CYBER RESILIENCE IN ASIA-PACIFIC

A REVIEW OF NATIONAL CYBERSECURITY STRATEGIES

UNITED NATIONS UNIVERSITY
Institute in Macau

AUTHORS

Mamello Thinyane and Debora Christine

DISCLAIMER

This publication aims to provide accurate information regarding the subject matter covered. The views and opinions expressed in this publication are those of the authors. They do not purport to represent the official views and opinions of the United Nations University, the United Nations, or any associated organisations.

ACKNOWLEDGEMENTS

This work is supported by the Science and Technology Development Fund of Macau (FDCT) under Grant No. 0016/2019/A

CONTACT

Any questions or comments should be addressed to Mamello Thinyane, United Nations University, Casa Silva Mendes, Estrada do Engenheiro Trigo No. 4, Macau SAR
Email: mamello@unu.edu

SMART CITIZEN CYBER RESILIENCE PROJECT

This report is produced as part of the a project that aims to enhance the resilience of citizens in smart digital futures. It recognizes civil society stakeholders as significant actors in the co-production of national and global cyber resilience.

https://cs.unu.edu/smart-citizens-cyber-resilience

UNITED NATIONS UNIVERSITY

The United Nations University institute in Macau is a research institute at the intersections of information and communication technologies and international development. It conducts policy-relevant research and generates solutions, addressing key issues expressed in the UN 2030 Agenda for Sustainable Development.

RECOMMENDED CITATION

Christine, D. and Thinyane, M. (2020) "Cyber Resilience in Asia-Pacific - A Review of National Cybersecurity Strategies", United Nations University

ISBN: 978-92-808-9121-8

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyber resilience effort and strategy has traditionally been considered from the position of enabling governments and businesses to deliver the intended outcomes despite disruptions to information and communication systems. There has also been a general focus on the security and resilience of critical information infrastructures, such as industrial control systems, supervisory control and data acquisition systems, and also on vital sectors, such as telecommunications, banking, and health services.

Despite the tendency for cyber resilience to be framed from narrow technologies and systems domains, it is an attribute of the whole system and should be considered not only from the perspective of the siloed operational domains but also of the interdependent and interconnected cyber ecosystem.

There is a global recognition of the need for multi-stakeholder partnerships and engagement towards achieving cyber resilience. For example, the World Economic Forum underscored this need in their 2012 report titled 'Partnering for Cyber Resilience.'[1]

The motivation for the ownership of the cyber resilience goal has traditionally been minimal for individual citizens and civil society organisations. However, the civil society is increasingly becoming a key stakeholder in the cyber ecosystem due to several reasons: they represent one of the significant cyber-attack surfaces and vectors (e.g., through social engineering), they suffer an immense loss due to adverse cyber events including identity theft, data leakages, and dis/misinformation, and they have an essential role to play in the co-production of cyber resilience at the individual, community, national, and global levels.

This research investigated the co-production of cyber resilience in Asia and the Pacific by reviewing the national cybersecurity strategies of 14 nation-states in the region to explore the following:

- The involvement of civil society stakeholders in the development of the cybersecurity strategies
- The extent to which resilience is incorporated into the cybersecurity strategies
- The extent to which whole-of-society perspectives are adopted in the strategies
- The roles, responsibilities, and mechanisms for participation ascribed to civil society stakeholders (i.e., individual citizens, communities, and third-sector organisations) in the strategies

The following are the main findings on the extent to which cyber resilience is incorporated in the national cybersecurity strategies of the selected countries.

USE OF 'RESILIENCE' TERMINOLOGY

- Most countries use the term resilience in the national cybersecurity strategies, but few elaborate on the operationalisation of resilience.
- While some countries do not use the term 'resilience', they do include strategies for building resilient systems and ensuring business continuity (e.g., Malaysia, Japan, and South Korea).

RESILIENCE AS A GOAL

Beyond being an element of the national cybersecurity strategy, some countries identify a secure and resilient environment as one of the overarching goals of the national cybersecurity strategy.

CYBER RISKS IDENTIFIED

- All countries identify not only state-level and entity-level cyber risks; they also note individual-level risks (e.g., identify theft).
- People are identified as one of the critical attack surfaces in the strategies.

ROLES AND RESPONSIBILITIES

- Several countries identify the role of community-level stakeholders in the strategy.
- Third-sector organisations are encouraged to participate in:
  - Information-sharing
  - Outreach activities
  - Evaluating cybercrime law (e.g., Bangladesh)

PROTECTION OF VULNERABLE GROUPS

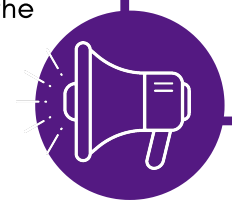
- Several countries identify specific population groups and sectors that are vulnerable to cyber-attacks:
  - Children and young people
  - Women
  - Tourism sector (e.g., Samoa),
  - Elderly communities (e.g., New Zealand, Sri Lanka)
  - Rural communities
- Specific mechanisms to empower the vulnerable are also identified:
  - Child online protection (e.g., Afghanistan, Samoa, Vanuatu, China).
  - Outreach programmes

CAPACITY-BUILDING

- Countries adopt a variety of approaches for building cyber capacity in citizens:
  - Professional training programmes – including sector-specific training
  - Educational programmes run in schools, colleges, and universities
  - Certification and accreditation for professionals

PUBLIC COMMUNICATION

- All countries use diverse programmes and materials to raise awareness of cybersecurity risks.
- Singapore adopts an advanced public outreach approach and draws on behavioural insights to nudge good cyber hygiene practices in the general public.



CITIZEN CO-PRODUCTION OF CYBERSECURITY

- Few countries mention specific tools or platforms to facilitate citizen's participation in cybersecurity.
- Countries have 'hotlines' for citizen reporting of adverse cyber events.

INTRODUCTION

The last decades have seen increased ubiquity and proliferation of digital technologies across many sectors of society. While these technologies provide innumerable benefits to society, they are also associated with numerous adverse impacts in society, economic costs of cyber-attacks, risks of cyber espionage and cyber warfare, social harms from socio-technical threats, and technical compromises to critical infrastructures.

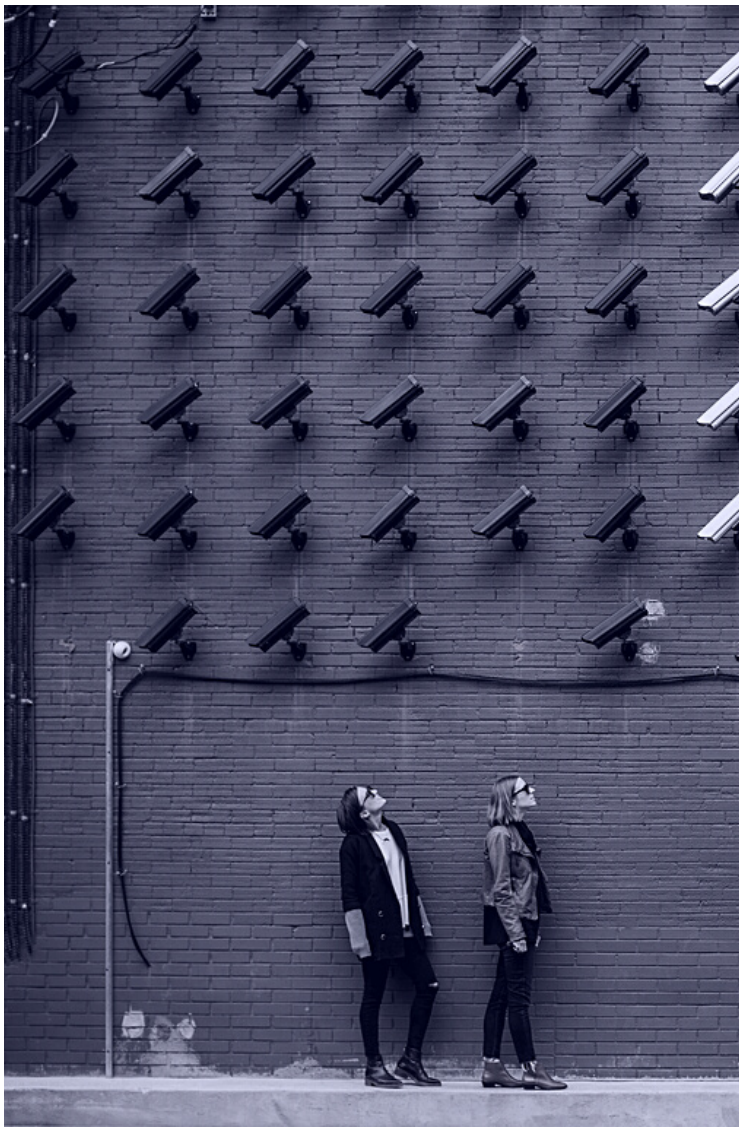
The 2020 Global Risks Report identifies technological risks associated with cyber-attacks, data fraud and theft, and infrastructure breakdown, among the top ten most likely and most impactful global risks.[2] It is, therefore, essential that risk management strategies are put in place to mitigate adverse cyber events and their cascading impacts in society.

Several multilateral frameworks recognise the need for societal resilience against imminent global threats. The UN Sustainable Development Goals (SDGs) advance the goal of 'making cities and human settlements inclusive, resilient, and sustainable' under SDG11.[3] The Sendai Framework for Disaster Risk Reduction also places a key focus on strengthening resilience against disasters, which are broadly defined as 'man-made hazards and related environmental, technological, and biological hazards and risks'.[4]

Lastly, the New Urban Agenda, which was adopted at the Habitat III Conference in 2016, emphasises the need for 'strengthening resilience in cities to reduce risk and impact of disasters'.[5]

As a general concept, resilience describes the capacity of a system to respond to and recover (with increased strength) from shocks, stresses, and disasters.

Socio-ecological resilience transforms the boundary of the resilience framing to consider the opportunity for self-reorganisation and for new trajectories to emerge from disturbance.



Therefore, it recognises the possibility of a system to move to a new, better state or to 'bounce forward'.[6]

Within the cyber domain, resilience refers to the ability of the ecosystem to prepare, absorb, recover, and adapt to adverse cyber incidents, including those associated with cyber-attacks.[7]

Cyber resilience is not only an evolution from a posture of preventing and mitigating adverse cyber events, it is also increasingly being included explicitly in cyber maturity models being adopted around the world.

In the current 21st-century information society, where technology and society are deeply intertwined, adverse cyber events should be understood as the consequence of the failure of multiple factors, including technological factors, human factors, and natural factors.[8] Resilience thus needs to be understood as an arrangement of the social and technical systems.[9]

The social dimension comprises the social, cultural, political, and economic circumstances that shape societies' capability to respond to crises and disasters; while the technical dimension concerns the resilience of complex, interdependent and interconnected information and communication infrastructures.

To accommodate this socio-technical approach to cyber resilience, the definition of cyber resilience advanced in this report is '*the capacity for positive adaptation to achieve the desired functioning in the context of significant adverse cyber events*'.

The goal of cyber resilience in this framing is *to support individuals, communities, organisations, and countries to achieve desired outcomes in their use of cyber resources.*

The recognition of the interplay between various actors and elements within the cyber ecosystem, as well as the multidimensionality of cyber resilience, has given rise to the notion of co-production of cyber resilience. Co-production of cyber resilience can be understood as the participation and active contribution of a broad set of stakeholders towards cyber resilience. This report seeks to understand how co-production of cyber resilience between different societal stakeholders is enabled in Asia-Pacific countries by existing cyber resilience postures.

ASIA-PACIFIC FOCUS

Rapidly growing connectivity and the accelerating pace of digital transformation in Asia-Pacific have increased the vulnerability of the region to cyber risks. According to the Internet Society's Survey on Policy Issues in Asia-Pacific in 2018, cybersecurity is the top Internet policy concern for the region's Internet users.[10] While these issues require states to improve their cyber capacity maturity, cybersecurity is still an evolving sector in the region, with a visible gap between countries with different cyber maturity.

Cybersecurity is a relatively new problem area for some states in Asia-Pacific. While some states are already drafting their second or third edition of their national cybersecurity strategies (hereafter referred to as NCS), others are still in the initial development phase.

Almost half of Asia-Pacific states have no national cybersecurity strategies yet. Some instead have master plans that cover aspects of cybersecurity in the form of national digital policy (e.g., Pakistan, Brunei, Lao People's Democratic Republic), ICT masterplans (e.g., Cambodia, Solomon Island, Micronesia), and e-governance masterplans (e.g., Myanmar). Countries such as Indonesia, Mongolia, and Pakistan have laws and programmes related to cybersecurity, including cybersecurity centres and national computer emergency/incident response team (CERT/CIRT), but do not have a cybersecurity strategy yet. Meanwhile, some countries, such as Nepal and Fiji, are still in the process of drafting their strategies. Given the diverse landscape of cybersecurity in the Asia-Pacific region, it is necessary to consider strategic approaches to building cyber resilience at the regional level.

Many countries are currently looking into fostering national resilience. However, with

the transnational nature of adverse cyber incidents and the rapid propagation of these incidents across the globe, cyber resilience becomes a matter of international solidarity and multilateral approaches. Indeed, such perspectives and approaches are critical and necessary for the protection of the globalised digital economy and society.

