forums, including in ASEAN-led initiatives. It's also active in cybercrime and cybersecurity information exchanges with key partners (including, until recently, the Australian Federal Police) and through membership of the ITU's IMPACT program. It was a member of the 2013 UNGGE. Indonesia has also reached out to international partners to improve its own internal governance and capabilities, most notably by signing a memorandum of understanding with Japan's National Institute of Information and Communications Technology for cooperation in the ICT field. The government's also reportedly considering initiating a cybersecurity cooperation program with Estonia. While Indonesia is engaged internationally, its participation is generally passive, which has resulted in a lower score.

SCORE: 6

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

Indonesia has several public and private CERTs, including one member of FIRST. While the operational capacity of the CERTs could be stronger, Indonesia's score is improved by the active participation of Indonesian CERTs in forums such as APCERT, which it co-founded with Australia and Japan. Both the Indonesian Computer Emergency Response Team (ID-CERT) and the Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (ID-SIRTII/CC) are operational members of APCERT.

SCORE: 6

2 | MILITARY

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

The Indonesian Defence Minister has announced the planned establishment of the Cyber Defence Operations Centre to coordinate national cybersecurity efforts, including service-specific work by the Indonesian military on cybersecurity. The centre is also slated to draft a national doctrine on cybersecurity and conduct implementation strategies across defence and other departments. The creation of a dedicated 'cyber army' has also been proposed. The Defence Minister explained that the force would consist of elite membership embedded in the various branches of the Indonesian military to protect domestic networks against cyberattack. It's unclear what progress has been made on this initiative. This announcement shows that there's awareness of cyber threats in the Indonesian military, but the response is unclear.

SCORE: 4

3 | BUSINESS

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

There are some moves by the Indonesian Government to engage business on cyber issues specifically related to the oversight and regulation of ISPs. Indonesia's score reflects the seemingly irregular nature of that engagement.

SCORE: 3

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

With the internet economy equalling 1.3% of 2010 GDP[18] and increasing internet penetration, particularly via mobile devices, there's significant potential for the development of the digital economy in Indonesia. However, only 7.4% of the workforce is currently working in knowledge-intensive jobs, and the lack of a comprehensive government strategy to further develop the digital economy means that Indonesia scores poorly.[19]

SCORE: 4

4 | SOCIAL

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

Recently, there's been strong domestic media coverage of foreign intelligence-gathering targeting Indonesian leaders. There's also semi-frequent coverage of 'attacks' against government websites and debates about freedom of speech online. It's difficult to establish whether there's a deeper understanding of cyber issues outside those concerns. Indonesian leaders have recently taken to publicly emphasising cybersecurity issues, which may help to broaden the debate beyond its current focus on foreign surveillance.

SCORE: 4

b) What percentage of the population has internet connectivity?

The individual internet usage rate in Indonesia is 15.4%.[20] The Indonesian Government has stated that its goal is to roll out broadband services to 15 million households by 2015, which would constitute about 20% of households nationally.

SCORE: 2

JAPAN

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	7
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	7
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	8
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	9
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	6
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	8
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	7
b) What percentage of the population has internet connectivity?	8

OVERALL ASSESSMENT

Japan's a highly engaged and capable actor in cyberspace. The government has clearly demonstrated its intentions to be proactive on cyber issues, publishing a Cybersecurity Strategy in 2013 and having instituted a wide range of legislation. Japan has some significant challenges to overcome, primarily at the intragovernmental level, but has shown clear determination to address these issues. It's heavily engaged regionally and internationally on cyber issues and continues to be a global leader in the digital economy.

WEIGHTED SCORE: 75.3

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

Japan has developed a solid organisational structure for government cyber efforts centred on the Cabinet Office's National Information Security Center (NISC) and Information Security Policy Council, which were established in 2005. The NISC is charged with securing national security and emergency response systems and drafting standards, recommendations and reports on cyber issues. The Chief Cabinet Secretary chairs the Information Security Policy Council, which handles cyber policy and works with the NISC and the Government Security Operation Coordination Team to ensure the implementation of policies at the ministerial and agency levels. National government cyber efforts have benefited from continuity, as Suguru Yamaguchi has served as the Adviser on Information Security since 2004. The National Police Agency guides cybercrime efforts, while the Japan Self-Defense Force established its Command, Control, Communications, and Computer Systems Command in 2008. Despite a strong organisational structure and wide breadth of cyber efforts, a lack of intergovernmental coordination and fragmentation in government operations have been identified as limitations on Japan's effectiveness.

SCORE: 7

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

Japan has demonstrated a clear understanding of its vulnerabilities in cyberspace and what needs to be done to address them. In June 2013, the Japanese Government adopted the Cybersecurity Strategy, which is focused on building cyber resilience and provides a solid foundation for future cyber efforts. The issue of collective defence as it applies to cyberspace is a serious area of concern for Japan, as interpretations of its constitutional limitations on the use of force have confused the range of options available to respond to cyberattacks. Japan has a relatively strong cyber relationship with critical infrastructure owners and operators that is set to grow under the 2013 strategy. It has a *Freedom on the net* 2013 status of 'Free'[21], and has instituted very limited content control measures.

SCORE: 7

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

Japan is highly engaged with the international community on cyber issues and has a published International Strategy on Cyber Security. As a signatory to the Budapest Convention and a member of the UNGGE, it's also strongly engaged in bilateral and multilateral efforts, in particular with the US and regional countries and through ASEAN.

SCORE: 8

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

Japan is home to 22 members of FIRST, and JPCERT/CC is the key Computer Security Incident Response Team (CSIRT) in the country. JPCERT/CC helped to form and provides secretariat functions for APCERT and regularly engages with CERTs in the larger Asia–Pacific region.

SCORE: 9

2 MILITARY

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

The recent Japanese National Security Strategy clearly outlines Japan's interests in cyberspace, including means to address current limitations in Japanese cyber capabilities. The Japan Self-Defense Force (JSDF) Command, Control, Communications and Computer Systems Command is charged with the development of national cyberdefence capabilities. Under the command, the JSDF established a Cyber Defense Unit. The defence force is seen to have the necessary structures in place for cyber operations. The JSDF is working to improve its capability, especially through cooperation with the US, but a shortage of qualified personnel, an inability to respond to attacks, weak capabilities and problems in information sharing within the force remain areas of concern.

SCORE: 6

3 BUSINESS

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

Japan has a fairly mature understanding and good awareness of private industry cyber risks, as is laid out in the 2013 Cybersecurity Strategy. The Japanese Cyber Security Information Sharing Partnership was established to facilitate information-sharing between and among manufacturers and government. Under the strategy, the NISC will further efforts for 'organic collaboration' within government institutions and with critical infrastructure providers. In April 2013, Japan launched a cyber team to help companies recover from cyberattacks.

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 is a strong segment of Japan's economy. Internet activities accounted for 4.7% of 2010 GDP[22], and 37.8% of the workforce is employed in knowledge-intensive jobs.[23] Japan is home to some of the world's largest IT and internet companies, including Hitachi, Panasonic, Fujitsu and Rakuten. The Japanese economy has a strong digital infrastructure, but there's room for increased use of digital technologies in both business-to-business and business-to-consumer interactions.

SCORE: 8

4 SOCIAL

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

Public awareness and media coverage of cyber issues have grown quickly in the wake of the March 2013 cyberattacks launched against South Korean organisations and following intensified government efforts in cybersecurity. The government is actively involved in raising awareness under the rubric of cyberspace hygiene, including by promoting 'Cyber Clean Day' and events as part of Information Security Awareness Month and the International Cyber Security Campaign.

SCORE: 7

b) What percentage of the population has internet connectivity?

Japan has 79.1% internet penetration and strong fixed and wireless infrastructure.[24] It was an early and enthusiastic adopter of mobile internet technology, leading to mobile broadband subscriptions equal to 113.1% of the population.

SCORE: 8

MALAYSIA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	7
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	5
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	7
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	7
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	4
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	5
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	6
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has internet connectivity?	6

OVERALL ASSESSMENT

Malaysia has a sound organisational cyber architecture but is weighed down by weak cyber legislation. The country's very active in the technical elements of international cyber diplomacy and is showing increased interest in the policy aspects. Growing internet penetration is a good sign for its digital economy, as is the government's tailored strategy to develop the sector.