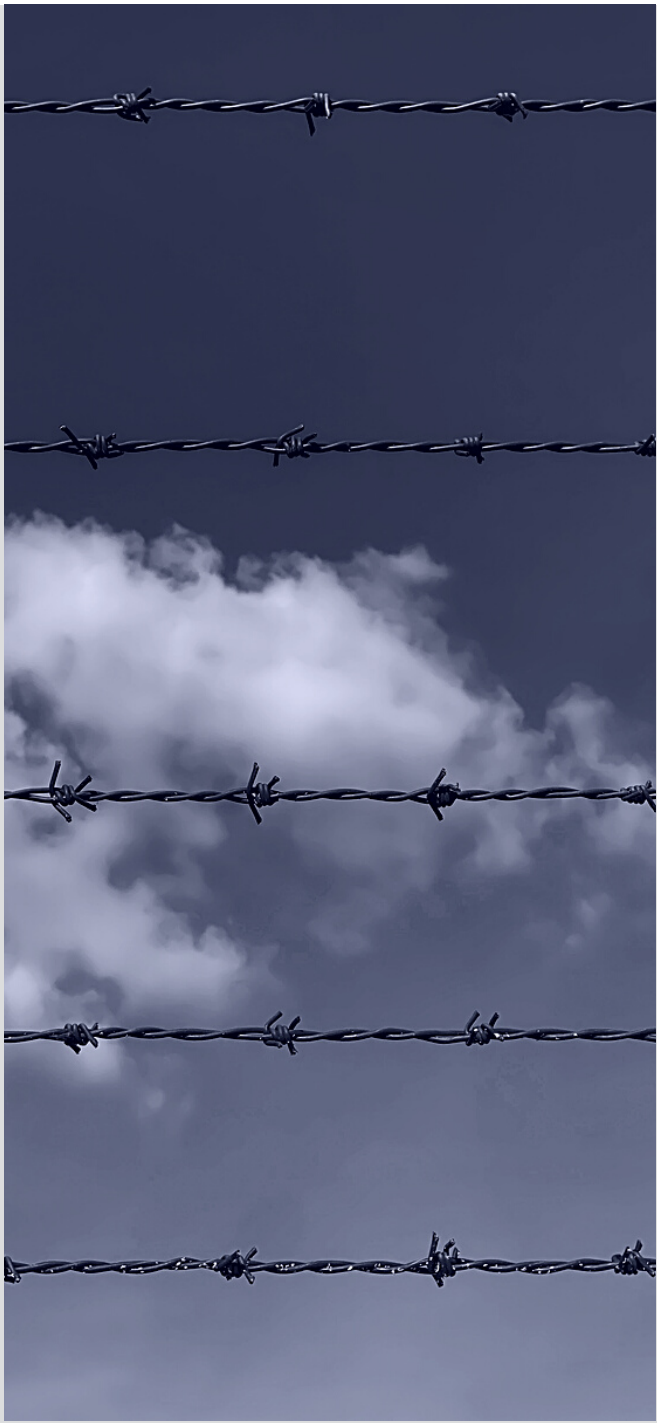
This study serves as both a starting point and problem analysis for discussing what the next steps would be for increasing cyber resilience within the Asia-Pacific and for operationalising the whole-of-society approach in national cybersecurity strategies.

NATIONAL CYBERSECURITY STRATEGIES

As a strategic document, a national cybersecurity strategy aligns the whole of government by defining strategic directions of cybersecurity efforts, conveys national priorities towards international partners, and provides a focus and a structure for discussions with stakeholders. It informs the formulation of national cybersecurity policy and regulations. As such, countries with national cybersecurity strategies that address key issues comprehensively have better avenues for operational and tactical efforts towards ensuring cybersecurity.

Cybersecurity strategies also influence and have an impact on the legal environment in the respective countries. Thus, specific provisions of these strategic documents may be assessed as preparatory and as precursors to respective legislative processes.

This study is interested in exploring the strategic-level enablement of cyber resilience in Asia-Pacific, as can be drawn from the national cybersecurity strategies of the various countries.



METHODOLOGY

RESEARCH QUESTIONS

This study is framed around two main lines of inquiry, to explore: the different approaches to cyber resilience as outlined in the national cybersecurity strategies, as well as the enablement of active participation of civil society stakeholders in the co-production of cyber resilience.

SELECTION OF NATIONAL CYBERSECURITY STRATEGIES

Not all countries in Asia-Pacific have an NCS . Among countries with no NCS, however, different blueprints that cover aspects of cybersecurity exist in the form of national digital policies, ICT masterplans, or e-governance masterplans. Other countries have legislative and regulatory provisions related to cybersecurity.

For this study, the NCS's of the following 14 Asia-Pacific nation-states are reviewed: Afghanistan (AFG), Australia (AUS), Bangladesh (BGL), China (CHN), India (IND), Japan (JPN), Malaysia (MYS), New Zealand (NZL), the Philippines (PHL), the Republic of Korea (hereafter referred to as 'South Korea') (SKR), Samoa (SAM), Singapore (SGP), Sri Lanka (SLK), and Vanuatu (VNT).

The countries are selected across levels of commitment to cybersecurity and cyber maturity (e.g., Global Cybersecurity Index,[11] The Australian Strategic Policy Institute's Asia-Pacific Cyber Maturity Metric),[12] and the overall achievement in its social and economic dimensions (e.g., UNDP's Human Development Index).[13]

The following databases are used to collect the NCS documents: ITU's cybersecurity strategy repository, United Nations Institute for Disarmament Research's cyber policy

portal, and North Atlantic Treaty Organisation's Cooperative Cyber Defence Centre of Excellence's (CCDCOE) cybersecurity strategy repository.

Aside from the NCS, other sources are consulted to understand countries' engagement in international discussions on cybersecurity, the national cybersecurity authorities, and the existence of national CERTs.

Table 1. *Asia-Pacific states across levels of commitment to cybersecurity, cyber maturity, and human development*

Country	GCI	ASPI	HDI
Afghanistan	Low	-	Low
Australia	High	equal 2nd of 25	Very high
Bangladesh	Medium	18th of 25	Medium
China	High	8th of 25	High
India	High	10th of 25	Medium
Japan	High	equal 2nd of 25	Very high
Malaysia	High	7th of 25	Very high
New Zealand	High	6th of 25	Very high
Philippines	Medium	15th of 25	High
Samoa	Medium	-	High
Singapore	High	4th of 25	Very high
South Korea	High	5th of 25	Very high
Sri Lanka	Medium	-	High
Vanuatu	Low	17th of 25	Medium

HEURISTICS

A template analysis approach was employed to analyse the NCS documents based on the following list of heuristics.

Table 2. *Themes used in the analysis of the national cybersecurity strategies*

No.	Cyber resilience aspects	Measures
1	Strategic objectives and guiding principles	Short- and long-term goals of the strategy which will be met by targeted actions and processes
2	Incorporation of resilience thinking	Mention of, definition of, and description of resilience, and implicit incorporation of resilience thinking
3	Cyber threats	Identified based on the nature and target of the threat
4	Stakeholders	Identified stakeholders, as well as their roles and responsibilities
5	Institutions coordinating cybersecurity in the country	The institutional actors involved in the governance of cybersecurity
6	Capacity-building	Awareness-raising and capacity-building activities for the general public and specific segments of the society
7	Programmes to improve incident management and response capabilities	Models/frameworks/metrics for assessing and enhancing cybersecurity capacity, including drills, exercise, information-sharing platforms, react-recovery plans, and early warning systems
8	National multi-stakeholder partnership in cybersecurity	Intra-state cooperation between different stakeholders
9	Participation in international partnership in cybersecurity	Ratified/acceded international treaty/agreement on cybersecurity, membership in international cybersecurity association/forum, or plan about any of the aforementioned measures
10	Vulnerable groups in the context of cybersecurity	Specific population groups that are vulnerable to cyber risks
11	Avenues through which civil society stakeholders can participate in the co-production of cybersecurity	Means for civil society stakeholders' participation across the processes of cybersecurity, including the development and evaluation of NCS, and the implementation of cybersecurity measures
12	Research and development in cybersecurity	Existing or planned research and development activities in cybersecurity-reated fields

LIMITATIONS OF RESEARCH

The following limitations of this research need to be noted and highlighted.

Firstly, the investigation of the cyber resilience strategies of the countries is based on the review of national cybersecurity strategies. The authors recognise that for some countries, national cybersecurity strategies are but one out of a suite of strategies related to the cyber domain within the country. Accordingly, there might be aspects of the national cybersecurity strategy that are further articulated in other related documents.

Secondly, national cybersecurity strategies are not living documents and are, therefore, not in sync with the reality of cyber resilience in many countries. The authors are aware of efforts across several countries to update their national cybersecurity strategies. Despite this limitation, the authors have noted the importance of national strategies for setting the national goals and agenda and therefore recognise the merit of undertaking this investigation at the strategic level, as opposed to tactical and operational levels.

Lastly, the research has relied on publicly available English versions of the national cybersecurity strategies. The authors recognise the challenges and limitations associated with translation between different languages. They also recognise that there might be strategy documents that are not publicly available from repositories consulted for this research.

CYBER RESILIENCE POSTURE IN ASIA-PACIFIC

STRATEGIC OBJECTIVES OF ASIA-PACIFIC COUNTRIES' CYBERSECURITY STRATEGY

The objectives of national cybersecurity strategies reflect the differences in national contexts (see Figure 1). Ideally, these objectives relate to the problems or challenges that drive the formulation or revision of NCS, met by targeted actions and processes, and presented with an evaluation framework to assess the accomplishments of the stated objectives.

RESILIENCE THINKING IN CYBERSECURITY STRATEGIES

Having a definition of cyber resilience is vital for operationalising the concept into strategic directions, processes, procedures, and evaluation frameworks. Some fundamental elements of cyber resilience could include identification of the resilient objects and resilience goals, risk assessment, adaptive management, effective communication and coordination, development of cyber-aware culture and cyber capabilities across all levels of governments and society, and incident exercises.

Except for China, Asia-Pacific countries under review mention the term 'resilience' in their NCS. Only Singapore provides a definition for 'cyber resilience'. Bangladesh, India, Japan, New Zealand, the Philippines, South Korea, and Sri Lanka provide a descriptive text to indicate what cyber resilience means to them. In the case of Afghanistan, Australia, Malaysia, Samoa, and Vanuatu, while the term 'resilience' is only mentioned with no definition nor description provided, resilience is still identified as a strategic objective.

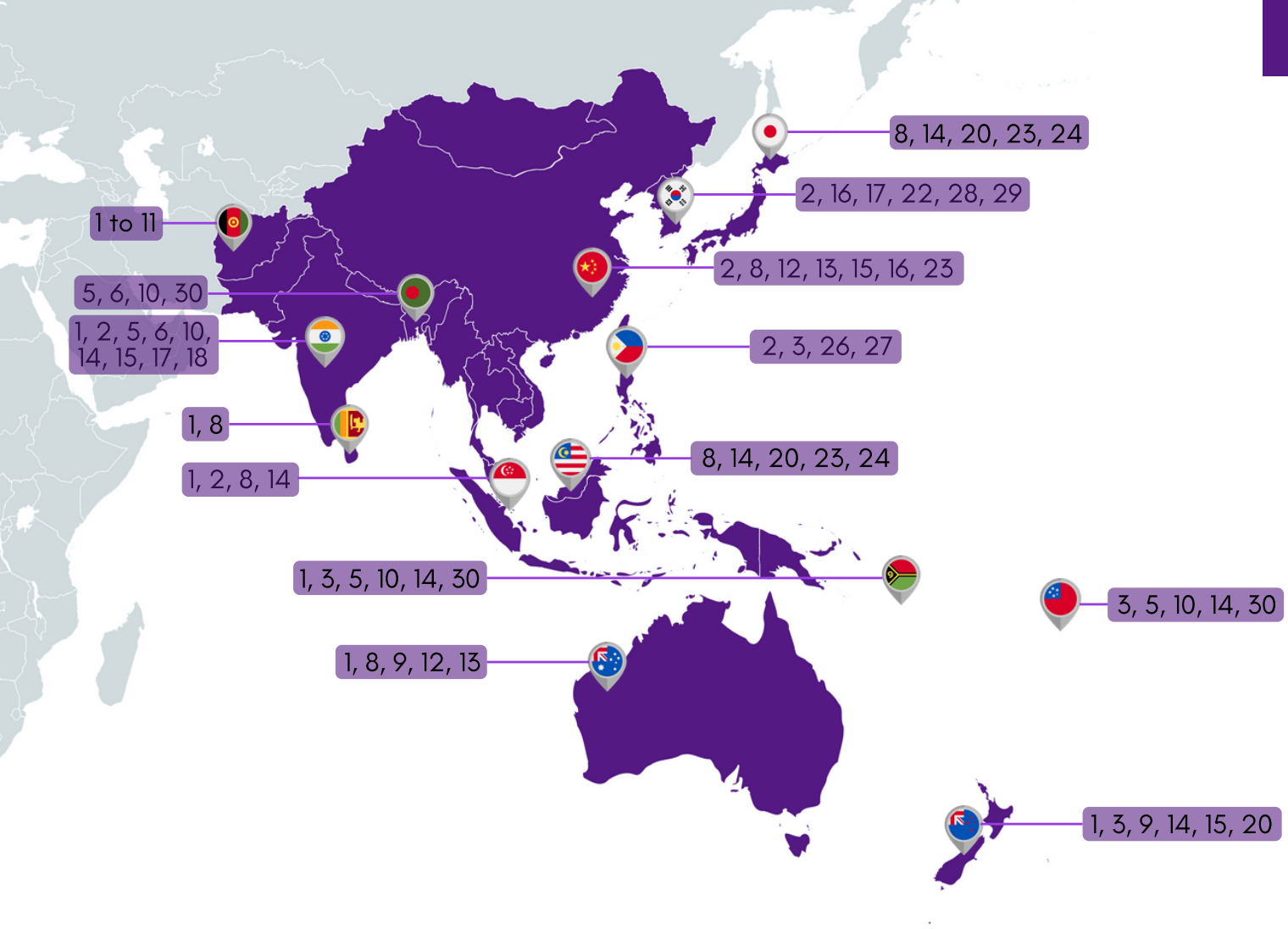


Figure 1. *Strategic objectives of Asia-Pacific states' national cybersecurity strategies*

1	Create a safe, secure, and resilient cyberspace	16	Establish/enhance cybersecurity governance
2	Protect the security of national data, information, and critical infrastructure	17	Build/improve capabilities to prevent and respond to cyber threats
3	Enhance cybersecurity awareness and the capability to protect oneself online	18	Reduce vulnerabilities and minimize damage from cyberattacks
4	Protect vulnerable groups in the cyberspace	19	Develop security technologies that address national security requirements
5	Establish/strengthen the legislative and regulatory framework for cybersecurity	20	Capacity-building to prepare a workforce of cybersecurity professionals
6	Establish/strengthen national partnership in cybersecurity	21	Establish incentive mechanisms to support the adoption of standard cybersecurity practices and processes
7	Network and systems resilience to cyberattacks	22	Foster a culture of cybersecurity
8	Create a cybersecurity ecosystem that supports a sustainable value-creation for economic growth and prosperity	23	Safeguard national security and social stability
9	Cyber smart nation: thriving in the digital age	24	Promote research and development in cybersecurity
10	Establish and implement a framework for technical cybersecurity measures	25	Develop a framework for compliance and enforcement of cybersecurity measures
11	Establish/strengthen national partnership in cybersecurity	26	Make government information environment secure
12	Strengthen cybersecurity capability	27	Make businesses secure
13	Defend sovereignty in the cyberspace	28	Build homegrown cybersecurity industry
14	Contribute to strengthening international collaboration in cybersecurity	29	Lead international cooperation in cybersecurity
15	Establish/strengthen mechanisms for effective prevention, investigation, and prosecution of cybercrime	30	Establish/improve cybersecurity organisational and coordination structures