WEIGHTED SCORE: 57.9

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

The Malaysian Government appears to be actively building a structure to manage cybersecurity risks in a coordinated manner through the establishment of CyberSecurity Malaysia and an active CNI protection program. CyberSecurity Malaysia has responsibility for emergency response, security capability, capacity development, outreach, risk assessment and cybersecurity evaluation and certification. The agency also penned the country's National Cyber Security Policy. Malaysia will score higher in this category following the full implementation of the strategies outlined in the policy.

SCORE: 7

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

While Malaysia's organisational approach has been strong, its supporting legislation is generally vague. This may be contributing to a dramatic increase in the rates of cybercrime. CyberSecurity Malaysia put the cost of cybercrime at US$300 million for the first six months of 2013, a 100% increase on the previous year. Malaysia's score is also reduced because the existing legislation has the potential to allow government to strongly regulate information within the country. Limited internet censorship has already occurred in Malaysia and many fear stricter future control, resulting in a 'Partly Free' *Freedom on the net* status.

SCORE: 5

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

Malaysia is highly active in the region in bilateral and multilateral projects through ASEAN and ITU–IMPACT, with a focus on the exchange of technical data and signatures. In March 2014, Malaysia co-chaired an ASEAN Regional Forum workshop with Australia on confidence building measures in cyberspace. Malaysia's score would be improved if it engaged further in higher level policy discussions as well as technical information exchanges.

SCORE: 7

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

MyCERT is an agency of the Ministry of Science, Technology and Innovation and is active in APCERT and the Organisation of Islamic Cooperation CERT. Malaysia is home to two members of FIRST.

MyCERT operates a computer security incident response hotline ('Cyber999') and runs the CyberSecurity Malaysia Malware Research Centre. MyCERT also holds technical workshops throughout Asia and in the Middle East.

SCORE: 7

2 | MILITARY

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

Reports indicate that the Malaysian Armed Forces have begun to develop capabilities to protect national assets, including from cyber threats, and the Malaysian Defence Minister has publicly supported the development of an ASEAN master plan for Southeast Asia's cybersecurity. Malaysia's score reflects an awareness of cyber risks within the armed forces, but is reduced by the lack of clear policy direction for the development of cyber capabilities.

SCORE: 4

3 | BUSINESS

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

CyberSecurity Malaysia has an outreach program to provide advice and support to Malaysian business, including the Cyber999 emergency response hotline. Malaysia's score would be improved if there were further evidence of a two-way dialogue between Malaysian business and the Malaysian Government.

SCORE: 5

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

The Malaysian digital economy is small but growing. It accounts for 4.1% of GDP[25], and 26.8% of the workforce works in knowledge-intensive jobs. The World Economic Forum characterises take-up by business as 'aggressive'.[26] Malaysia's score reflects the existence of a government strategy to further develop this sector, and is likely to improve as the sector grows in importance.

SCORE: 6

4 | SOCIAL

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

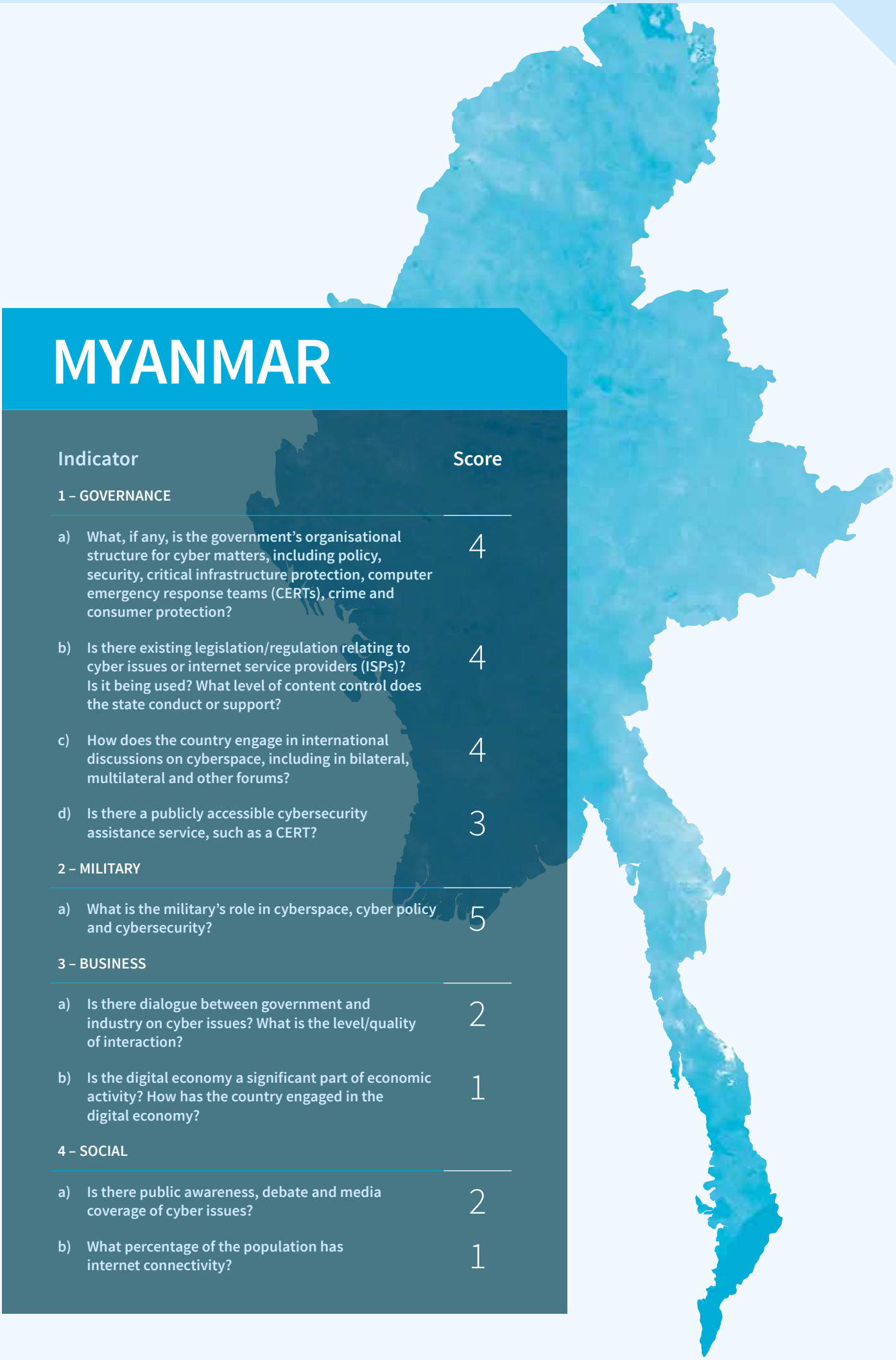
Discussion of cybersecurity incidents is common in the Malaysian media, but there's little discussion of other cyber issues. Malaysia's score reflects the nascent state of most cyber discussions in Malaysian media, think tanks and academia.

SCORE: 5

b) What percentage of the population has internet connectivity?

The internet is used by 65.8% of Malaysians, one of the highest rates in Southeast Asia.[27] Despite active efforts by the Malaysian Government to promote internet and mobile accessibility, penetration remains low outside urban areas.

SCORE: 6



MYANMAR

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	4
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	3
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	5
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	1
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	2
b) What percentage of the population has internet connectivity?	1

OVERALL ASSESSMENT

Myanmar has developed an ICT master plan, but it's mainly concerned with expanding very basic online services. Myanmar's military has a relatively well-developed cyber capability, which is probably a remnant of the armed forces' previous role in conducting widespread domestic surveillance. The country's lack of ICT infrastructure and very low internet penetration have prevented the emergence of a digital economy and public and business–government dialogue.

WEIGHTED SCORE: 29.7

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

Myanmar has one of the lowest levels of internet penetration in the region. Even when factoring in mobile internet usage, penetration reached only 2.8% in 2013. Unsurprisingly, the government doesn't possess an organisational policy structure for cyber matters. Current plans concern the development of e-education, human resource development and ICT legislation.

In July 2011, Myanmar announced the creation of its ICT Masterplan 2011–2015. The plan is designed to help develop the country's infant ICT infrastructure. This is the country's second master plan; the first, covering 2005–2010, led to an increase in Myanmar's telephone density from 1% to 5.4% in 2011.

Despite very low levels of cybercrime in the country, the Myanmar Police Force has created an IT crime section for what it has identified as an 'emerging future issue'.

The Myanmar Computer Science Development Council has ultimate control in creating national ICT policy and defining long-term and short-term ICT plans. The Posts and Telecommunications Department defines standards, coordinates cooperation with international organisations and oversees implementation.

Myanmar has no CNI protection policy.

SCORE: 4

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

The Computer Science Development Law (1996) criminalises the use of a computer network to undermine state security, community peace or national unity or to distribute state secrets, among other actions. The Wide Area Network Order (2002) and the Electronic Transactions Law (2004) both build upon the 1996 law and are products of the period of military rule and censorship within the country. Moves to alter or remove the more draconian elements of legislation restricting free speech have come up against firm opposition, and only small inroads have been made in relation to a reduction in sentencing. Under the Anti-Human Trafficking Law, posting pornographic material on the internet is punishable by five to ten years' imprisonment, in addition to a possible fine. Continued strict measures earned the country a *Freedom on the net* report status of 'Not Free'.[28]

The ICT Masterplan 2011–2015 contains provisions and plans for the creation of ICT legislation, but the plans haven't yet been pursued.

SCORE: 4

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

Myanmar drew on South Korean support in the formation of its ICT Masterplan 2011–2015, and Myanmar's Ministry of Science and Technology is planning to launch a US$1 million e-learning centre with the South Korean Government.

Myanmar is a member of TSUBAME (an internet threat monitoring system), IMPACT and APCERT.

The Singaporean Government has assisted in the development of Myanmar's Defence Services Computer Directorate. The Russian and Chinese governments have also provided training to military personnel.

Myanmar's international interactions continue to be one-way; it plays a very minimal role in international policy discussions.

SCORE: 4

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

Myanmar Computer Emergency Response Team (mmCERT) is a non-profit organisation within the Myanmar Computer Federation that acts as a single point of contact for cyber incidents in Myanmar. mmCERT works with the public and business to raise cybersecurity awareness, but has been criticised in the media for its weaknesses in publicising information. It's an operational member of APCERT.

SCORE: 3

2 | MILITARY

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

The Defence Services Computer Directorate, under the Army Chief of Staff, encompasses network centric warfare, military-oriented cyber capabilities and electronic warfare. The Army's military strategy has been expanded to include cyberwarfare as part of 'people's war under modern conditions'.

Military Affairs Security (formerly the Directorate of Defense Services Intelligence) also possesses a cyber unit, but is more politically focused, carrying out monitoring both domestically and internationally. There are suggestions that the unit's capability has grown exponentially in recent years with the assistance of other countries in the region. Russia and China have provided training to officers, and Singapore and China have both provided physical infrastructure support.

SCORE: 5

3 | BUSINESS

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

There are limited opportunities for interaction through mmCERT, and communications seem to be limited to one-way messaging.

The Open Technology Fund released a report into internet access and openness in February 2013. One of its key findings was that there was a 'lack of open and formal process for private industry or civil society to engage with government'.[29]

SCORE: 2

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

Very low levels of internet connectivity within Myanmar have prevented the growth of a meaningful digital economy. Some 26% of the country's population lives below the poverty line, and 50% of total GDP is tied to the agricultural sector.

SCORE: 1

4 | SOCIAL

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

Low levels of internet connectivity have led to a generally low level of public understanding and discourse on cyber issues. However, organisations such as the Myanmar Standard Computing Education Centre and the Myanmar Computer Professionals Association are facilitating a basic level of dialogue.

SCORE: 2

b) What percentage of the population has internet connectivity?

Myanmar has one of the lowest internet penetration levels in the region: the ITU estimates that 1.1% of individuals use the internet.[30] Only 7% of the population own mobile phones, and landline density is lower at 1%.

The government has plans to increase mobile penetration to 50%. It has awarded contracts to two external mobile network providers, but SIM cards remain prohibitively expensive for most people and network coverage remains very poor.

SCORE: 1

NORTH KOREA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	3
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	1
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	2
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	7
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	1
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	2
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	1
b) What percentage of the population has internet connectivity?	1

OVERALL ASSESSMENT

North Korea's unique political situation has resulted in a paradoxical cyber maturity assessment. North Korea possesses a sophisticated military cyber capability backed by a targeted and proactive research, development and education program. Although attempts have been made to leverage this capability to build a domestic IT industry, political and social challenges and the larger internet blackout in the country are very strong limiting factors.

WEIGHTED SCORE: 20.7

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

North Korea has a highly centralised organisational structure for government activities, including cyber issues. Evidence suggests that the General Staff Reconnaissance Bureau is the central authority for the country's cyber capabilities. The Central Party Investigative Group is charged with technical education and training, the Unification Bureau uses cyber-based psychological operations on behalf of the government, and the Korea Computer Centre is believed to operate several research and development centres with several branches in China, Germany and Syria. Although government cyber organisation is highly structured, it's primarily concentrated in the military; there's little or no evidence of policy, cybercrime and cybersafety bodies.

SCORE: 3

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

North Korea has little domestic cyber infrastructure and highly limited internet connectivity. Legislation appears to be limited to governing military operations, content censorship and limiting access. The country has a very strong censorship regime and extremely limited internet access. Access to the national intranet, Kwangmyong, is heavily regulated and mainly limited to a select few.

SCORE: 1

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

North Korea has adopted a highly reclusive foreign policy, which extends to cyber issues. There's evidence that it has leveraged bilateral relationships, historically with the former Soviet Union and now with Russia, Iran and China, for technology sharing and IT training, but it isn't openly involved in multilateral and internet governance engagement.

SCORE: 2

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

There's no evidence of a publicly accessible CERT program in North Korea. With highly limited public access to the internet, an air-gapped domestic intranet and advanced government cyber capabilities, there's little demand to develop a national CERT.

SCORE: 0

2 MILITARY

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

The North Korean military is believed to have highly developed cyber capabilities and a well-organised and extensive education and research program to support future operations. Unit 121 is believed to be its primary offensive cyber force; personnel estimates range from 300 to 3,000 people. It's believed that North Korea's military has successfully infiltrated South Korean government and private sector systems, but there's little understanding of the military's defensive capabilities.

SCORE: 7

3 BUSINESS

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

With strong centralised planning and control over domestic industry, there's a high level of overlap between government and business, but there's little evidence of any open dialogue between the government and industry on cyber issues.

SCORE: 1

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

Although the digital economy isn't a significant part of North Korea's economy, there have been attempts to leverage growing digital expertise to improve the country's IT sector. Organisations such as the Korea Computer Center and Pyongyang Informatic Centre are aiming to export IT services, software and cybersecurity systems.

SCORE: 2

4 SOCIAL

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

Public awareness of cyber issues appears to be limited to highly controlled coverage by government media, including accusations of cyberattacks by South Korea and the US. North Korea does have a proactive educational program to develop domestic offensive cyber capabilities.

SCORE: 1

b) What percentage of the population has internet connectivity?

Internet connectivity is highly limited. Access to the tightly controlled Kwangmyong intranet is also extremely limited, probably to fewer than 1,000 individuals and a select group of research institutions, government ministries, schools and factories.[31]

SCORE: 1

PAPUA NEW GUINEA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	3
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	3
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	3
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	2
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	2
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	1
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	1
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has internet connectivity?	2

OVERALL ASSESSMENT

Papua New Guinea (PNG) is taking proactive steps to improve its cyber maturity, but a lack of resources and infrastructure has proven to be a limiting factor in this area. The government has recognised the importance of the issue, joining ITU–IMPACT, pressing for increased investment in digital infrastructure, and calling for a Cyber Cell in its most recent Defence White Paper. Through international engagement, particularly with Australia, PNG has been strongly involved in addressing cybercrime issues, and similar support in other areas of cyber governance and to build technical capabilities could prove highly beneficial for the country.

WEIGHTED SCORE: 23.0

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

PNG's organisational structure for cyber issues is relatively limited and focused mainly on IT development and cybercrime issues. The National Information and Communications Technology Authority (NICTA) is responsible for the regulation and licensing of ICT and aims at 'making ICT services work in PNG's public interest'.[32] PNG has been proactive in developing its policy and capacity to police cybercrime in an effort led by NICTA in consultation with international partners.

SCORE: 3

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

Much of PNG's cyber legislation and regulation is being developed through the ITU's Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC) programs. NICTA has also been proactive in developing ICT regulations and is currently involved in the development of a cybercrime Bill. There's concern over recent efforts to censor online 'subversive' discussion through the creation of a government 'monitoring committee', but the capacity to enforce those measures is questionable. PNG is making a concerted effort to adopt external frameworks to build domestic cyber legislation and regulation, especially in the area of cybercrime, but the efforts remain ongoing and capacity for implementation is an area for improvement.