Table 3. *Incorporation of resilience thinking in Asia-Pacific NCS*

Country	Incorporation of resilience		The resilience of...
AFG	Mentioned, but no explicit definition or description		the resilience of the cyberspace ecosystem
AUS	Mentioned, but no explicit definition or description		the resilience of the networks, systems, and the national resilience
BGL	Described	(involves) timely identification, communication, and recovery from cybersecurity events and weaknesses affecting critical information infrastructure	the resilience of critical infrastructure
CHN	No mention, definition, nor description		
IND	Described	(involves) rapid identification, information exchange, investigation, and coordinated response, and remediation for mitigating the damage caused by malicious cyberspace activity	the resilience of the cyberspace, critical information infrastructure, and systems
JPN	Described	(involves) adoption of 'mission assurance' approach to reducing risks to an acceptable level and ensure the safe and continuous operations and services	the national resilience and resilience against cyber-attacks
MYS	Mentioned, but no explicit definition or description		the resilience of the critical national information infrastructure
NZL	Mentioned, but no explicit definition or description	(involves) resistance against, and protection from cyber threats, and the ability to respond to incidents across system	the resilience of the nation-state in cyberspace, the significant infrastructures, and the public sector; and among different groups of people
PHL	Described	The objective (of the Resilient Enterprise State) is predictive and mission-focused to isolate and contain damage, secure supply chains, and protect critical critical infrastructure to continue operation through cyber-attacks	the resilience of the nation-state and the critical information infrastructures
SAM	Mentioned, but no explicit definition or description		the resilience of the cyberspace
SGP	Defined	Cyber resilience is the ability of the critical information infrastructures to withstand cyber-attacks, allowing them to continue operating under the toughest conditions and recover quickly after a disruption	the physical and cyber resilience
SKR	Described	Strengthen security and resilience of the national core infrastructure against cyber-attacks to ensure continuous provision of critical services	the resilience of the nation's core infrastructure and critical services
SLK	Described	(includes) detection, prevention, response, and recovery capabilities	the resilience of the cybersecurity ecosystem and the critical infrastructure
VNT	Mentioned, but no explicit definition or description		the resilience of the cyberspace and of the ICT infrastructure

It can be observed from Table 3 that countries focus on different aspects of cyber resilience. However, most focus on the resilience of the cyberspace and the critical infrastructure.

While countries that provide a description of resilience thinking within the cyber domain indicate what cyber resilience entails, the Philippines and Singapore are more elaborate than other countries in operationalising cyber resilience into cyber resilience aspects in the NCS. The said aspects include the desired state of resilience; measurement instruments and evaluation mechanisms to assess cybersecurity and, by extension cyber resilience maturity; as well as cyber incident exercises. Meanwhile, in implicitly describing resilience, New Zealand emphasises the need to focus on the wider system beyond significant infrastructures to achieve resilience.

Countries such as Afghanistan, India, Japan, and Malaysia mandate a requirement of developing and implementing a business continuity management plan as a strategy to build a culture of resilience. Meanwhile, Japan and South Korea seek to enable continuous operation and provision of critical services in the face of diverse cyber-attacks — an approach which Japan refers to as 'mission assurance'.

CYBERSECURITY INCIDENT EXERCISES

Cybersecurity incident exercises can help to facilitate the testing of existing emergency plans, improve familiarity with crisis response, identify areas for improvement in the case of actual adverse cyber events, and increase cooperation between different sectors.

Countries under review recognise the importance of cybersecurity incident exercises for improving preparedness, response, and recovery efforts. India and the Philippines mandate the organisation of regular cybersecurity drills at different levels. Afghanistan makes it imperative for its CERT to participate in cyber drills with regional CERTs. Japan runs cybersecurity exercises among stakeholders of various sizes across the public and private sectors. Singapore's Cybersecurity Agency (CSA) runs a multi-sector exercise. South Korea conducts nation-wide public-private-military joint drills to enhance response capabilities against a cyber crisis. Bangladesh, China, and Malaysia conduct assessment to their cybersecurity posture. Further, Australia, Japan, Singapore, and South Korea have already participated in joint cybersecurity drills with international partners.

Related to the exercises are cybersecurity metrics. Cybersecurity metrics are references that are used for assessing the various aspects of cyber capabilities, evaluate readiness, monitor progress, and improve cybersecurity measures. Only several countries specifically identify these metrics.

Singapore uses the Readiness Maturity Index (RMI) framework to assess the readiness of

critical information infrastructure in terms of their capabilities for risk-based mitigation, early detection of threats, and robustness of the response measures. The framework facilitates the development of action plans to improve governance and procedures. Singapore also conducts a cybersecurity readiness maturity assessment which enables agencies and CII operators to identify areas for improvement on cybersecurity.

The Philippines has a cybersecurity maturity model which enables it to periodically assess their cyber capacity and provides a path forward for improvement. The Philippines' cybersecurity model defines the state of 'Resilient Enterprise' and the state of 'Reactive and Manual' as two ends of a continuum. Australia, Bangladesh, China, and Malaysia indicate the existence of a cybersecurity readiness measure.

Sri Lanka and Samoa are in the process of developing cybersecurity metrics. Meanwhile, Afghanistan, India, Japan, New Zealand, South Korea, and Vanuatu do not identify the existence of any of these measurement instruments or plan to devise them.

WHOLE-OF-SOCIETY POSTURE IN CYBERSECURITY STRATEGIES

The needs and roles of civil society stakeholders within the domain of cybersecurity and cyber resilience have traditionally been neglected in dominant cybersecurity discourse.[14]

In this study, the incorporation of a whole-of-society posture is assessed from the recognition of the role and responsibilities of civil society stakeholders in the NCS, and the identification of means for their participation in the co-production of cyber resilience. To some extent, the provision of these means is in line with the positioning of citizens as 'active agents' in cyber resilience who are expected to 'conduct the absorption and recovery action in an autonomous manner'.[7]

Civil society stakeholders are regarded as comprising individual citizens and third-sector organisations. Meanwhile, co-production of cyber resilience can be seen as a continuum of participatory activity. On one end is prevention measures, which traditionally include installation of software, cyber hygiene practices, and responsible online behavior, which are usually promoted by the state. On the other end is unilateral cyber resilience activities to police cyberspace and counteract cybercriminals, which could be initiated by civil society stakeholders themselves or facilitated by the state.

HUMANS AS ATTACK VECTORS

Cyber threats identified in the NCS can be classified based on the nature or source of the threat (i.e., natural hazards, institutional threats, and civilian attacks), the target of the threat (i.e., physical assets, civilian, or institutions), or attack vector, i.e., technological assets (physical assets and network), digital assets (e.g., digital data and online accounts), and humans.

From the review, only Afghanistan, China, and Malaysia do not identify individual-level cyber threats. Aside from different forms of social engineering and fraud, specific cyber threats targeting individuals are identified by Sri Lanka (i.e., revenge porn), Samoa (i.e., access to pornographic materials), and Vanuatu (i.e., child-specific cyber threats).

EFFECTIVE COMMUNICATION AND CAPACITY-BUILDING FOR THE PUBLIC AT LARGE

Cyber resilience relies on a baseline awareness level of the public, which contributes to the overall societal preparedness. Articulating the cybersecurity risk landscape in a comprehensive and broadly accessible way is a necessary first step towards managing and mitigating the associated risks at a societal level.

Further, with individuals identified as one of the significant attack vectors, there is a need for capacity-building measures that enhance individual resilience and capabilities that enable individuals to protect themselves and mitigate cyber risks.

Cybersecurity awareness-raising activities organised in countries under review range from setting up dedicated online platforms or using existing communication platforms for information-sharing, to organising public awareness campaigns.

Among the countries that specifically identify activities targeted at the public at large, Singapore provides the most details of its programmes. Singapore's NCS mentions at least five programmes — Community Safety and Security Programmes, Public Cyber-Outreach & Resilience Programme (PCORP), Total Defence, Let's Stand Together, and Cyber Security Awareness Alliance — to provide cybersecurity awareness, readiness, and basic skills to the general public.

In terms of self-help cybersecurity tools, Australia has Stay Smart Online and SCAMwatch, Singapore has Scam Alert, and South Korea has a 'Public Notification on Information Security' system. Through these platforms, cyber hygiene practices for individual citizens are promoted.

Except for Samoa, which is still in the process of establishing its CERT, countries under review also utilise the online platforms of CERT for communicating cybersecurity-related information to the public.

VULNERABLE GROUPS

The identification of groups that are vulnerable to cyber risks is useful to address their specific cybersecurity challenges and provide the support that they need. Except for India, Malaysia, and South Korea, countries identify groups that are vulnerable to cyber risks. However, not all of those countries identify interventions to assist the identified vulnerable groups.

Children and young people, and women are groups that are identified the most in the NCS. Australia established specialised entities that provide information and resources to help children and young people enjoy safe online experiences.

Afghanistan, Samoa, and Vanuatu mandate the development of Child Online Protection Policy to promote and implement precaution and protection of children, and the establishment of a working group comprising stakeholders from the private, public, and third sectors to work on child online protection-related issues.

Bangladesh engages civil society in outreach to children and individual users. China makes the protection of children online imperative while Japan mandates the promotion of moral education alongside the provision of cybersecurity education and ICT skills to youth due to the rise in cybercrime perpetrated by young people.

Other vulnerable groups identified in the NCS include tourists (Samoa), rural and semi-urban citizens, elderly communities (New Zealand, Sri Lanka), and small and medium-sized business owners (Australia, Japan, New Zealand, the Philippines, Singapore, Sri Lanka).

Table 4. *Vulnerable groups identified in the national cybersecurity strategies*

Countries	Women	Children and young people	Rural communities	SME owners	Others
AFG		●			
AUS	●	●		●	
BGL		●			
CHN		●			
IND					
JPN				●	
MYS					
NZL		●		●	●
PHL		●		●	
SAM		●			●
SGP		●		●	
SKR				●	
SLK	●	●	●		●
VNT		●			

CO-PRODUCTION OF CYBER RESILIENCE WITH CIVIL SOCIETY STAKEHOLDERS

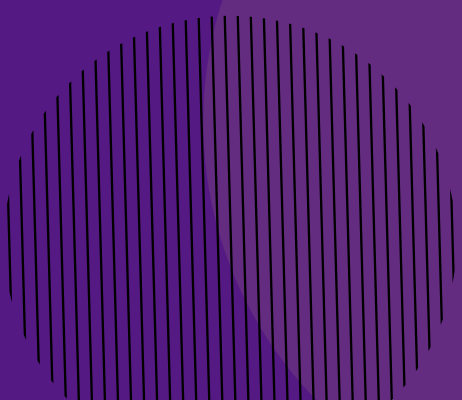
In all countries under review, cybersecurity is regarded as a shared responsibility to which all stakeholders need to contribute. Citizens are encouraged to independently foster an understanding of cybersecurity issues and the impacts of adverse cyber events, perform cyber hygiene practices to secure their cyberspace-linked systems and technologies, and participate in cybersecurity awareness-raising programmes.

Meanwhile, the Philippines, while acknowledging the government's limitation to patrol the cyber environment, calls for the participation of the cyber community in conducting neighbourhood watch against malicious individuals prowling the Internet.

Except for Samoa, countries under review designate the online platforms of national CERTs as a portal to receive and handle cyber incident reporting. Other than that, no other means of co-production are explicitly identified in the NCS. In most NCS, the affordance of the CERTs' online platforms to support civil society in the co-production of cyber resilience is not even identified.

Only few countries under review explicitly assign third-sector organisations with specific roles in the overall processes of developing, implementing, and evaluating NCS. Aside from the general call to participate in the information-sharing network on cyber vulnerabilities, threats, and attacks and in raising public awareness on cybersecurity issues and cybercrime prevention, several countries encourage contributions by third-sector organisations in specific areas: Bangladesh – in evaluating cybercrime law, China – in strengthening the protection of young people online and building a cyberspace governance platform, and Singapore – in raising cybercrime prevention awareness.

COUNTRY PROFILES



AFGHANISTAN

HDI: LOW
ASPI INDEX: N/A
GCI: LOW

STRATEGY STATS
PUBLICATION YEAR: 2014
AVAILABLE AT: ITU, UNIDIR, CCDCOE

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

The increasing use of Information and Communication Technologies (ICTs) in the public sector organisations motivated the formulation of Afghanistan's NCS.

Afghanistan aims to establish and achieve a safe, secure, and resilient cyberspace. To achieve this, it puts forward strategies to establish a cybersecurity regulatory framework and enhance CERT capabilities, strengthen the security of e-government systems, safeguard data privacy, promote public-private partnership, facilitate training for cybersecurity professionals, and enter into international cooperations in cybersecurity.

It recognises that the vulnerabilities inherent in ICTs may cause a denial of service or abuse of service attacks, resulting in large scale economic losses, disturbance of public order, and threats to national security.

PERCEIVED THREATS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Afghanistan identifies attacks on information systems and data, and specifically denial of service attacks, as the main cyber threats to the country.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

The vision of Afghanistan's NCS is towards establishing a safe, secure, and resilient cyberspace. Therefore, resilience in Afghanistan's NCS refers to the resilience of the cyberspace ecosystem. Establishing a resilient cyber ecosystem is one of the key strategies advanced to achieve its cybersecurity goals.

There is no explicit definition or description of what a resilient ecosystem means. However, further elaboration of the strategy implies that a resilient ecosystem is enabled through strengthening the governance of cyber and information security domains; encouraging both public and private sectors to mainstream cybersecurity efforts in their respective organisations; supporting the Afghanistan CERT (AFCERT) in its work to serve its

constituency; and ensuring the quality of IT products used within the government bodies.

Afghanistan encourages both public and private sectors to have information security policies that align with their business profile and services in compliance with international standards and best practices. Among the requirements that need to be considered in the policies are business continuity and disaster recovery plans.

Despite the lack of elaboration on the use of the term 'disaster' in the NCS, it could be inferred that Afghanistan considers cybersecurity risks as disaster risks and successful large-scale cyber-attacks as national disasters. This perspective aligns with the Sendai Framework's framing of technological risks as significant disaster risks.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Both the private and public sectors are encouraged to assign a senior manager as the Chief Security Officer (CSO) with the responsibility to lead cybersecurity initiatives in their respective organisations; develop information security policies aligned with their organisational profile and services, and in compliance with international standard; and dedicate a budget for cybersecurity activities and measures.

Stakeholders comprising government Chief Information Officers (CIOs), ICT heads, the private sector, and academia participated in the development of the national cybersecurity strategy.

While identified as one of the beneficiaries of the secure cyberspace, citizens are not given a specific role in the NCS.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Professional cybersecurity training programmes are designed for cybersecurity professionals in the public and private sectors. Meanwhile, the national CERT, AFCERT is mandated to provide cybersecurity-related awareness activities to all government and non-government agencies. There are also capacity-building programmes that are targeted at government and private sector stakeholders.

Cyber-related awareness activities are also provided to all government and non-government agencies through the Network Operation Center (NOC) in the form of workshops, seminars, and various other activities.

Meanwhile, to enhance the AFCERT's capabilities and improve its performance, cybersecurity exercises and cyber drills with regional CERTs, as well as advanced training and capacity-building programmes are provided for AFCERT.

The government also plans to engage with donor communities to coordinate training and capacity-building programmes on cybersecurity, as well as to secure scholarship opportunities for studies in the field of information security.

CYBER CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

In terms of cybersecurity education, the NCS does not mention specific capacity-building policies and programmes targeted at learning institutions, particularly with regard to incorporating cybersecurity education into the school curriculum.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

The NCS does not mention specific capacity-building measures targeted at the general public.

PROGRAMMES INTENDED TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

The government mandates AFCERT to participate in conducting cybersecurity exercises and cyber drills with regional CERTs. It also mandates periodic risk assessment and security standard compliance of the critical information infrastructure.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Afghanistan does not mention any cybersecurity research and development activities in the NCS.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The Information Systems Security Directorate (ISSD) of Ministry of Communications and Information Technology (MCIT) is the authority responsible for coordinating the cyber and information security efforts in Afghanistan, including developing a framework for cyber and information security. When ISSD reaches a certain maturity level, it is expected to become an independent entity within the government structure to ensure its full integrity.

MCIT established AFCERT. AFCERT's mandate is to be the focal point of cyber incident response and computer crime investigation within the government and private sectors. AFCERT is tasked with providing awareness and capacity-building to its constituency, coordinate with law enforcement and regional CERTs regarding cybercrime investigation, establish provincial CERTs, and operate a 24/7 incident investigation and response service.

The National Cybersecurity Strategy of Afghanistan (NCSA) Committee, chaired by Information Systems Security Directorate of MCIT and comprising several government entities, is responsible for developing Afghanistan's NCS.

MULTI-STAKEHOLDER PARTNERSHIPS FOR CYBERSECURITY IN THE COUNTRY

Public-private partnership is fostered in the implementation of the cybersecurity action plan, particularly towards the protection of critical information infrastructure.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

There is no specific mention of international agreements or partnerships that Afghanistan is currently engaged in. However, it plans to engage and coordinate training and capacity-building programmes with donor communities (World Bank, ITU, USAID) and secure funds for information security training, seminars and workshops for cybersecurity personnel within the government and private sectors.

MCIT plans to engage with international organisations in efforts to counter cybercrime. It also seeks to develop and enhance multilateral relationships in cybersecurity with other countries within the region through collaborations between CERTs and law enforcements. Currently, AFCERT is not a member of the Forum of Incident Response and Security Teams (FIRST) or Asia-Pacific CERT (AP-CERT). Further, despite being a member of the Organisation of Islamic Cooperation (OIC), AFCERT does not have a membership in OIC-CERT.

Currently, Afghanistan has membership in the UN, ITU, and INTERPOL.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

Afghanistan's NCS makes no point about available avenues for engaging civil society stakeholders in the effort to build and maintain cybersecurity and cyber resilience.

Moreover, AFCERT's online portal cannot be used to report cyber incidents as AFCERT focuses on providing assistance to the private and public sectors.

AUSTRALIA

HDI: VERY HIGH
ASPI INDEX: EQUAL 2ND OF 25
GCI: HIGH

STRATEGY STATS
PUBLICATION YEAR: 2016*
AVAILABLE AT: ITU, UNIDIR, CCDCOE

*AUSTRALIA LAUNCHED AN UPDATED STRATEGY IN AUGUST 2020

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

Australia aims to advance its national cyber partnership; strengthen its cyber defences; contribute to global efforts to creating an open, free, and secure Internet; foster growth and innovation in cybersecurity; and build its cybersecurity capacity to prepare for a smart future.

These strategic goals are informed by the experience of encountering cyber-attacks that have affected the public and private sectors, as well as the public at large and the Snowden disclosures.

Australia's 2016 NCS formulation is guided by adherence to the norms of a free, open, and secure Internet. It is also in response to the need to boost its cybersecurity capability in alignment with the release of the 2015 National Innovation and Science Agenda, the Defence Industry Plan, and the 2016 Defence White Paper.

PERCEIVED THREATS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Australia identifies several cyber threats across attack vectors: cyber espionage, spearfishing, illegal modification of data, malware, social engineering, ransomware, and online fraud. It does not identify any threats deriving from natural hazards.

Australia also considers cyber threats stemming from the increasing connectedness of devices to the Internet of Things.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Resilience in Australia NCS refers to the resilience of networks, systems, and national resilience.

One of Australia's national cybersecurity goals is for its networks and systems to be hard to compromise and resilient to cyber-attacks. There is no explicit definition or description of what being resilient means to them. However, from the priority actions operationalised to achieve the goal, it can be inferred that resilience is to be achieved through joint efforts by stakeholders, i.e. sustained sharing of cybersecurity-related

information to build collective understanding about cyber threats, voluntary cybersecurity assessment by stakeholders in their respective organisations using guidelines co-designed with the private sector, and joint cybersecurity response exercise, as well as through boosting the capacity of the cybersecurity coordinating agency, supporting government agencies to improve their cybersecurity, and supporting small businesses.

Australia identifies the pooling of cybersecurity resources as an efficient way to develop quick responses to compromises and to build national resilience.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

The research community participates in the cybersecurity meetings that inform the shaping of the national cybersecurity agenda and in co-designing the national guidelines on good cybersecurity practice that all organisations can use. Along with the government and the private sectors, the research community works in improving the cybersecurity skills pipeline by ensuring that cybersecurity skills are incorporated into the school curriculum at all levels.

The private sector and the government establish cyber threats-sharing centres and an online cyber threat sharing portal.

Organisations in the public and private sectors are demanded to improve their cyber defences.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Specialised professional training in cybersecurity is targeted at law enforcement officers in the Australian Crime Commission and the Australian Federal Police, and executives in the private sector.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

In terms of education programmes that are targeted at students, the government engages with the research and academic community to improve cybersecurity education at all levels of the education system while ensuring that the school curriculum supports the provision of workforce with cybersecurity skills.

The government engages with the academic and research community and the private sector to establish academic centres of cybersecurity excellence in universities, adjust school curriculum to support the cybersecurity skills pipeline, raise the national cybersecurity awareness through sustained awareness initiatives and education campaigns, and hold cybersecurity competition for students.

To promote cybersecurity careers among tertiary students and help generate a sustained national pipeline of cybersecurity professionals, Australia holds an annual cybersecurity competition, the Cyber Security Challenge Australia. Besides, cybersecurity apprenticeship and scholarship to study technology courses are offered.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

Cybersecurity awareness-raising efforts are organised through sustained awareness initiatives and education campaigns, community education, and the provision of an online platform that provides useful advice to the public regarding the protection of their personal and financial information online (Stay Smart Online).

The government also operates SCAMwatch, a portal which provides information to individuals and businesses on how to identify and report scams.

PROGRAMMES INTENDED TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

Australia engages different stakeholders in co-designing cybersecurity governance 'health checks' and in conducting joint cybersecurity exercise.

In 2016, Australia participated in CyberStorm, an international cybersecurity exercise programme led by the United States.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Australia aims to invest in research to better understand the costs of malicious cyber activity to the Australian economy and ensure that organisations have local information to inform their investment and risk management decisions for cybersecurity. The country mentions several existing research and development activities in the NCS.

The government collaborates with other stakeholders to establish centres of cyber security excellence in universities and an industry-led Cyber Security Growth Centre which will provide strategic coordination of a national cyber security innovation network and drive investment in cybersecurity innovation in Australia.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The Australian Cyber Security Centre (ACSC), based within the Australian Signals Directorate (ASD) leads the national cybersecurity efforts. ACSC brings together the Australian government's cybersecurity capabilities to share cybersecurity threat information and combat cybersecurity threats.

The Australian Cybercrime Online Reporting Network (ACORN) provided advice on how to recognise and avoid cybercrime, as well as alerts of current cyber threats, and facilitated cyber incident reporting. Currently, these functions are delivered by ReportCyber.

Hosted by ACSC, Australia's national CERT (CERT Australia) partners with businesses and advises on cyber security threats to the owners and operators of Australia's critical infrastructure.

Meanwhile, AusCERT is a membership-based, independent, self-funded, not-for-profit CERT that is based in the University of Queensland. It provides a range of services, including cyber incident management, sensitive information alert, and

cybersecurity capacity-building. AusCERT also contributes to building a partnership between Australia with other international CERTs and representing Australia in international cybersecurity forums. AusCERT partners with businesses and critical infrastructure owners and operators and advises them on cybersecurity threats.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

Multi-stakeholder partnership in cybersecurity involving the government, businesses, and research community manifest in a variety of forms.

The collaboration between the government and the private sector is mandated in the sharing of information on threats and responses through joint cyber threat-sharing centres in key capital cities and an online cyber threat-sharing portal.

Australia has Australian Cyber Security Research Institute (ACSRI) which is a collaborative network that coordinates strategic research and education effort between government agencies, the private sector, and researchers. There is also the Australian Internet Security Initiative (AISI), a public-private partnership run by ACSC that helps to reduce malware infections and service vulnerabilities occurring on Australian Internet protocol (IP) address ranges.

Through the data innovation group Data61, representatives from industries, government, and academia partner to propel cybersecurity innovation, with a particular focus on support for cybersecurity start-ups and technical capability development.

Further, both the annual Cyber Security Challenge Australia and the Cyber Security Growth Centre embody the collaboration between Australian government with the private sector and the academic and research communities.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

Australia mentions several international partnerships that it has engaged in, including chairing the United Nations Group of Governmental Experts, participating in the 2015 ASEAN Regional Forum (ARF) cyber work plan, joining the Freedom Online Coalition to advance internet freedom, collaborating with policing agencies in the Indo-Pacific region on training and capacity-building initiatives to counter cybercrime, and being a lead partner in the East Asia Summit and Asia-Pacific Economic Cooperation (APEC)'s efforts to counter online extremism and combat online terrorist propaganda.

Since 2013, Australia has acceded to the Council of Europe Convention on Cybercrime (Budapest Convention). It is also a member of Pacific Cyber Security Operational Network (PaCSON), ITU, the UN, INTERPOL, and the Commonwealth of Nations. In 2015, Australia became a founding partner of the Global Forum on Cyber Expertise.

CERT Australia is not part of FIRST or AP-CERT while AusCERT has membership in both forums.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Children and young people, women, and MSMEs are identified as vulnerable in the NCS.

Australia established the Office of the Children's eSafety Commissioner to provide information and resources to help guide children and young people towards safe, enjoyable experiences online. It also provides a complaints system to assist children who experience serious cyberbullying.

To help small- and medium-sized business owners set up their cybersecurity measures, the Australian government co-design an online cyber threat-sharing portal with the private sector. The government also provides support for small businesses to have their cybersecurity tested by certified practitioners.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

Australia has ReportCyber (previously ACORN) which facilitates cybercrime reporting including by individuals. It also has a cybersecurity hotline.

BANGLADESH

HDI: MEDIUM
ASPI INDEX: 18TH OF 25
GCI: MEDIUM

STRATEGY STATS
PUBLICATION DATE: 2014
AVAILABLE AT: ITU, UNIDIR, CCDCOE

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

Bangladesh aims to create a safe, secure, and resilient information infrastructure. It sees the management of cybersecurity as the way to ensure security and economic vitality. The Strategy serves to fulfill the country's need for a coherent vision for the governance of national cybersecurity efforts as well as guidance for international cooperation in cybersecurity.

The development of Bangladesh's NCS is informed by concern over uncertainty about cyber risks and vulnerabilities stemming from increasing complexity and interconnectivity of technology that is used to support critical systems.

PERCEIVED THREATS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Bangladesh identifies several cyber threats across attack vectors: cyber espionage targeting government and private enterprises, silent surveillance on a state's security posture, phishing to facilitate credit card fraud, and attacks on critical infrastructure. It also identifies threats in relations to cyber vulnerabilities, such as disruption during patching, poor technical design, and the exploitation of known but unfixed vulnerabilities in the cybersecurity strategy.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Resilience in Bangladesh's NCS refers to the resilience of critical infrastructure.

The goal of Bangladesh's NCS is creating a safe, secure, and resilient critical national information infrastructure for the economy and society.

There is no explicit definition or description of what resilience means to them. However, in the elaboration of Action 3 (i.e. National Incident Management Capacity) under Priority 3 (i.e. Organisation Structures), Bangladesh identifies timely identification, communication, and recovery from cybersecurity events and weaknesses affecting critical information infrastructure, and the collaboration with the private sector as important mitigation strategies against malicious cyberspace activity.

As part of its key actions to enhance the national cyber incident management capacity, Bangladesh encourages the development of business continuity and disaster recovery capacity through the collaboration between the government and the private sector.