SCORE: 3

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

PNG has been proactive in reaching out to international partners to develop domestic cyber policies and capabilities. Working with ITU–IMPACT, the Australian Attorney-General's Department, APEC, various development organisations and other actors, it's been strongly engaged in internal capacity building. However, international engagement on governance issues remains limited.

SCORE: 3

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

PNG is not home to a recognised domestic CERT; however, it's a member of PacCERT, which covers 22 constituent countries throughout the Pacific.

SCORE: 2

2 | MILITARY

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

Despite recent attempts to bolster the strength of the PNG Defence Force, which has limited capabilities and resources, cyber issues have traditionally not been a priority for the country. The 2013 Defence White Paper made reference to establishing a defensive 'Cyber Cell' to protect a yet to be developed 'Integrated ICT Network', but outlined no timelines or implementation strategies. Clear evidence of military cyber policy and capacity in cyber operations remains limited.

SCORE: 2

3 | BUSINESS

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

There's little evidence of strong official engagement between the government and industry on cyber issues. However, the government is actively pursuing efforts with private entities to improve internet accessibility in the country, and NICTA is engaged with the ICT sector for the development of physical infrastructure.

SCORE: 1

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

PNG has a limited digital economy, but recent structural reform has increased opportunities in the telecommunications sector. As competition increases in the ICT sector, reduced internet costs and improved accessibility and speed will open new opportunities for the country's digital economy.

SCORE: 1

4 | SOCIAL

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

Public awareness and debate concerning cyber issues and the use of ICT have grown quickly within PNG. Connectivity driven by mobile phone use and the spread of social networks has resulted in what many have called the 'PNG Spring'. Forums such as SharpTalk have spurred public discourse of all sorts, including on cyber issues. The government has also been proactive in increasing cybersafety through the Pacific Islands Chiefs of Police Cyber Safety Pasifika program.

SCORE: 4

b) What percentage of the population has internet connectivity?

Internet connectivity in PNG is very limited, at only 2.3% total internet penetration.[33] However, the rapid adoption of mobile technology has the potential to quickly expand internet penetration. While the government has been actively supporting a national transmission network for the country, infrastructure and costs are likely to remain the main barriers to improved connectivity for some time.

SCORE: 2

PHILIPPINES

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	5
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	4
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	5
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	4
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	5
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	6
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	5
b) What percentage of the population has internet connectivity?	3

OVERALL ASSESSMENT

The Philippines has demonstrated an awareness of cyber threats, but a lack of sufficient legislation and capabilities is a clear limitation. As emphasised in the 2011 Digital Strategy, with sufficient investment in infrastructure the Philippines has the potential to bolster its currently limited digital economy. While there are intentions to improve national cyber maturity, a lack of resources tempers the prospect of significant near-term developments.

WEIGHTED SCORE: 43.4

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

The Philippines Government has shown an awareness of cyber threats and has made some efforts to address them, with a narrow focus on cybercrime issues. However, those efforts are generally ineffectively implemented or not implemented at all. The Philippines' score for this indicator reflects the country's awareness of cyber risks, but also its inability to deal with them effectively.

SCORE: 5

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

There's very limited internet regulation in the Philippines, which has earned it a *Freedom on the net* status of 'Free'.[34] Only one law, the Anti-Child Pornography Act of 2009, places restrictions on online content. The country has a strong Bill of Rights, and ISPs are generally uncooperative when it comes to releasing information to government agencies. When strong online libel and monitoring provisions were added to the 2012 Cybercrime Prevention Act, the public and industry backlash was so severe that the bill was derailed and the provisions eventually dropped. A 2010 Symantec report indicated that up to 87% of Filipino internet users have been victims of online crime or 'malicious activities', but only two people have ever been successfully convicted for hacking under the E-Commerce Act passed in 2000. This may improve as the Philippines National Police's Anti Cyber Crime Group builds capability. CNI protection is relatively unorganised.

SCORE: 4

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

The Philippines participates in several multilateral cyber-oriented working groups and workshops led by organisations such as APEC, ASEAN and the UN, with a particular focus on the area of cybercrime. Although involved in these forums and a member of ITU–IMPACT, it often shows no interest in taking an active role in them. It maintains infrequent bilateral dialogues on cyber issues, mainly with the US. The Philippines' score for this indicator score reflects its narrow engagement focus and lack of active engagement.

SCORE: 5

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

PH-CERT is the Philippines' national representative to APCERT. It's a non-profit, voluntary organisation that draws its funding from membership fees and sponsorship arrangements. Recently, PH-CERT has faced operational problems due to lack of financial support and low staffing. The Philippines National Police Criminal Investigation and Detection Group has publicly stated that it will revive the government CERT (GCSIRT), which was disbanded in 2008, but it's unclear whether that has occurred.

SCORE: 4

2 | MILITARY

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

The Armed Forces of the Philippines have created a Security Operation Center with a primarily defensive role, protecting military systems. However, a higher score wasn't given because it's unclear to what extent the centre has been implemented.

SCORE: 5

3 | BUSINESS

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

Currently, only around 19.7% of the workforce[35] is involved in knowledge-intensive jobs. While there appear to be mechanisms to aid the growth of the country's ICT-led industries in a purely economic sense through the 2011 Digital Strategy, there's little evidence of proactive measures to engage industry on cybersecurity matters. Therefore, the country scores poorly in this area.

SCORE: 2

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

The Philippines' 2011 Digital Strategy shows that there's an awareness of the benefits to be gained from developing the nation's digital economy, and of the barriers to such development. However, it's unclear what practical action has been taken to overcome those barriers. The strategy noted that, with improved infrastructure, the Philippines could rival India in the global market for business process outsourcing.

SCORE: 6

4 | SOCIAL

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

There's currently a discussion driven by the media about the vulnerability of government and public-facing computer networks. This followed several high-profile breaches. Some non-government organisations and academic institutes are also beginning to hold discussions on cybersecurity issues. But there's a lack of a deeper research agenda, in part due to an academic environment that's too focused on the technical elements of ICT but also because of the underdevelopment of the think-tank community.

SCORE: 5

b) What percentage of the population has internet connectivity?

The Philippines' score for this indicator reflects an internet penetration of about 36.2%.[36] Unequal distribution of access between urban and rural areas, high costs of access and slow speeds all remain challenges for improved internet access.

SCORE: 3

SINGAPORE

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	8
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	7
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	8
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	7
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	7
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has internet connectivity?	8

OVERVIEW

Singapore has a very strong cyber governance structure, including accompanying legislation that covers both computer misuse and CNI protection. Singapore's very active in international cyber forums and has a very capable CERT team. The military has also established a hub for defending defence networks. Business–government dialogue is very strong, and the e-commerce sector holds great potential. The Singaporean public is highly networked and very aware of cyber issues.

WEIGHTED SCORE: 74.7

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

The Singapore Government's National Infocomm Security Committee brings together relevant government departments to implement a coordinated whole-of-government response to cybersecurity issues, in line with the National Cyber Security Masterplan 2018 released in July 2013. The plan also established the Critical Infocomm Infrastructure Protection Assessment Program, and an active National Cyber Security Exercise Program for CNI owners is also in place.

The new National Cyber Security Centre (NCSC) headed by the Singapore Infocomm Technology Security Authority is currently being established and is likely to enhance Singapore's capabilities in the early detection and prevention of cyberattacks.

SCORE: 8

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

Singapore has successfully implemented legislation, such as the Computer Misuse and Cybersecurity Act, to prevent and respond to cyber issues, including cybercrime and hacking. However, the regulations include provisions that allow the government to compel organisations to disclose data to the government for the purpose of pre-emptive cybersecurity. There are also strict regulations for websites that discuss political issues.

SCORE: 6

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

Singapore scores highly for its involvement in technical information exchange, anti-cybercrime collaboration and CERT engagement. The Infocomm Development Authority of Singapore founded the ASEAN CERT Incident Drill and has led the drill since July 2006. The authority has also signed information-sharing agreements with government organisations in other advanced economies. The agreements also allow joint training and development opportunities. Singapore has the potential to score higher for this indicator if it takes a more active leadership role in discussions on international cyber policy and security issues.

SCORE: 7

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

SingCERT was established by the Singaporean Government in 1997 under the Infocomm Development Authority. SingCERT has been active in organising and hosting ASEAN and APCERT exercises. Singapore hosts seven FIRST members.