Despite no elaboration on why the term 'disaster' is used in the NCS, it could be inferred that Bangladesh considers risks deriving from the field of cybersecurity as disaster risk and that successful large-scale cyber-attacks as disasters. This is in line with the Sendai Framework's framing of technological risks as one of the disaster risks.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Bangladesh recognises that critical information infrastructure protection is everyone's responsibility. It creates a mechanism for the sharing of information on cyber-attacks, threats, and vulnerabilities between non-governmental bodies locally and globally.

Bangladesh mandates for the cybercrime law to evaluated by non-governmental organisations, academics, citizens, willing foreign governments, and the private sector.

Bangladesh encourages the private sector to build their cybersecurity culture, share the state of their cybersecurity capacity, and support professional cybersecurity certifications.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Professional cybersecurity training programmes are designed for cybersecurity professionals at law enforcement agencies and the private sector.

Bangladesh seeks support from the private sector for organising professional cybersecurity certifications and for supporting the programmes in addressing the shortage of cybersecurity professionals.

To increase the capability of cybersecurity professionals, Bangladesh seeks to create a continuum of cybersecurity positions, identify cybersecurity certification programmes, invest in cybersecurity education and research, and coordinate cybersecurity training.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

Bangladesh plans to include cybersecurity awareness to the national education curriculum.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

There is no specific capacity-building measure targeted at the general public mentioned in the NCS. However, the NCS mentions the promotion of cybersecurity skills, training, and awareness as a sub-activity that the government would address.

PROGRAMMES INTENDED TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

Bangladesh conducts national vulnerability assessments to understand the potential consequences of cyber threats and vulnerabilities.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Bangladesh plans to foster innovation in cybersecurity to develop long-term cybersecurity solutions. The country also seeks to invest in cybersecurity education, research, and development.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

Existing cybersecurity authorities are not mentioned in the NCS. However, from UNIDIR's database, it can be understood that the Information & Communication Technology Division under the Ministry of Posts, Telecommunications and Information Technology is responsible for coordinating Bangladesh' cybersecurity affairs. Under the same ministry, Bangladesh Computer Council (BCC) is responsible to formulate national ICT strategy and policy and create related standards and specifications.

The NCS proposes the establishment of the National Cybersecurity Council to be the focal point for coordinating cybersecurity efforts and to lead the collaboration between the government institutions with industry. The Council will be responsible for developing a national plan for securing critical infrastructure and services, providing strategic advice and processes for managing cybersecurity programmes, and providing integrated security advice.

The NCS also mentions that Bangladesh plans to make a Cyber Warning and Information Network at Cybersecurity Council.

There are two officially recognised computer incident/emergency response teams in Bangladesh, i.e. Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) which was established in 2016 and bdCERT, which was established in 2007. Under the Bangladesh government, BGD e-GOV CIRT is acting as the national CIRT which is responsible for receiving, reviewing, and responding to computer security incidents and activities, and works with various government units, critical infrastructure operators, law enforcement agencies, academia, and civil society. bdCERT, on the other hand, is an independent CERT that provides emergency response services to its members and the wider computer network community, including government, business, and academic organisations.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

Public-private partnership in cybersecurity is encouraged in the implementation of cybersecurity initiatives and policies, the development of national continuity and contingency plans, the development of new legislation and regulation on cybersecurity, and the provision of input for the government's participation in international discussions that shape the policies on issues related to cybersecurity.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

There is no specific mention of international agreements or partnerships that Bangladesh is engaged in. However, Bangladesh encourages government officials to participate in international cooperation, dialogue, and coordination activities focusing on cybersecurity.

There is also no mention of international fora or associations that Bangladesh is currently part of. However, it seeks to support the government to participate in international cooperation, dialogue, and coordination activities focusing on cybersecurity.

From relevant sources, it can be found that Bangladesh has membership in ITU, the UN, and INTERPOL. Both BGD e-Gov CIRT and bdCERT has membership in AP-CERT and OIC-CERT, but only BGD e-GOV has membership in FIRST. As a Commonwealth Member State, Bangladesh supports and participates in a variety of cybersecurity-related initiatives by the Commonwealth of Nations.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Bangladesh identifies children as groups vulnerable to sexual trafficking. While there is no specific intervention identified in the cybersecurity strategy to address this issue, Bangladesh recognises the importance of engaging civil society in outreach to children in the effort of building the cybersecurity culture.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

In the NCS, the participation of non-governmental organisations and citizens in evaluating the cybercrime law is encouraged.

Bangladesh mandates for the cybercrime law to be evaluated by non-governmental organisations, academics, unaffiliated interested citizens, willing foreign governments, and the private sector. It also mandates that all critical infrastructure owners develop a mechanism to share information about cyber-attacks, threats, and vulnerabilities with the public and non-governmental bodies locally and globally.

In the effort of building the national culture of cybersecurity, Bangladesh engages with civil society in outreach to children and individual users.

In terms of cybersecurity incident reporting, the BGD e-GOV CIRT online platform facilitates such reporting by individuals. However, this portal is not identified in the cybersecurity strategy.

CHINA

HDI: HIGH
ASPI INDEX: 8TH OF 25
GCI: HIGH

STRATEGY STATS
PUBLICATION YEAR: 2015
AVAILABLE AT: ITU, UNIDIR, CCDCOE

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

China emphasises the motivation to maintain the country's sovereignty and security, and the aspiration to build a community of 'common destiny' in cyberspace. In the NCS, it regards a strong cyber power as the key to realising the 'Two Centenaries' goal of the Communist Party of China (CPC). The goal comprises becoming a moderately well-off society by 2021 and a fully developed society by 2049, and to achieving the 'Chinese Dream' of rejuvenation of the Chinese nation.

The formulation of China's NCS is guided by the interest in building cyberspace with common destiny and safeguarding national sovereignty, security, and development, as well as refusal to cyber hegemonies. It is also driven by the need to ensure 'the public's right to know, right to participate, right to express opinions', as well as to respect their personal privacy.

PERCEIVED THREATS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

China identifies cyber terrorism, cyber espionage, harmful online content, hacker attacks, online fraud, infringement of intellectual property rights, online rumours, and personal data breach as cyber threats.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

China's NCS does not include a resilience perspective.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

China mandates that protecting critical information infrastructure should be a shared responsibility of the government, businesses, and the entire society.

China also mandates the government, social organisations, communities, schools, and households to engage in common efforts of child protection online.

Meanwhile, Internet users are encouraged to improve their skills to distinguish and resist online rumours and online criminal activities.

The private sector is assigned the role to protect critical information infrastructure.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

China seeks to implement cybersecurity talent pipelining, establish cybersecurity academies and innovation parks, and organise cybersecurity awareness activities.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

China promotes the inclusion of cybersecurity education in the school curriculum and the establishment of cybersecurity-related majors in universities. It aims for cybersecurity education to be included in textbooks.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

China mentions no specific programmes aimed to enhance the cyber capacity of the general public. However, it acknowledges the importance of raising the netizens' ability to recognise online disinformation, fraud, and harmful information, and mandates the organisation of cybersecurity propaganda activities.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

China implements cybersecurity assessment structures.

CYBERSECURITY RESEARCH AND DEVELOPMENT

China plans to establish cybersecurity academies and innovation parks.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

There is no mention of the specific agencies involved in China's cybersecurity governance in the NCS. However, from UNIDIR's database, it can be understood that the Office of the Central Cyberspace Affairs Commission is the central Internet regulator, censor, oversight, and control agency under the Central Committee of the CPC which is responsible for policy formulation and implementation.

China's national CERT, CNCERT/CC, is a non-governmental, non-profit cybersecurity technical centre and the key coordination team for China's cybersecurity emergency response community. CNCERT has its presence in 31 provinces, autonomous regions, and municipalities across mainland China.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

There is no mention of multi-stakeholder partnerships in cybersecurity.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

There is no specific mention of international agreements or partnerships that China is engaged on in the cybersecurity strategy. However, China is a member of the Shanghai Cooperation Organisation (SCO), APEC, the UN, ITU, and INTERPOL. With other SCO nations, China signed the organisation's Agreement on Cooperation in the Field of Ensuring International Information Security. Through APEC, China engages actively in the discussion on international collaboration on cyberspace issues.

China is a participant of the ARF, which alongside other ASEAN Dialogue Partners and the ASEAN Member States, produced a Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security.

Further, as a member country of the bloc of emerging economies comprising Brazil, Russia, India, China, and South Africa (BRICS), China is part of the CyberBRICS, which is a project that aims to identify best practices and develop policy suggestions in the areas of cybersecurity governance, Internet access policy, and strategies for the digitalisation of public administrations in the BRICS.

China's CERT, CNCERT/CC is a member of FIRST and AP-CERT. It also engages with APEC, ITU, SCO, ASEAN, BRICS and other international and regional organisations.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Children and young people are identified as vulnerable in the NCS. China mandates the provision of a safe online environment for children and young people. While the NCS does not mention a specific intervention to achieve this, China enlists collective efforts of the government, social organisations, communities, schools, and households to strengthen the protection of children and young people online and create a favourable online environment for them.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

The online portal of CNCERT/CC accepts a cybersecurity incident report from individuals. However, this portal is not identified in the cybersecurity strategy.

INDIA

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

India aims to build secure and resilient cyberspace for citizens, businesses, and the government. It puts forward strategies to secure the cyber ecosystem, strengthen the cybersecurity governance and the resilience of national critical infrastructures, establish cyber vulnerability management and incident response, develop cybersecurity technologies, prepare skilled cybersecurity workforce, create a culture of cybersecurity, and develop in-country partnerships and global cooperation in cybersecurity.

The formulation of India's NCS is motivated by the national priorities for rapid social transformation and inclusive growth that rely on secure cyberspace, and to have India become a prominent player in the IT global market.

PERCEIVED THREATS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

India identifies a variety of cyber threats across several attack vectors: uncontrolled exploits, malware, phishing, natural disaster with cyber consequences, identity theft, hacktivism, advanced persistent threats, denial of service, botnets, supply chain attacks, and threats arising out of technological developments (e.g., cloud computing, mobile computing).

HDI: MEDIUM
ASPI INDEX: 10TH OF 25
GCI: HIGH

STRATEGY STATS
PUBLICATION YEAR: 2013
AVAILABLE AT: ITU, UNIDIR, CCDCOE

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Resilience in India's NCS refers to the resilience of the cyberspace, critical information infrastructure, and ICT systems.

India's NCS vision is to build secure and resilient cyberspace for citizens, businesses and the government. One of its strategic objectives is to establish mechanisms for response, resolution, and crisis management through effective predictive, preventive, protective, response, and recovery actions.

Despite no explicit definition or description of what resilience means, it can be inferred from the Mission of the NCS that India perceives the minimisation of damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation as contributing elements towards being resilient.

India recognises rapid incident identification, information exchange, investigation and coordinated response, and remediation as actions for mitigating the damage caused by malicious cyberspace activities.

India also mandates the implementation of, among others, business continuity management and cyber crisis management plan, by all critical sector entities to reduce the risk of disruption and improve the overall national cybersecurity posture.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

All organisations are encouraged to develop information security policies which comply with international best practices, integrate these policies within their business plans, and allocate budget for implementing cybersecurity initiatives and emergency response mechanisms.

Academia is encouraged to collaborate with industry in joint cybersecurity research and development programmes.

The government is responsible for the promotion of cybersecurity literacy and for conducting awareness-raising activities.

Citizens/home users are expected to be aware of cybersecurity issues.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Professional cybersecurity training programmes are designed for cybersecurity professionals in law enforcement agencies. Further, certification for all cybersecurity roles is mandated.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

The NCS makes no mention of specific capacity-building policies and programmes targeted at students, nor of plans to incorporate cybersecurity education into the school curriculum.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

India aims to launch a comprehensive national cybersecurity literacy campaigns, workshops, seminars, and certifications. Further, it mandates the organisation of cybersecurity training programmes both in formal and informal sectors.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

There are no specific programmes mentioned in the NCS. However, India mandates the facilitation of regular cybersecurity drills and exercises at national, sectoral, and entity levels to

enable the assessment of the security posture and level of emergency preparedness in resisting and dealing with cybersecurity incidents.

CYBERSECURITY RESEARCH AND DEVELOPMENT

India is committed to undertaking research and development in cybersecurity that addresses the short, medium, and long-term needs of the national cybersecurity sector. It is also committed to support the production of to cost-effective, tailor-made indigenous security solutions that meet a wider range of cybersecurity challenges and target for export markets.

India also plans to establish Centres of Excellence, think tank for developing cybersecurity policy inputs, and cybersecurity concept labs for raising awareness and developing skills in key areas of cybersecurity.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The Ministry of Electronics and Information Technology is the government entity responsible for developing the NCS.

The National Critical Information Infrastructure Protection Centre (NCIIPC) is the nodal agency with respect to coordinating all measures to protect national critical information infrastructure.

CERT-In, established in 2004, functions as the nodal agency for the coordination of all cybersecurity emergency response and crisis management efforts. Under the Ministry of Electronics and Information Technology, CERT-In is also responsible for establishing and operationalising sectoral CERTs.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

Public-private partnerships in cybersecurity in India are established to provide cybersecurity training infrastructures as well as tested and certified IT products. India also seeks to foster national and global cooperation among security agencies, CERTs, defence agencies and forces, law enforcement agencies, and the judicial systems.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

There is no mention of specific international agreements or partnerships that India is engaged in. However, it aims to develop bilateral and multilateral relationships in the area of cybersecurity with other countries.

As one of the member states of the Commonwealth of Nations, India participates in cybersecurity-related initiatives, including the Commonwealth Cyber Declaration, which focuses on building effective national cybersecurity response and stability in cyberspace through international cooperation. India also has membership in the UN, ITU, INTERPOL, the Global Forum on Cyber Expertise, and SCO. Further, as a member country of BRICS, India is part of the CyberBRICS.

CERT-In has membership in FIRST and AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

India does not identify any vulnerable groups in the national cybersecurity strategy.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

The online portal of CERT-In accepts cybersecurity incident reports from individuals. The website clearly states that Indian citizens are one of CERT-In's stakeholders. However, this portal is not identified in the cybersecurity strategy.

JAPAN

HDI: HIGH
ASPI INDEX: EQUAL 2ND OF 25
GCI: VERY HIGH

STRATEGY STATS
PUBLICATION YEAR: 2015

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

Japan aims to build sustainable ecosystem in cyberspace to realise 'Society 5.0' where new values and services are continuously generated for the people. To achieve this, the country adheres to its basic position on cybersecurity comprising the country's cybersecurity objectives, ideals, and principles. A set of cybersecurity initiatives in the public and private sectors are promoted.

Japan employs the principles of assurance of the free flow of information, the rule of law, openness, autonomy, and multi-stakeholder collaboration.

The formulation of the NCS is guided by the consideration over increased cyber threats with major significant effects impacts on society, risk of reduced competitiveness due to information breaches, loss from financial theft and fraud, and the Tokyo 2020 Paralympic Games.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Japan identifies state-sponsored cyber-attacks, unauthorised access to digital assets, malware, and cybercrime committed by youth out of curiosity as cyber threats in the cybersecurity strategy. It also identifies vulnerabilities in Internet of Things (IoT) devices, supply chains, and open innovation as attack vectors.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Resilience in Japan's NCS refers to the national resilience and resilience against cyber-attacks.

There is no explicit definition or description of what resilience means to them. However, resilience in Japan's NCS is related to the ability to defence, deterrence, and situational awareness capabilities.

Japan encourages all organisations providing services and operating critical infrastructure to adopt 'mission assurance' approach, which aims to reduce risks to an acceptable level and ensure the safe and continuous operations and services.

Critical infrastructure operators are encouraged to prepare business continuity plans and contingency plans based on the concept of mission assurance.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Japan mandates all individuals and organisations to participate in the sharing of information on cybersecurity and mutual coordination of cybersecurity efforts from peacetime to damage prevention.

Senior executives/managers of all organisations are mandated to identify operations or services that represent their missions and take all responsibility for secure and sustainable provision.

The private sector is particularly expected to cooperate with the government in analysing cybersecurity risks associated with the use of advanced technologies, in preparing guidelines based on the analysis, and in preparing cybersecurity measures for the entire lifecycle of IoT devices from design through the disposal.

Academia is expected to work with the industry and the public sector in shaping the curriculum for the development of human resources to meet the cybersecurity workforce demand. They are also expected to support the government in identifying the legal provisions that enterprises should refer to when implementing cybersecurity measures.

All stakeholders are required to be aware of their own roles with regard to cybersecurity and implement necessary measures independently.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

The government works with the private sector to prepare professional cybersecurity programmes targeting senior executives and those at strategic management levels.

The government also provides incentives for investments in cybersecurity to promote the adoption of cybersecurity measures among enterprises. Further, the government supports the use of cybersecurity insurance and cryptocurrency services.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

Japan includes cybersecurity and ICT skills in the national educational curriculum at the elementary and secondary levels. This is further reinforced by making Computer Science a required subject from elementary school, cultivating logical modes of thinking, developing an understanding of ICTs according to the levels of children's development, and enriching the teacher training curriculum to include cybersecurity-related education materials. These strategies are linked to the need to prepare a cybersecurity workforce.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

Japan does not mention specific programmes to enhance the cyber capacity of the general public in the NCS.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

To increase the capabilities of critical infrastructure operators to respond to incidents appropriately, Japan conducts joint training and exercises between the public and private sectors.

Japan also participates in international joint cyber drills and training to enable coordinated response over cyber incidents with other countries.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Japan plans to promote research and development on risk analysis and threat countermeasures for advanced technologies. The country also focuses its cybersecurity research and development activities to improve its defensive and response capabilities and to ensure resilience. The government plans to promote cybersecurity research which considers the social science perspectives.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The Cybersecurity Strategic Headquarters, chaired by the Chief Cabinet Secretary and comprising several ministers, is responsible for promoting consistent and exhaustive implementation of information security measures across agencies and facilitating coordination among governmental bodies.

The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) plays a leading role as the focal point in coordinating intra-government collaboration, establishing cybersecurity standards for government agencies, and promoting multi-stakeholder partnerships in cybersecurity. NISC acts as the secretariat of the Headquarters in collaboration with the private and public sectors.

A non-governmental national CERT that is officially recognised, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) is responsible for coordinating national CSIRTs in dealing with cyber-attacks. It acts as a 'CSIRT of CSIRTs' in the Japanese community.

As part of its preparation for the Tokyo 2020 Games, the government plans to establish the Cyber Security Incident Response Coordination Center (Government Olympic/Paralympic CSIRT) which is tasked with responding to cybersecurity incidents during the occasion.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

In Japan, engagements between the public sector and private sectors start from the identification of cybersecurity risks associated with the use of advanced technologies and within the supply chain, and the formulation of frameworks for implementing operational-level cybersecurity measures.

The government also works with industry, academia, and the public sector to share information on the demand for cybersecurity personnel.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

At the international level, Japan positions itself as the leader in the discussions on cybersecurity. Japan proactively assists developing countries in their cyber capacity-building efforts and promotes cross-country sharing of cyber threat information.

Japan seeks to strengthen its participation in international cooperation against measures that inhibit free trade in cybersecurity areas.

Japan is a member of the Group of 7 (G7) which has a working group on cybercrime and pursues activities in cybersecurity, including the G7 24/7 Cybercrime Network and regular ICT Ministers meetings. Japan is also a member of APEC which has a focus and activities in the field of cybersecurity. Further, Japan is a participant of the ARF and has membership in the Global Forum on Cyber Expertise, the UN, ITU, and INTERPOL.

Japan ratified the Budapest Convention on Cybercrime. JPCERT-CC is a member of both FIRST and AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Small- and medium-sized business owners are identified as vulnerable in the NCS. To help them improve their cybersecurity capacity, the government prepares easy-to-understand case studies of cybersecurity measures for small and medium enterprises (SMEs) which include models for the safe use of information systems. The country also strengthens consultation on cybersecurity incidents to help those enterprises. Further, Japan provides incentives for the enterprises to adopt cybersecurity measures.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

Japan mandates senior executives or managers of all organisations to identify operations or services that represent their 'missions' and take the responsibility for ensuring secure and sustainable provision of services.

The online portal of JPCERT-CC accepts cybersecurity incident reports from individuals. However, this portal is not identified in the cybersecurity strategy.

MALAYSIA

HDI: HIGH
ASPI INDEX: 7TH OF 25
GCI: VERY HIGH

STRATEGY STATS
PUBLICATION DATE: 2006
AVAILABLE AT: ITU, UNIDIR, CCDCOE

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

The guiding principle of Malaysia's cybersecurity strategy is self-reliance. As such, it aims to create a secure, resilient, and self-reliant national information infrastructure, which promotes stability, social well-being, and wealth creation.

The formulation of Malaysia's NCS is motivated by the alarming rise of premeditated attacks with potentially catastrophic effects to interdependent networks and information systems. It is also driven by the national agenda to move towards a knowledge-based economy which relies on the secure cyber ecosystem.

PERCEIVED THREATS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Malaysia does not mention specific cyber threats in the cybersecurity strategy.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Malaysia's NCS vision is a secure, resilient, and self-reliant critical national information infrastructure.

Resilience in Malaysia's NCS refers to the resilience of critical national information infrastructure. However, there is no explicit definition or description of what resilience means to them.

Malaysia has a standard business continuity management framework to support the country's cybersecurity emergency readiness (Thrust 7 in the NCS).

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Other than the general role of the government as the primary actor in cybersecurity, Malaysia's NCS does not identify other stakeholders.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Professional cybersecurity training programmes are designed for cybersecurity professionals at law enforcement agencies. Capacity-building programmes are also provided for researchers and information security professionals.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

There is no specific mention of education programmes on cybersecurity in the cybersecurity strategy.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

There is no specific mention of cybersecurity capacity-building for the general public in the cybersecurity strategy. However, as part of its 'Developing Self-reliance' strategy, Malaysia aims to build the culture of cybersecurity.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

Malaysia has periodic vulnerability assessment programmes. However, there is no further explanation of the programmes in the NCS.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Malaysia focuses its cybersecurity research and development activities on strengthening its cybersecurity industry.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The National Cyber Security Agency (NACSA) is the national lead agency for cybersecurity matters, with the objectives of securing and strengthening Malaysia's resilience in facing the threats of cyber-attacks, by co-ordinating and consolidating the nation's best experts and resources in the field of cybersecurity. NACSA oversees all national cybersecurity functions formed under the National Security Council of Malaysia. NACSA runs the National Cyber Coordination and Command Centre (NC4) which is responsible to deal with cyber threats and crisis at the national level and ensures coordination and cooperation between critical national information infrastructure operators.

CyberSecurity Malaysia provides a variety of technical cybersecurity services. It operates under of the Ministry of Science, Technology, and Innovation (MOSTI), reports to NACSA, and is overseen by the National IT Council for policy direction and the National Security Council in times of national crisis.

One of CyberSecurity Malaysia services, Malaysian Computer Emergency Response Team (MyCERT) is responsible for handling cyber incident reports from the general public and conducting malware research.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

Malaysia does not mention existing multi-stakeholder partnerships in the NCS. However, public-private partnerships are indicated as input towards achieving effective cybersecurity governance.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

There is no specific mention of international fora or associations on cybersecurity that Malaysia is currently engaged in. However, it seeks to participate in international cybersecurity bodies, panels, multi-national agencies, and cybersecurity conferences.

Malaysia adopts the Commonwealth Cyber Declaration, like other member states of the Commonwealth of Nations. Malaysia is also a member of APEC, ASEAN, the UN, ITU, OIC, the Global Forum on Cyber Expertise, and INTERPOL.

MyCERT is a member of FIRST, AP-CERT, and OIC-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

There are no specific vulnerable groups identified in the national cybersecurity strategy.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

Malaysia has Cyber999, a service provided by MyCERT that deals explicitly with cybersecurity incident report from individual internet users. Cyber999 can be accessed through its online platform and mobile apps. However, none of the online services provided by CyberSecurity Malaysia is identified in the cybersecurity strategy.

NEW ZEALAND

HDI: VERY HIGH
ASPI INDEX: 6TH OF 25
GCI: HIGH

STRATEGY STATS
PUBLICATION YEAR: 2019
AVAILABLE AT: ITU, UNIDIR

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

The growing cyber risks associated with the evolving technology, the increasing sophistication of cyber threats, and the rise of state-sponsored cyber operations drive the improvement of New Zealand's NCS from its previous one.

Through its cybersecurity strategy, New Zealand aims to create a secure digital world where they can be confident and thrive to make the most of opportunities provided by the Internet without suffering harm or loss. To accomplish this, the national cybersecurity strategy comprises measures to enable the development of cybersecurity-aware and active citizens, strong and capable cybersecurity workforce and ecosystem, resilient and responsive New Zealand, and the country's active international engagement, as well as to support New Zealand to become proactive in tackling cybercrime and in international partnership in cybersecurity.

New Zealand's NCS is guided by the following principles: builds and maintains trust; people-centric, respectful, and inclusive; balances risk with being agile and adaptive; uses collective strengths to deliver better results and outcomes; and open and accountable.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

New Zealand identifies state-sponsored espionage, cyber terrorism, and theft of intellectual property as the main cyber threats in the cybersecurity strategy.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

A resilient and responsive New Zealand is one of the priority areas in the NCS.

Resilience in New Zealand's NCS refers to the resilience of the nation-state in cyberspace, the significant infrastructures, and the public sector; and among different groups of people.

New Zealand uses a descriptive text to indicate what cyber resilience means to them. Cyber resilience is regarded as involving resistance against and protection from cyber threats, and the ability to respond to incidents across system.

Comparing the notion of resilience adopted in the new NCS to the previous one, New Zealand expands the focus of resilience to consider the wider system, including the protection of important information infrastructures; the protection and resilience of businesses, non-governmental organisations, community organisations, and individuals; the use of cyber tools and partnerships to support national security and law enforcement activities; supporting organisations in securing their systems; and improving the information security capabilities and the resilience of the public sector.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

All stakeholders, i.e. individuals, businesses, non-government organisations, and government are encouraged to develop cybersecurity awareness and play an active role in reporting cyber incidents.

The leadership role of government in cybersecurity is acknowledged in the NCS. However, close partnerships with the private sector, non-government organisations, the technical community, and the international community are recognised as vital.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

New Zealand has introduced a greater cybercrime training for New Zealand Police.

Aside from that, New Zealand plans to support the expansion of roles and opportunities for cybersecurity workers and incentivise the supply of skilled cybersecurity workers.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

There are no specific programmes identified in the NCS.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

New Zealand conducts an annual awareness campaign on cybersecurity to build cyber awareness and resilience among different groups of people. It also strives to increase the availability of educative tools to support people's security and safety online, and to educate vulnerable users so that they can prevent their own victimisation.

New Zealand had Connect Smart, a cybersecurity awareness and capability campaign organised through a public-private partnership that ran from 2014 to 2020. Through Connect Smart website, home-users, businesses, and schools were provided with information and tips to

protect themselves from cyber risks and attacks. Starting April 2020, this function is delivered by the national CERT, CERT NZ.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

There are no specific programmes mentioned in the NCS.

CYBERSECURITY RESEARCH AND DEVELOPMENT

New Zealand does not specify its existing cybersecurity research, development, and innovation activities. However, it aims to create a strong and capable cybersecurity ecosystem which supports high-quality cybersecurity research and the development of a world-class cybersecurity academic research community.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The National Cyber Security Centre within the Government Communications Security Bureau (GCSB) is the coordinating agency for New Zealand's cybersecurity activities. New Zealand's NCS also identifies the National Cyber Policy Office (NCPO) which leads the development of policy advice to the government on investing in cybersecurity activities.

NCPO runs New Zealand's national CERT, CERT NZ. CERT NZ works with other organisations in the cybersecurity environment across the private, public, and not-for-profit sectors in New Zealand ,including partnering with Netsafe, New Zealand's independent, non-profit online safety organisation.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

The government of New Zealand, through GCSB, has deployed CORTEX which is a suite of capabilities that counters cyber threats to organisations of national significance, such as the operators of critical national infrastructures. Through CORTEX, Malware-Free Networks (MFN), which is a cyber threat detection and disruption service, is offered.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

New Zealand does not mention any of the international partnerships it engages in in the NCS. However, it mentions that it has been considering accession to the Budapest Convention.