SCORE: 8

2 MILITARY

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

The Singaporean Armed Forces have established a Cyber Defence Operations Hub, aimed at protecting domestic military networks. This indicates that there's an awareness of cyber risks and that work is underway to address them. Singapore's score would be higher if there were a publicly available Singaporean Armed Forces strategy or policy on how the armed forces will engage with cyber threats.

SCORE: 7

3 BUSINESS

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

Singapore scores highly for this indicator because it has a strong relationship with its CNI providers and private sector engagement is a key aspect of its National Cyber Security Masterplan. The score's also boosted by the strong commercial links between the Singapore Government and Singaporean CNI operators.

SCORE: 8

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

Singapore's size and connectivity mean that the digital economy has strong potential for growth, but there appears to be a reluctance by Singaporeans to use the internet for e-commerce. Knowledge-intensive jobs account for 51% of the workforce[37], and electronics hardware production is an important part of Singapore's manufacturing sector.

SCORE: 7

4 SOCIAL

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

There's a widespread awareness of cyber risks in Singapore, aided by government-supported information-raising activities, such as sector-specific Infocomm security programs, scholarships for cybersecurity research and the Cyber Security Awareness Alliance, which seeks to raise public knowledge of cybersecurity and basic security practices.

SCORE: 9

b) What percentage of the population has internet connectivity?

Singapore has high internet connectivity: about 74.2% of its population uses the internet.[38] Mobile internet, with 123.3 mobile-broadband subscriptions per 100 inhabitants, is also very popular.

SCORE: 8

SOUTH KOREA

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	7
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	6
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	7
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	8
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	7
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	8
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has internet connectivity?	9

OVERALL ASSESSMENT

South Korea is a leading technological actor in cyberspace and has some of the world's most advanced digital infrastructure. As evidenced by clear governmental organisation and a body of legislation on cyber issues, the South Korean Government is highly aware of and responsive to all cyber issue areas. With a highly capable military and advanced digital economy, South Korea scores well across the board in this assessment. However, in defining cyberspace primarily as an operational domain, the country's overemphasis on security comes at the expense of cybercrime and international cyber governance.

WEIGHTED SCORE: 75.5

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

South Korea has a strong organisational structure for cyber issues, centred primarily on the National Cyber Security Strategy Council and the National Cyber Security Center (NCSC). The Strategy Council oversees the development of national cybersecurity infrastructure and the coordination of policy and roles within government. The NCSC falls within the National Intelligence Service and is the main cyber policy agency taking the lead in identifying and responding to cyber threats. The National Intelligence Service, the National Police Agency, the Cyber War Center and the Korea Communications Service respond to cyber issues within their areas of concern under the coordination of the NCSC. South Korea's also considering the creation of a cybersecurity secretary post within the office of the President. In developing its governmental structures for cybersecurity, South Korea has demonstrated a clear understanding of the major facets of cyber policy. It has particularly strong policies on CNI protection and resilience.

SCORE: 7

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

South Korea has a strong catalogue of cyber legislation and regulation, along with an active critical infrastructure cyber policy. In 2011, it adopted the National Cyber Security Strategy, which defines cyberspace as an operational domain and emphasises a three-tier defence system, strengthening security measures, building a solid legal framework, and strengthening international cooperation. Legislation provides the government with wide legal flexibility to act in cyberspace, which has led to some international concern about South Korea's content-control activities. Because of the government's heavy censorship powers and ISP regulations, South Korea received a status of 'Partly Free' in the 2013 *Freedom on the net* report.[39] Despite South Korea's strong legislation and robust interaction with critical infrastructure operators, content-control issues reduce its score for this indicator.

SCORE: 6

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

South Korea has highlighted strengthening international cyber cooperation in its 2011 Cyber Strategy and played host to the recent Seoul Conference on Cyberspace. Despite numerous bilateral and multilateral initiatives, South Korea's engagement remains somewhat disjointed, with a tendency to focus on security issues over wider cyber issues, such as internet governance.

SCORE: 7

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

South Korea hosts seven members of FIRST. The two leading national CERTs are KrCERT/CC, which falls under the purview of the Korea Internet and Security Agency, and KNCERT/CC, which is part of the National Intelligence Service. KrCERT/CC is an operational member of APCERT and focuses on the private sector, including broadcasting, telecommunications and ICT.

SCORE: 8

2 | MILITARY

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

South Korea has a capable military cyber capacity. The Defense Information Warfare Response Center of the Defense Security Command protects military networks, while the Cyber Command unit handles wider online security. South Korea has both defensive and offensive capabilities and in February 2014 announced its intention to develop offensive cyber capabilities specifically to target North Korea's nuclear program. However, recent allegations of military cyber unit interference in national elections reduce the country's score for this indicator. A new Cyber Defence Department, set to be launched in May 2014, aims to halt these domestic interference issues. The new command is to be established under the Joint Chiefs of Staff, with responsibility for all cyberwarfare missions. It will also include an oversight committee and a whistleblower program.

SCORE: 7

3 | BUSINESS

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

The South Korean Government has a very mature relationship with the business sector. The Korea Internet Security Center of the Korea Communications Commission oversees the security of private-sector networks. The National Cyber Security Center works with the military and public and private sectors to coordinate information-sharing partnerships, prevent cyberattacks and coordinate cyber emergency responses.

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 is an important part of South Korea's economy. Internet activities accounted for 7.3% of 2010 GDP[40], and 22.4% of the workforce is involved in knowledge-intensive jobs.[41] South Korea is home to some of the world's largest IT companies, most notably Samsung. Although business-to-business internet use has room for growth, business-to-consumer internet use is high.

SCORE: 8

4 | SOCIAL

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

There's heavy coverage of cybersecurity issues in the media, mainly because of the pervasive threat from North Korea. The government has also taken a proactive approach to raising public awareness and preparedness, sponsoring numerous educational mass media and advertising campaigns focused on cybersecurity. The Mobile Security Forum, launched by the Korea Communications Commission in 2010, focused on smartphone and mobile internet use, and the Korea Information Security Agency aims to make South Korea the strongest, safest, most advanced country on the internet.

SCORE: 9

b) What percentage of the population has internet connectivity?

South Korea has one of the most advanced cyber infrastructures in the world, and 84.1% of the population uses the internet.[42] South Korea regularly ranks as having the world's fastest internet speeds. Maintenance and upgrades to infrastructure remain an important priority for the government.

SCORE: 9

THAILAND

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	5
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	5
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	4
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	5
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	4
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	2
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	5
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	4
b) What percentage of the population has internet connectivity?	3

OVERALL ASSESSMENT

Thailand has a moderately developed organisational structure for cyber issues and is pursuing positive legislative agendas, although there's some concern about content control. The government and military have made positive moves to develop cyber governance and capability. This includes efforts to increase investment in digital infrastructure, internet connectivity and the ICT sector. If current efforts are continued and backed by much-needed investment, Thailand's cyber maturity outlook is generally positive.

WEIGHTED SCORE: 41.6

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

Thailand's organisational structure for cyber issues is reasonably developed, with several institutions in place and improving clarity about roles and responsibilities. Cyber policy is primarily owned by the Ministry of Information and Communications Technology. However, the government has recently raised the profile of cyber issues by launching the National Cyber Security Committee, chaired by the Prime Minister. The Electronic Transactions Development Agency is charged with coordinating the implementation of cyber strategies and measures and is working with international partners to improve national cyber capacity. The Royal Thai Police is charged with maintaining law online. Basic frameworks for national cyber efforts are in place, suggesting a clear understanding and willingness to act on cyber issues. The support structures to further develop policy and implement measures remain a work in progress.

SCORE: 5

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

Thailand's cyber legislation and regulation are largely a work in progress. The government is actively pursuing legislation to improve cybersecurity, to police cybercrime, and to develop clear national cyber strategies. However, the legal measures needed to support government cyber activities remain limited. Thailand does have in place extensive legislation on content control; this is primarily focused on enforcing Chapter II, Article 8 of the Constitution, which states that 'the King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action.' Despite heavy legal authority to regulate online content, political, social and human rights discussions unrelated to the monarchy are largely unregulated, earning Thailand a 'Partly Free' status in the 2013 *Freedom on the net* report.[43]

SCORE: 5

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

Thailand's international engagement on cyber issues is largely focused on capacity building and less on wider cyber issues, such as internet governance. Thailand's a member of the ITU–IMPACT program, hosted the 2013 FIRST Conference, and has expressed support for the ASEAN Regional Forum's efforts to develop a Work Plan on Cyber Security. Thailand has established many international partnerships to improve domestic cyber capabilities, including with the International Council of Electronic Commerce Consultants and the SANS Institute.