New Zealand participates in cybersecurity capacity-building in Asia-Pacific, supports the Commonwealth Cyber Declaration, and engages in the discussion on internet governance (e.g. ICANN). It has membership in the UN, ITU, INTERPOL, the Global Forum on Cyber Expertise, and Pacific Cyber Security Operational Network (PaCSON). New Zealand is also a participant of the ARF and member of APEC.

CERT NZ is a member of both FIRST and AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Child and young people, elderly, as well as SMEs, are identified as vulnerable groups in the NCS.

To help owners of SMEs improve their cybersecurity capability to protect their business information, the government of New Zealand develops a cyber credentials scheme. However, the NCS does not specify interventions to assist other groups that are identified as vulnerable.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

The online portal of CERT NZ facilitates cybersecurity incident reporting from individuals. This capacity is identified in the NCS.

Meanwhile, the government's close partnership with non-government organisations, the private sector, and the technical community is identified as a requirement for successful cybersecurity strategy implementation.

PHILIPPINES

HDI: HIGH
ASPI INDEX: 15TH OF 25
GCI: MEDIUM

STRATEGY STATS
PUBLICATION YEAR: 2019
AVAILABLE AT: ITU, UNIDIR

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

The Philippines aims to reach the state of having a 'Trusted and Resilient Infostructure'. Infostructure here refers to information infrastructure. To accomplish this, the country seeks to strengthen its infostructure resilience, engage the private sector actors in the protection and resilience practices against cyber-attacks, and encourage individual users to adopt good cybersecurity practices.

For the Philippines, the urgency for improving NCS is motivated by previous experiences of adverse cyber events. These include the hacking of Philippine Voters' Database by Anonymous Philippines and cyber espionage in 2016. The maturity level of the country's cybersecurity, which is still at a Reactive and Manual state, also makes it important for the Philippines to refine the NCS.

The formulation of the Philippines' NCS is informed by the principles of the rule of law, autonomy and self-governance, the balance between the free flow of information and privacy rights, and risk-based management approach.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

The Philippines identifies cyber threats across several attack vectors: cyber espionage, script kiddies, hacktivism, malware, ransomware, phishing, distributed denial of service (DDoS), defacement, cyber terrorism, and threats arising from increasing connectivity to IoT.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Resilience in the Philippines' NCS refers to the resilience of the nation-state and the critical information infrastructure.

The Philippines aims to attain the Resilient Enterprise State, which is the highest level of its cybersecurity maturity model. At the

Resilient Enterprise state, the objective is predictive and mission-focused to isolate and contain damage, secure supply chains, and protect key critical infrastructure to continue operation despite cyber-attacks.

In regard to the critical infostructures, the desired state of resilience for the Philippines is of having resilient critical infostructures that can operate during and after cyber-attacks.

The Philippines' NCS aims to ensure the continuous operation of the critical infostructures and the public and military networks; and enhance the ability to respond to threats before, during, and after occurrence.

Further, the Philippines identifies having an incident response, business continuity, and recovery plans as some of the indicative success measures of reaching the desired state of having resilient CIIs.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

The role of citizens, businesses, organisations, education providers, and governments are recognised as important for building the layers of cybersecurity defence.

The private sector, as the owners of CIIs, are mandated to protect CIIs. Meanwhile, the participation of academia and education providers in developing cybersecurity development is encouraged.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

The Philippines aims to conduct a CISO Program which comprises capacity-building activities for CISOs.

Training is also provided for the staff of CERTs in government agencies.

The Philippines also aims to establish a pool of information security and cybersecurity experts. This is to be accomplished through several activities, including establishing communities of practice (COP), cyber training facilities, and certification programmes.

Capacity-building programmes are also provided for law enforcement agencies and cybersecurity trainers.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

Cybersecurity subjects are integrated into tertiary education curriculum as well as programmes organised by the Technical Education and Skills Development Authority (TESDA).

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

Public awareness about cybersecurity is raised through media campaigns, outreach projects involving youth organisations and community-based agencies, and national cybersecurity awareness month.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

The Philippines has a cybersecurity maturity model consisting of five stages of a continuum, from Reactive and Manual on one end to Resilient Enterprise on the other end.

The Philippines mandates the implementation of benchmarking to ensure that the ICT equipment is compliant with the established standards of the government (i.e., Cybersecurity Assessment and Compliance programme). It also mandates the participation of all government agencies in National Cyber Drills and Exercises.

The Philippines uses a risk management approach for its CII protection. This involves three stages of risk assessment: identification, analysis, and evaluation.

The Philippines establishes a mandatory review of all its software licenses, machines, and devices to ensure that all necessary components are up to date and are still well within its life cycle period.

CYBERSECURITY RESEARCH AND DEVELOPMENT

The Philippines plans to establish a Threat Intelligence and Analysis Operations Center which will house the cybersecurity research and development activities and host the testing of emergency plans.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The Cybercrime Investigation and Coordination Center (CICC), under the Department of Information and Communications Technology, functions as a coordinating body of all cybersecurity activities in the Philippines which also facilitates collaboration, cooperation, support, and participation from other stakeholders and the international bodies for cybersecurity-related activities.

The National Cybersecurity Inter-Agency Committee (NCIAC) serves as the central hub for harmonising and integrating national cybersecurity efforts, thus supporting a more efficient and effective strategic planning and implementation of cybersecurity measures.

The NCS mentions that there are four different CERTs in the Philippines: National CERT, Government CERT, Sectoral and Private CERT, and Organisational CERT.

The government-run national CERT, CERT-PH, is tasked to provide both government and private entities proactive countermeasures against cybersecurity threats. CERT-PH leads, manages, and oversees the various Government, Sectoral, and organisational CERTs. Meanwhile the Cybersecurity Philippines CERT (CSP-CERT) is a non-profit CERT which is also officially recognised.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

The Philippines aims to establish public-private partnership forums for enhancing

information sharing on cyber-attacks and vulnerabilities to cyber threats. The country also plans to establish cooperation and coordination among CERTs, law enforcement agencies, academia, and industries.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

The Philippines does not mention specific international engagements in cybersecurity in the strategy document.

However, the Philippines ratified the Budapest Convention in Cybercrime. The country is also a member of APEC, ASEAN, the UN, ITU, INTERPOL, and Global Forum on Cyber Expertise.

Further, it aims to facilitate international cooperation on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression, and prosecution.

None of the Philippines' CERTs has membership in FIRST or AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Children and young people, and SMEs are identified as vulnerable groups in the NCS.

Despite identifying these groups as vulnerable to cyber threats, there are no specific interventions mentioned in the cybersecurity strategy to help them. However, the need to raise the cybersecurity awareness of both groups is recognised.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

In the NCS, civil society is identified as one of the stakeholders for the implementation of cybersecurity plans, programmes, and activities.

Non-government organisations are expected to participate in cybercrime prevention programmes along with the private and public sector institutions. In the NCS, the Philippines acknowledges the government's limitation to patrol the cyber environment, and thus calls for the cyber community's participation in organising neighbourhood watch against malicious individuals prowling the Internet.

The online portals of both the government-run CERT-PH and non-profit CSP-CERT accept cybersecurity incident reports from individual citizens.

SAMOA

HDI: HIGH
ASPI INDEX: N/A
GCI: MEDIUM

STRATEGY STATS
PUBLICATION YEAR: 2017
AVAILABLE AT: ITU, UNIDIR, CCDCOE

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

Samoa aims to provide a secure and resilience cyberspace for its stakeholders. To achieve this goal, it identifies measures to strengthen the governance of cybersecurity, build the capacity of citizens, and strengthen the cooperation with local and global partners.

The development of the NCS is driven by the recognition of the country's need for an enhanced cybersecurity framework as the country is increasingly relying on the globalised cyberspace and ICTs.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Samoa identifies infrastructure impairment, cybercrime, hacking, virus attacks, access to pornographic materials, and misuse of information and network security in the cybersecurity strategy.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Samoa's NCS envisions a secure and resilient cyberspace. There is no explicit definition or description of what resilience means to Samoa. However, it can be inferred from the goals identified to achieve the vision that the resilient cyberspace is enabled through strengthening cybersecurity governance, enhancing the cybersecurity capacity of citizens, and strengthening cooperation in cybersecurity response.

The Samoa NCS mentions the need to ensure continuity of state's operations, development, and well-being of digital citizens as the motivation for developing the NCS.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Information sharing between the private and public sectors around cybersecurity is encouraged. Businesses are encouraged to operate securely in the cyberspace.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Samoa mandates the development of a sustainable training programme for professionals in law enforcement, finance, IT engineering, and information service providers. It also plans to develop a framework for the certification and accreditation of national agencies and public sector professions aligned with internationally recognised cybersecurity standards.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

Samoa plans to develop a tertiary-level Computer Science curriculum, that includes content on cybersecurity measures, as well as primary- and secondary-level school curriculum that includes good cybersecurity and cyber safety practices.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

Samoa plans to provide training and awareness-raising activities on cybersecurity. It also plans to use government's and mainstream media outlets, as well as the Feso'ota'i Centre Outlets to distribute Internet Safety Messages which are contextualised and in line with cultural norms.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

Samoa mandates the implementation of the National Benchmarking scheme that aims to ensure compliance of cybersecurity measures with international standards and to assess the impacts of cybersecurity breaches on different actors.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Samoa does not mention any research and development in cybersecurity in the NCS.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The National ICT Steering Committee (NICT), under the Ministry of Communication and Information Technology, leads the coordination and the implementation of the cybersecurity strategy.

Samoa also plans the establishment of a national computer incident response team (CIRT) for dealing with cybersecurity threats and attacks on citizens, tourist, businesses, and government.

It also mandates the establishment of a unit within Police Services (Ministry of Police) that serves as a single point of contact for cybercrime.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

The public and private sectors collaborate and share cybersecurity-related information

and assets (i.e. people, process, tools). Further, several government agencies; companies providing telecommunications, technology, and public access internet services; and non-government organisations working in child protection are involved in the country's Child Online Protection Working Group (COPWG).

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

Samoa is still in the process of establishing international partnerships in cybersecurity; the MCIT and Office of the Regulator (OOTR) are tasked with making recommendations regarding potential regional agreements. There is no mention of specific international engagements in the cybersecurity strategy.

Samoa seeks to participate in cybersecurity-related networks, such as the G8's 24/7 Cybercrime Network.

Samoa has membership in the UN, ITU, INTERPOL, the Commonwealth, and the PaCSON.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Children and young people and tourists are identified as vulnerable in the NCS.

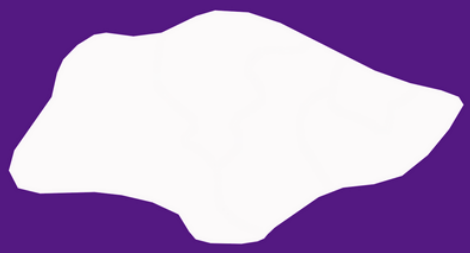
Samoa develops a Child Online Protection (COP) strategy to promote the use of ICT and implement precaution and protection of children users. It also has a Child Sexual Abuse Material (CSAM) Filtering Policy.

Despite identifying tourists as one of the vulnerable groups, there is no specific intervention mentioned in the cybersecurity strategy to help this group.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

Samoa is still in the process of establishing a CIRT. Currently, it has no mechanism for accepting cybersecurity incident reports from citizens.

SINGAPORE



HDI: VERY HIGH
ASPI INDEX: 5TH OF 25
GCI: HIGH

STRATEGY STATS
PUBLICATION YEAR: 2016
AVAILABLE AT: ITU, UNIDIR, CCDCOE

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

The formulation of Singapore's NCS is driven by the need to reinforce Singapore's position as a smart nation and a resilient and trusted global centre of trade and commerce.

Through the deployment of its cybersecurity strategies, Singapore aims to strengthen the resilience of CIIs, develop a vibrant cybersecurity ecosystem, create safer cyberspace, and forge strong international partnerships.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Singapore identifies cyber threats across several attack vectors: defacements of website, data theft, ransomware, cyber espionage, disruptions to Internet services, attacks on critical infrastructure, malware, scams, hacks, and vulnerabilities of IoT.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Singapore provides a definition and clear elaboration of cyber resilience in the NCS.

Resilience in Singapore's NCS refers to cyber resilience and the resilience of critical infrastructures. Cyber resilience is defined as the ability of its CIIs to withstand cyber-attacks, allowing them to continue operating under the toughest conditions and recover quickly after a disruption.

Singapore identifies the three aspects central to resilience, i.e. recover, restore, and remediate. It further elaborates that for a system to have the ability to return to normal operations as soon as possible or to facilitate their continued operations in sub-optimal conditions during a prolonged attack, there needs to be an integration of prevention activities, an expedient incident response plan, and a comprehensive recovery strategy to mitigate the effects of adverse cyber incidents.

Resilient cyber infrastructure is regarded as a means of providing peace of mind to

Singaporeans and for reinforcing trust in the country as the global centre of trade and commerce. The trust and participation of all stakeholders are regarded as pre-requisites to achieving resilient critical services.

The Singaporean government works with critical sectors to ensure that they incorporate disaster recovery plans and business continuity plans into their CII protection plans.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Cybersecurity is recognised as the collective responsibility of all stakeholders, including the government, businesses, individuals and the community.

Communities and associations are encouraged to foster their members' understanding of cybersecurity issues and promoting the adoption of good cyber practices.

Businesses and individuals are required to take preventive measures to secure their computer systems and digital devices to prevent malicious actors from hijacking their systems and devices to cause harm to others.

Higher learning institutes are engaged by the government to collaborate in growing the cybersecurity workforce and in building cybercrime investigations and forensics capabilities.

The private sector, including start-ups, are expected to produce best-in-class, exportable cybersecurity solutions. They also have a role in leveraging good personal data management, particularly to gain customer trust. Private companies are encouraged to collaborate with the government in helping cybersecurity professionals develop complementary skills, such as risk management and communication, and to reach out to SMEs.

Key private sector stakeholders, for example, in banking and technology industries, are mandated to raise awareness of cybercrimes and to encourage the adoption of good cyber hygiene practices. They are also required to conduct Data Protection Impact Assessment as part of the design, rollout, and review of systems, applications, and business processes.