SCORE: 4

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

The primary CERT in Thailand is ThaiCERT, an APCERT operational member and the only Thai representative in FIRST. ThaiCERT is operated within the Electronic Transactions Development Agency and engages with regional partners regularly. Efforts were underway to upgrade ThaiCERT to become a national incident response team by February 2014.

SCORE: 5

2 MILITARY

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

The Thai military currently has limited capability and authority on cyber issues, but its leadership has expressed an interest in developing legislation to legalise the operation of a cyber army. Thailand hosted the 2013 USPACOM Cyber Endeavour program, which focused on communications and IT interoperability.

SCORE: 4

3 BUSINESS

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

Dialogue between the Thai Government and industry on cyber issues remains fairly limited. However, mechanisms are in place to build dialogue within the Cyber Security Operations Centre. The Ministry of Information and Communications Technology has also introduced a 24-hour hotline to help improve engagement with the public on cyber threats.

SCORE: 2

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

Knowledge-intensive jobs are performed by 10.8% of the Thai workforce.[44] Heavy investment in infrastructure and new technology for cellular networks are expected in the near future, and the Thai ICT sector is expected to expand by 10%.[45]

SCORE: 5

4 SOCIAL

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

Social media adoption in Thailand has been high, but wider knowledge of cybersecurity and cybersafety remains low. The upper socioeconomic groups tend to have a higher concern about privacy issues than is found among lower socioeconomic groups. Media censorship enforced during times of political crisis has resulted in an increased political discourse about online content control, but larger discussions of cyber issues remain relatively limited.

SCORE: 4

b) What percentage of the population has internet connectivity?

In Thailand, approximately 26.5% of individuals use the internet, and the spread of mobile technologies has greatly improved connectivity.[46] The Ministry of Information and Communications Technology is particularly concerned about internet penetration and plans to increase technology adoption through the SmartThailand project and the One Tablet per Child campaign.

SCORE: 3

UNITED KINGDOM

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	9
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	8
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	9
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	6
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	8
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	8
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has internet connectivity?	8

OVERVIEW

The UK is a world leader in several cyber maturity areas, including international engagement, business–government dialogue, public awareness and the digital economy. The military also has a clearly defined policy and investment strategy for its cyber capabilities, and is one of the few national defence forces to have such a strategy.

WEIGHTED SCORE: 81.2

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

The UK has established a comprehensive structure within government to address cyber issues, including policy, crime, defence and critical infrastructure, under the leadership of the Office of Cyber Security and Information Assurance (OCSIA) within the Cabinet Office. Work carried out under the National Cyber Security Programme, is coordinated by the OCSIA, who work with the Home Office, Ministry of Defence, Government Communications Headquarters (GCHQ), the Centre for Protection of national Infrastructure (CPNI), the Foreign and Commonwealth Office and the Department for Business, Innovation and Skills, to implement the programme.

SCORE: 9

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

The UK's cyber-related legislation has been effectively developed and implemented. All UK ISPs are privately owned, existing within a freely operating market. There is minimal regulation of internet content or access other than material that is traditionally illegal over all public platforms including child pornography, or material that may incite racial violence or terrorism. The Digital Economy Act 2010 allows the blocking of sites that infringe intellectual property such as file sharing. Overall, British content control is limited, earning the country a *Freedom on the net* status of 'Free'.[47]

SCORE: 8

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

The UK has positioned itself as a thought leader on international cyber policy issues, most notably through the establishment of the London International Cyberspace Agenda in 2011 and its ongoing involvement in the UNGGE, The Organization for Security and Co-operation in Europe (OSCE) and World Economic Forum processes. It's also highly active in pursuing bilateral dialogues with a host of nations on these issues, and often includes cybersecurity as an agenda item in official meetings with bilateral partners. Additionally it has invested £2 million in a Global Centre for Cyber Security Capacity Building.

SCORE: 9

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

While the UK has several private CERTs, including 17 FIRST members, and dedicated government and defence force CERTs it only recently established its first national CERT (CERT-UK) in March 2014. CERT-UK will work to develop the UK's cyber resilience to state-sponsored and criminal attacks on elements of critical infrastructure and within government departments in a holistic and coordinated manner that engages with the private sector and academia. CERT-UK also has responsibility for national cyber incident management response. However, the UK is scored lower as the centre is in its infancy and therefore, as yet, operationally unproven.

SCORE: 6

2 | MILITARY

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

The UK Ministry of Defence is developing a full-spectrum cyber operations capability in partnership with the GCHQ. The Joint Cyber Unit, under Joint Forces Command, will recruit regular and reservist personnel specifically for their cyber skills to develop the country's capacity in this area. This includes an offensive cyber capability to enhance the UK's military capability, at a cost of around £500 million. The UK scores highly for this indicator because it has a clear policy goal for its military cyber capability and has invested in it. It scores no higher because the integration of GCHQ's intelligence capability and the Ministry of Defence's offensive requirements is still under development.

SCORE: 8

3 | BUSINESS

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

The UK Government has engaged with business on cybersecurity information sharing through the Cyber Security Information Sharing Partnership (CISP) which provides a platform for companies to share cyber threat information in real time and involves over 250 large firms and major organisations. The government is also active in developing the skills base and threat awareness of British personnel in support of the country's cybersecurity industry. The UK's engagement is systematically and consistently implemented.

SCORE: 8

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

The UK's digital economy is worth about £82 billion per year, £45 billion of which is from e-commerce. The UK was ranked 1/144 for business-to-consumer internet use in the 2013 World Economic Forum Networked Readiness Index. Some 42.5% of the workforce is engaged in knowledge-intensive jobs[48], and the internet economy accounted for 8.3% of 2010 GDP.[49]

SCORE: 8

4 | SOCIAL

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

There's significant mature discussion of cybersecurity issues in the British media, think tanks and academic domain. There are a number of cyber-specific programs within key think tanks and academic departments throughout the country which help foster informed public debate on the key issues. In 2013, the Home Office announced a dedicated £4 million cyber awareness program for businesses and private users.

SCORE: 9

b) What percentage of the population has internet connectivity?

According to the ITU, 87% of individuals in the UK used the internet in 2011.[50] In 2013, 36 million adults (73% of all adults in the UK) accessed the internet every day, 72% of adults bought goods or services online, and 83% of households had internet access (42% of which had fibre or cable broadband).

SCORE: 8

UNITED STATES

Indicator	Score
1 – GOVERNANCE	
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	9
b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	7
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	10
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	9
2 – MILITARY	
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	9
3 – BUSINESS	
a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	8
b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	9
4 – SOCIAL	
a) Is there public awareness, debate and media coverage of cyber issues?	9
b) What percentage of the population has internet connectivity?	8

OVERALL ASSESSMENT

The US is a leading actor in cyber governance and technical capabilities, backed by a strong digital economy, including Silicon Valley and many large and start-up tech communities throughout the country. The Obama White House has doubled down on cyber efforts initiated by the previous administration, but congressional gridlock has proven to be a major roadblock to legislative progress. Heavily engaged internationally at all levels of government, the US also possesses advanced offensive and defensive military cyber capabilities.

WEIGHTED SCORE: 86.3

1 GOVERNANCE

a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?

The US has a strong organisational structure to handle cyber issues, with responsibilities divided among government departments and agencies. The White House has an appointed US Cybersecurity Coordinator at the level of Special Assistant to the President to guide Executive branch efforts. The Department of Homeland Security (DHS) and the Department of Defense (DoD) are the primary cybersecurity actors. DHS is charged with securing federal civilian networks and the 'broader cyberecosystem', while DoD protects military domains and possesses defensive and offensive cyber capabilities. DHS is also the primary agency charged with CNI protection, which has been bolstered by recent Executive efforts, including Executive Order 13636. Anti-cybercrime responsibility is generally disseminated among local and state authorities under existing jurisdictional arrangements, with the Federal Bureau of Investigation leading federal efforts. Despite a strong structure in place, the lack of a clear whole-of-government cyber strategy and problems in interdepartmental coordination remain weaknesses for US Government cyber efforts.

SCORE: 9

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

While there's no overarching framework legislation governing cyber issues, the US does have a strong collection of policies and regulations relating to cyber issues. The Executive branch has been especially proactive in promoting federal government cyber policies as well as public–private partnerships on cyber issues. The US has a clear and public cyber strategy and a strong ability to implement cyber programs. The internet is largely seen as a 'self-governing' domain, so ISP regulation is lax, although recent moves by the Federal Communications Commission suggest interest in government protection of net-neutrality. Content control is severely limited under the Constitution, earning the US a *Freedom on the net* 2013 status of 'Free'.[51] Despite a strong slate of policies, the recent inability of Congress to pass any legislation on cyber issues is reflected in the score for this indicator.

SCORE: 7

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

The US exhibits a high level of multilayered international involvement on cyber issues, including bilateral and multilateral engagement and participation in international cyber initiatives. The US has ratified the Budapest Convention on Cybercrime, was a party to the UNGGE, is heavily involved in the creation of international cyber standards, and regularly takes part in international cyber initiatives. The Obama White House has published an International Strategy for Cyberspace that outlines US priorities and values in the cybersphere.

SCORE: 10

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

The US is home to 68 members of FIRST, including the CERT Program at Carnegie Mellon University. US-CERT, under DHS, is the leading national CERT and is proactive nationally as well as internationally.

SCORE: 9

2 MILITARY

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

DoD's role in cyberspace is largely concerned with signals intelligence, the defence of .mil domains, and offensive and defensive military cyber operations. Cybersecurity has been identified as a national security priority in the National Security Strategy, and DoD has published a Strategy for Operating in Cyberspace to guide its cyber efforts. The US military possesses sophisticated offensive, defensive, and surveillance capabilities, but internal coordination and governing policies concerning those operations could use further development.

SCORE: 9

3 BUSINESS

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

The US Government has a strong dialogue with the larger business community, in particular with technology companies, defence contractors, banks and other big businesses. Informal and formal meetings between government officials and industry representatives occur regularly, and official programs under DHS, the Federal Trade Commission and the Federal Bureau of Investigation's InfraGard program enhance the dialogue. The Executive Branch is seeking to further improve cooperation, especially for critical infrastructure security.

SCORE: 8

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

The US is home to some of the largest IT, software, hardware and internet companies in the world, as well as to numerous start-up communities. Knowledge-intensive jobs account for 36.3% of the workforce[52], and the internet economy accounted for 4.7% of 2010 GDP.[53]

SCORE: 9

4 SOCIAL

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

Public awareness of and debate on cyber issues are very high in the US, and are currently driven by media coverage of the National Security Agency's surveillance programs. While the mass media are focused on the National Security Agency, China and cybercrime at the expense of cyber governance issues, there's a robust think tank, non-government organisation, academic and independent coverage of a wide spectrum of cyber topics. Despite concerns about overall public apathy, grassroots efforts in response to recent legislation (the Stop Online Piracy Act and the PROTECT IP Act) suggest that concerns and the potential for mobilisation on cyber-related issues remain high.

SCORE: 9

b) What percentage of the population has internet connectivity?

In the US, 81% of individuals use the internet. However, the need for infrastructure upgrades and lack of coverage in rural and poorer communities remain areas for improvement.[54] Despite political overtures pushing for better access and increasing internet speeds, the US continues to lag behind in connection speeds.

SCORE: 8

APPENDIXES

APPENDIX A:
SCORING BREAKDOWN

Key indicators	Scoring breakdown	
1a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection?	0–2 =	No organisational structure, policy frameworks, or protections
	3–4 =	Basic organisational structures (mainly technical); some plans for policy and organisational development
	5–6 =	Policy frameworks and organisational structures exist, but are neither comprehensive nor properly implemented
	7–8 =	Strong policy frameworks and organisational structures exist, but implementation is not comprehensive
	9–10 =	Extensive, strong policy frameworks and organisational structures exist and are fully implemented
1b) Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs)? Is it being used? What level of content control does the state conduct or support?	0–2 =	No cybersecurity laws exist; insufficient legislation or excessive government regulation
	3–4 =	A few laws exist, but without adequate implementation measures
	5–6 =	A legal framework exists, with moderate implementation; some regulation in specific areas
	7–8 =	A strong legal framework exists and is adequately implemented; minimal content control and limited regulation, while maintaining the rule of law in an open society
	9–10 =	Laws cover most cybersecurity areas and are strongly implemented; little or no content control and regulation, while maintaining the rule of law in an open society
1c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	0–2 =	No international engagement
	3–4 =	Minimal international engagement; aid-based or basic technical/policing
	5–6 =	Some bilateral and multilateral engagement in technical/policing and policy
	7–8 =	Very strong bilateral and multilateral engagement in technical/policing and policy engagement
	9–10 =	Multilayered international engagement; bilateral and multilateral engagement, technical/policing and policy engagement, with leadership roles
1d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	0–2 =	No
	3–4 =	Minimal or limited response capability
	5–6 =	Uneven response
	7–8 =	Well-structured and planned response capability; international engagement
	9–10 =	Strong response capability; strong international leadership
2a) What is the military's role in cyberspace, cyber policy and cybersecurity?	0–2 =	No existing cyber capabilities
	3–4 =	Minimal or planned defensive capabilities
	5–6 =	Well-developed cyber capabilities; defined civilian and military roles
	7–8 =	Very well-developed cyber capabilities; well-defined civilian and military cyber roles; some international engagement
	9–10 =	Integrated military command; well-defined civilian and military cyber roles, with clear cyber policy strategy direction and ongoing international engagement

Key indicators	Scoring breakdown	
3a) Is there dialogue between government and industry on cyber issues? What is the level/quality of interaction?	0–2 =	No dialogue
	3–4 =	Limited dialogue
	5–6 =	Dialogue exists, but is one-way or with only a few sectors
	7–8 =	Two-way dialogue exists with a broad range of sectors
	9–10 =	Strong two-way dialogue exists, with capacity for the private sector to play an active role in policy and operational issues
3b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?	0–2 =	Little or no evidence of a digital economy
	3–4 =	There is an awareness of the benefits of the digital economy, which is a small portion of economic activity
	5–6 =	Digital economy is a growing part of economic activity, but no government policy to assist it exists
	7–8 =	Digital economy is a strong and expanding part of economic activity; some government policy to assist it exists
	9–10 =	Digital economy is a fully integrated element of the nation's economic activity; strongly developed and mature government policy to assist digital economic growth
4a) Is there public awareness, debate and media coverage of cyber issues?	0–2 =	No dialogue on cybersecurity issues
	3–4 =	Some, but little coverage or interest
	5–6 =	Awareness, but mainly media- and NGO-led
	7–8 =	Strong public, media and private sector debate on cybersecurity issues
	9–10 =	Very strong public, media, academic and private sector debate on cybersecurity issues
4b) What percentage of the population has internet connectivity?	0–2 =	0–20%
	3–4 =	30–40%
	5–6 =	50–60%
	7–8 =	70–80%
	9–10 =	90–100%

APPENDIX B:
OVERALL CYBER MATURITY COUNTRY RANKINGS (WEIGHTED)

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

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

APPENDIX C:
ENGAGEMENT OPPORTUNITIES INDICATORS

Indicator	Mature engagement	Engagement & development	Development
1 – GOVERNANCE			
a) What, if any, is the government's organisational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (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, sharing of best practices.	• Lack of structure or other challenges are a significant barrier to engagement on cyber issues. • Potential for development-based aid on cyber issues.
b) Is there existing legislation/ regulation relating to cyber issues or internet service providers (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 and/or enforcement. • Opportunity to assist in further development of legislation and/ or enforcement capacity-building.	• Lacks proficient legislation, regulation or CNI policy. • Could benefit from external assistance in both policy development and enforcement. • Candidate for adoption of existing frameworks or models (e.g. Budapest Convention on Cybercrime).
c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?	*Governance* • Full multilateral and bilateral engagement on cyber issues. • Strong opportunities for constructive engagement on cyber issues. • Potential for partnership to further common agendas.	*Governance* • Some opportunity for mainly bilateral engagement on cyber issues. • Potential for dialogue to develop common agendas.	*Governance* • Little opportunity for engagement on cyber governance issues.
	Technical & policing • Strong technical capabilities and cybercrime policing regime. • Potential for sharing or development of best practices.	*Technical & policing* • Demonstrated technical capabilities and concern about cybercrime issues, but room for improvement remains. • Potential recipient for technical aid and cybercrime partnerships.	*Technical & policing* • Limited demonstrated government interest in developing technical and/or anti-cybercrime capabilities.

Indicator	Mature engagement	Engagement & development	Development
d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?	• Established, internationally engaged CERT. • Opportunity to build CERT-to-CERT partnership and to share best practices and information.	• Non-engaged national CERT team present. • Opportunity to develop CERT-to-CERT dialogue.	• Little or no CERT capabilities • Opportunity to help establish national CERT team.
2 – MILITARY			
a) What is the military's role in cyberspace, cyber policy and cybersecurity?	• Clear military engagement with cyber issues. • Opportunity for dialogue, joint cyber exercises and information sharing.	• Clear military involvement with cyber issues. • Opportunities to develop and/or further cyber confidence-building measures.	• Little or no opportunity for constructive military-to-military engagement on cyber issues.
3 – BUSINESS			
a) Is there dialogue between government and industry on cyber issues? What is the level/ quality of interaction?	• Strong government–business dialogue/ interaction. • Government responsive to business cyber concerns. • Healthy business environment for 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 digital economy.
4 – SOCIAL			
a) Is there public awareness, debate and media coverage of cyber issues?	• Strong public awareness of cyber issues through new and traditional media outlets. • Cyber-knowledgeable end-users and wide adoption of digital media offer strong opportunities for business-to-customer interactions.	• Some awareness of cyber issues, mainly limited to new media (blogs, social media). • Opportunity to aid in the building of civic understanding of cyber issues.	• Little or no public awareness of cyber issues. • Opportunity for wide range of educational, outreach and capacity-building efforts on cyber issues.
b) What percentage of the population has internet connectivity?	• Strong existing infrastructure to support advanced digital economy.	• Some internet infrastructure available, often limited to urban areas. • Investment opportunities for infrastructure development.	• Development opportunity requiring high-level, long-term investment in basic infrastructure.

APPENDIX D:
SELECTED KEY INDICATORS

	Freedom on the net report[a]	ITU MIS 2013: % of individuals using the internet (2012)[b]	FIRST membership	WEF GITR Report: Knowledge-intensive jobs, % workforce (rank)[c]	Internet economy as % of 2010 GDP[d]	ITU–IMPACT membership	APCERT operational member teams
Australia	Free	82.3	6	42.9 (12)	3.3	No	CERT Australia, AusCERT,
Cambodia	Partly Free	4.9	0	2.5 (108)	n.a.	Yes	n.a.
China	Not Free	42.3	4	7.4 (100)	5.5	Yes	CCERT, CNCERT / CC
India	Partly Free	12.6	1	n.a.	4.1	Yes	CERT-In
Indonesia	Partly Free	15.4	1	7.4 (98)	1.3	Yes	ID-CERT, ID-SIRTII/CC
Japan	Free	79.1	22	37.8 (26)	4.7	No	JPCERT/CC
Malaysia	Partly Free	65.8	2	26.8 (51)	4.1[e]	Yes	MyCERT
Myanmar	Not Free	1.1	0	n.a.	n.a.	Yes	mmCERT
North Korea	n.a.	n.a.	0	n.a.	n.a.	No	n.a.
Papua New Guinea	n.a.	2.3 (total internet use penetration)	0	n.a.	n.a.	Yes	n.a.
Philippines	Free	36.2	0	19.7 (72)	n.a.	Yes	n.a.
Singapore	n.a.	74.2	7	51.0 (2)	n.a.	No	SingCERT
South Korea	Partly Free	84.1	7	22.4 (61)	7.3	No	KrCERT/CC
Thailand	Partly Free	26.5	1	10.8 (97)	n.a.	Yes	ThaiCERT
UK	Free	87	17	42.5 (13)	8.3	No	n.a.
US	Free	81	68	36.3 (29)	4.7	No	n.a.

n.a. = Not available

a http://freedomhouse.org/report/freedom-net-2013-global-scores

b www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf

c www3.weforum.org/docs/WEF_GITR_Report_2013.pdf

d www.bcg.com/documents/file100409.pdf

e www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries

ACRONYMS AND ABBREVIATIONS

ADF	Australian Defence Force
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
ASD	Australian Signals Directorate
ASEAN	Association of Southeast Asian Nations
AusCERT	Australia CERT
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
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security (US)
DoD	Department of Defense (US)
FIRST	Forum of Incident Response and Security Teams
GCHQ	Government Communications Headquarters (UK)
GCSIRT	Government Computer Security Incident Response Team (Philippines)
GDP	gross domestic product
ICT	information and communications technology
ID-CERT	Indonesia CERT
ID-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center
IMPACT	International Multilateral Partnership Against Cyber Threats
ISP	internet service provider
IT	information technology
ITU	International Telecommunication Union
JSDF	Japan Self-Defense Force
JPCERT/CC	Japan CERT/Coordination Center
KNCERT/CC	South Korea National Intelligence Service CERT for critical infrastructure in government/public sector
KrCERT/CC	Korea Internet Security Center (South Korea)
MIS	Measuring the Information Society report
mmCERT	Myanmar CERT
MyCERT	Malaysia CERT
NCSC	National Cyber Security Centre/Center (Singapore / South Korea)
NICTA	National Information and Communications Technology Authority (PNG)
NISC	National Information Security Center (Japan)
PacCERT	Pacific CERT
PH-CERT	Philippines CERT
PLA	People's Liberation Army
PNG	Papua New Guinea
SingCERT	Singapore CERT
ThaiCERT	Thailand CERT
TSUBAME	Internet Traffic Monitoring Data Visualisation Project
UK	United Kingdom
UN	United Nations
UNGGE	UN Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security
US	United States of America
US-CERT	United States CERT
USPACOM	United States Pacific Command
WEF GITR	World Economic Forum Global information Technology Report

NOTES

1 http://freedomhouse.org/report/freedom-net-2013-global-scores
2 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
3 www.bcg.com/documents/file100409.pdf
4 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
5 http://freedomhouse.org/report/freedom-net-2013-global-scores
6 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
7 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
8 http://freedomhouse.org/report/freedom-net-2013-global-scores
9 http://www.enterprisesurveys.org/data/exploreTopics/innovation-and-technology#east-asia-pacific
10 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
11 www.bcg.com/documents/file100409.pdf
12 www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201403/t20140305_46240.htm
13 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
14 http://freedomhouse.org/report/freedom-net-2013-global-scores
15 www.bcg.com/documents/file100409.pdf
16 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
17 http://freedomhouse.org/report/freedom-net-2013-global-scores
18 www.bcg.com/documents/file100409.pdf
19 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
20 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
21 http://freedomhouse.org/report/freedom-net-2013-global-scores
22 www.bcg.com/documents/file100409.pdf
23 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
24 www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
25 www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries
26 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
27 www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
28 http://freedomhouse.org/report/freedom-net-2013-global-scores
29 https://www.opentechfund.org/files/reports/otf_myanmar_access_openness_public.pdf
30 www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
31 http://blog.foreignpolicy.com/posts/2013/03/15/a_total_cyber_blackout_in_north_korea_would_affect_about_1000_citizens
32 www.nicta.gov.pg/Pages/Home.aspx
33 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
34 http://freedomhouse.org/report/freedom-net-2013-global-scores
35 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
36 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
37 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
38 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
39 http://freedomhouse.org/report/freedom-net-2013-global-scores
40 www.bcg.com/documents/file100409.pdf
41 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
42 www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
43 http://freedomhouse.org/report/freedom-net-2013-global-scores
44 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
45 www.buyusainfo.net/docs/x_1061713.pdf
46 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
47 http://freedomhouse.org/report/freedom-net-2013-global-scores
48 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
49 www.bcg.com/documents/file100409.pdf
50 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf
51 http://freedomhouse.org/report/freedom-net-2013-global-scores
52 www3.weforum.org/docs/WEF_GITR_Report_2013.pdf
53 www.bcg.com/documents/file100409.pdf
54 www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf

AUTHOR BIOGRAPHIES

DR TOBIAS FEAKIN

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

JESSICA WOODALL

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

KLÉE AIKEN

Klée Aiken is an Analyst working in ASPI's International Cyber Policy Centre. He joined ASPI in November 2013. Prior to joining the team, Klée spent several years working in DC, serving a stint with the Atlantic Council's International Security Program and Cyber Statecraft Initiative before taking a position as an Analyst with a small international consulting firm. Klée holds a Master's degree in International Relations from the Universiteit van Amsterdam in the Netherlands.