CII owners and operators are mandated to secure their systems and networks through compliance with policies and standards, conducting audits and risk assessments, and reporting cybersecurity incidents. They are also required to participate in cybersecurity exercises to ensure their readiness in managing cyber incidents.

All organisations are demanded to shift from compliance to accountability. Internet service providers (ISPs) are required to secure Internet infrastructure.

With the government planning to establish more national CIRTs, it expects more participation from industry and academia to join the teams.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Professional cybersecurity training programmes are targeted at cybersecurity professionals and public officers handling sensitive data.

Subjects covered in the skills-based courses include incident management and response, digital forensics and malware analysis.

Singapore has SkillsFuture, a comprehensive framework for upskilling and reskilling of mid-career professionals which allows them to be cross-trained in cybersecurity.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

Higher education institutions update their curriculum to be relevant to the industry needs of the cybersecurity workforce. Specialised courses in cybersecurity are provided for students who want to pursue formal degrees in cybersecurity. Singapore also offers innovative, cybersecurity education programmes.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

Singapore has a range of activities to build cybersecurity awareness of the general public. The Singapore Police Force (SPF) regularly shares prevention messages through various media platforms, engages the local communities through Community Safety and Security Programmes and roadshows, nudge the public to adopt cyber hygiene practices through its Public Cyber-Outreach & Resilience Programme (PCORP) which uses behavioural insights, and regularly engages key private sector stakeholders to enhance cybercrime prevention efforts, raise awareness of cybercrimes, and encourage the adoption of good cyber hygiene practices.

Other outreach programmes include Cybersecurity Awareness Campaign, national security awareness-building platforms such as Total Defence and Let's Stand Together, and Cyber Security Awareness Alliance which reaches out to diverse audiences through exhibitions, clinics, and talks.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

Singapore includes a Systematic Cyber Risk Management Framework and a Cybersecurity Readiness Maturity Assessment in the NCS.

The Singaporean government has a holistic CII Protection programme for government agencies and CII operators. The programme builds on the implemented Cybersecurity Readiness Maturity Assessment programme, which has enabled agencies and operators to identify areas for improvement.

Singapore also has Exercise Cyber Star, which is a multi-sector exercise conducted by the Cyber Security Agency of Singapore (CSA) that aims to test the cooperation across multiple sectors and address inter-dependencies during major cyber-attacks.

The government has the Readiness Maturity Index (RMI) framework which is useful to assess the readiness of CII sectors in terms of their capabilities for risk-based mitigation, early detection of threats, and robustness of the response measures. Using the RMI, the government can direct the CII sectors' effort to manage cyber risks and facilitates the development of action plans to improve governance and procedures.

Singapore has been hosting the annual ASEAN CERT Incident Drill which aims to strengthen cybersecurity preparedness and cooperation among CERTs in ASEAN member states.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Singapore has established a Fintech Innovation Lab in which cybersecurity solutions are tested and a Cyber Security Lab (CSL) which facilitates the upskilling of cybersecurity professionals in mitigating cyber threats and investigating cyber incidents.

SPF has partnered with local research institutes to develop new cybercrime investigations and forensics capabilities. The Ministry of Home Affairs (MHA) has also worked with higher-learning institutes to create conducive environments for the development of cyber-related innovations.

The government funds the National Cybersecurity R&D Laboratory at the National University of Singapore (NUS) which will be a shared resource for cybersecurity researchers in the academia, industries, and government agencies.

Singapore also plans to transform all universities to become cybersecurity centres of excellence.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

There are many agencies and functions involved in the governance of cybersecurity in Singapore.

The Cyber Security Agency of Singapore (CSA), managed by the Ministry of Communications and Information (MCI) coordinates the national efforts against large-scale cyber incidents across government, industry, academia, businesses, and the public at large, as well as internationally. With its formation, all cybersecurity agencies and initiatives are brought under a single agency.

The national response to cyber-attacks is led by an inter-agency Cybersecurity Crisis Management Group (CMG). It is responsible for the development of cybersecurity policies and standards, oversees the implementation of cybersecurity protection measures in the critical sectors, mobilises resources, and directs the operational responses in providing a coordinated response to cybersecurity threats.

The Monitoring and Operations Control Centre (MOCC), Cyber-Watch Centre (CWC), and Threat Analysis Centre (TAC) provide the government with cyber situational awareness of its networks.

The government also established the Cybercrime Command as a unit within the Criminal Investigation Department (CID) of the SPF.

Under the CSA, the Singapore Computer Emergency Response Team (SingCERT) gathers cyber intelligence and alerts users on the preventive measures they can adopt.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

There are many instances of multi-stakeholder partnership in cybersecurity in Singapore. The Singaporean government established a Cybersecurity Consortium which brings together actors from government agencies, industry, and academia to collaborate on research and development on practical cybersecurity solutions with the potential for commercialisation.

Through its Collaborative Social Programme (CoSP), SPF will work with several stakeholders in cybercrime prevention awareness activities.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

Singapore mentions several international partnerships it has engaged in and seeks to undertake.

At the regional level, Singapore is ASEAN Voluntary Lead Shepherd on Cybercrime which provides a platform for the ASEAN Member States (AMS) to coordinate the regional approach to cybercrime and work together on capacity-building, training and the sharing of information. Singapore leverages existing ASEAN channels, such as ASEAN Network Security Action Council (ANSAC) and ARF Mechanisms for fostering cyber confidence-building and capacity-building measures.

Singapore has been hosting the annual ASEAN CERT Incident Drill which aims to strengthen cybersecurity preparedness and cooperation among CERTs in ASEAN member states.

Singapore actively collaborates with INTERPOL and AP-CERT to enhance cyber incident reporting and response linkages. It partners with INTERPOL and other countries to roll out cyber capacity development programmes.

Through its Personal Data Protection Commission (PDPC), Singapore seeks to collaborate with foreign Data Protection Authorities to enhance each country's data protection laws.

Singapore has regularly hosted international cybersecurity activities, including the INTERPOL Global Complex for Innovation (IGCI), the IGCI Working Group and INTERPOL Operational Expert Group on Cybercrime, RSA Conference Asia Pacific and Japan (RSAC APJ), and Singapore International Cyber Week (SICW).

Singapore also has membership in the UN, ITU, the Commonwealth, and the Global Forum on Cyber Expertise. It aims to step up its international engagements to improve its handling of cybercrime and capability to identify cyber threats.

SingCERT has membership in both FIRST and AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Children and young people, and SME owners are identified as vulnerable in the NCS.

Through CoSP, SPF will work with schools and non-government organisations to raise cybercrime prevention awareness among vulnerable groups. Meanwhile, the Inter-Ministry Cyber Wellness Steering Committee brings cyber-wellness messages to youth.

Through the PDPC, Singapore equips SMEs with information on the requirements of the PDPA and good data management practices to adopt.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

Non-government organisations are engaged in the efforts to raise cybercrime prevention awareness among vulnerable groups. Through its online portal, SingCERT receives cybersecurity incident reports, including from individuals.

SOUTH KOREA

HDI: VERY HIGH
ASPI INDEX: 2ND OF 25
GCI: HIGH

STRATEGY STATS
PUBLICATION YEAR: 2016
AVAILABLE AT: ITU, UNIDIR, CCDCOE

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

South Korea aims to create free and safe cyberspace to support national security, promote economic prosperity, and contribute to international peace. To accomplish this, the country seeks to strengthen the security and resilience of its core infrastructures, improve its cyber defence capabilities, and build a strong cybersecurity ecosystem.

South Korea notes several drivers for refining its NCS. These include the increasing cyber risks associated with the proliferation of convergent technologies enabled by the Internet of Things (IoT), the increasing likelihood of cyberwar, the vulnerabilities of the country's cyberspace to cyber threats despite its advanced cybersecurity capabilities, and the concern over the increasing likelihood of political, economic, and military disputes escalating to conflicts in cyberspace.

The formulation of the NCS is guided by the principles of respect to citizens' fundamental rights, citizen participation and confidence-building in the cybersecurity policymaking process, as well as active and transparent disclosure of cybersecurity-related information that is important for the public.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

South Korea identifies cybercrime, cyber terrorism, advanced persistent attacks, and threats arising from increasing connectivity to IoT as the main threats facing the country.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Resilience in South Korea's NCS refers to the resilience of the nation's core infrastructure and services.

One of South Korea's strategic objectives is to strengthen the security and resilience of the national core infrastructure against cyber-attacks to ensure continuous provision of critical services, thus enabling stable

operations of the state. To achieve this goal, South Korea recognises that the security and resilience of the nation's core infrastructure against cyber-attacks need to be strengthened.

Measures to strengthen the resilience of the national information and communications network services include system performance advancements and expanding back-up facilities to guarantee the provision of services in the face of diverse cyber-attacks.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Cybersecurity is recognized as the responsibility of all that requires the cooperation between the government, individuals, businesses, and international community. South Korea aims to establish a cyber safety network where all these stakeholders help to strengthen the management of cybersecurity.

South Korea encourages cooperation among industry, academia, and research institutions in fostering an environment for entrepreneurship where innovative cybersecurity technologies and ideas can be developed and commercialised.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

There is no specific programme identified for cybersecurity capacity-building for professional. However, training cyber warfare specialists is identified as an action area to devise comprehensive and active countermeasures to cyber-attacks.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

There are no specific cybersecurity education programmes identified in the NCS.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

South Korea implements cyber ethics and cybersecurity educational programmes which are targeted at different sectors of society, such as students, government officials, military personnel, and company employees.

It develops and distributes basic good cybersecurity practices which the public can easily put into practice in their daily lives. South Korea also has a 'Public Notification on Information Security' system which provides the general public about important cybersecurity-related information.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

South Korea conducts national public-private-military joint crisis management drills to enhance response capabilities against nationwide cyber crises. One of the well-known drills is the Eulji Exercise (i.e., a joint cybersecurity drill with the USA).

Overall, the country recognises the importance of enhancing the government's capacity to identify, arrest, and prosecute perpetrators of cybercrime by expanding expertise to investigate such crimes and cooperation with relevant agencies at home and abroad.

CYBERSECURITY RESEARCH AND DEVELOPMENT

South Korea has enacted relevant laws and regulations to enhance the competitiveness of the security industry and support the country's cybersecurity research and development activities.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The National Security Office develops the NCS and is responsible for overseeing public-private-military cooperation, developing and implementing cybersecurity policies at the national level, and monitoring the implementation of the strategy and the improvement of the cybersecurity capabilities of government agencies, businesses, and individuals. Meanwhile, the National Cyber Security Center (NCSC) under the National Intelligence Service (NIS) is responsible for overseeing cybersecurity policy by coordinating the execution of such policy and devising necessary schemes and guidelines. The NIS also receives reports and counseling requests on industrial espionage.

Under the Ministry of Science and ICT, the Korea Internet and Security Agency (KISA) provides technical services and conducts research in cybersecurity.

South Korea has two established national CERTs: KrCERT/CC and KN-CERT. KrCERT/CC liaises with the private sector as part of its incident response duties, while KN-CERT has a public sector- and government-only focus. Kr-CERT is run by KISA while KN-CERT is run by the NCSC.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

Public-private-military cooperation is conducted in the sharing of threat information, issuance of cyber crisis warnings, crisis management drills, and conducting joint examinations and investigations. Further, the country shares cybersecurity information with specialised organisations internationally and provides foreign assistance in cybersecurity capacity-building to developing countries.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

The NCS makes no specific mention of international agreements or partnerships that South Korea engages in. However, South Korea is a member of APEC, the UN, ITU, INTERPOL, and the Global Forum on Cyber Expertise. It is also a participant of the ARF.

South Korea mentions its intention to partner with international organisations, such as the UN and ITU; strengthen bilateral and multilateral cooperation to respond to transnational cyber threats; and secure leadership in cybersecurity-related international cooperations, including by providing foreign assistance projects for cybersecurity capacity-building.

Both Kr-CERT and KN-CERT have membership in FIRST and AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

There is no vulnerable group that is identified in the cybersecurity strategy.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

There is no specific avenue identified in the NCS for the participation of civil society stakeholders. However, South Korea plans to develop multiple mechanisms to allow public participation and confidence-building in national cybersecurity policymaking process.

Through its online portal, KrCERT receives cybersecurity incident reports, including from individuals. However, this portal is not identified in the NCS.

SRI LANKA

HDI: HIGH
ASPI INDEX: N/A
GCI: MEDIUM

STRATEGY STATS
PUBLICATION YEAR: 2018
AVAILABLE AT: ITU, UNIDIR

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

Sri Lanka aims to create a resilient and trusted cybersecurity ecosystem for the citizens. Towards this goal, the country seeks to strengthen cybersecurity governance, build its cybersecurity capacity through the development of skilled cybersecurity workforce and improvement of cyber awareness of citizens, and develop partnerships to create a robust cybersecurity ecosystem.

Sri Lanka's NCS formulation is motivated by the country's experience of rapidly increasing cybersecurity incidents as well as the assessment that the country's cybersecurity capacity is still maturing.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Sri Lanka identifies credit card fraud, cyber terrorism, hacking, malware, denial of service, advanced persistent threats, botnet, unauthorised access to social media, and intellectual property theft as the main threats to the country in the cybersecurity strategy. It also identifies revenge porn as a specific cyber threat against individuals.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Sri Lanka's NCS aims to create a resilient and trusted cybersecurity ecosystem. Resilience in Sri Lanka's NCS refers to the resilience of the cybersecurity ecosystem and the critical infrastructure.

One of the pillars that underpin the strategy is a resilient digital government and infrastructure. This is achieved through implementing risk management processes, security policies and strategies at the organisational level, partnering with private companies owning and operating critical infrastructures, and increasing awareness and building the capacity of the public sector.

Sri Lanka works with industry sectors to jointly improve detection, prevention, response, and recovery capabilities.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

The collective efforts of end-users, academics, the private sector, Internet service providers, and critical infrastructure owners are recognised as necessary for ensuring cybersecurity.

Organisations are required to develop cybersecurity policies based on the maturity of their information system and in compliance with international standards.

ISPs are tasked with increasing customers awareness on cybersecurity risks and best practices for avoiding cyber threats.

Start-ups are encouraged to develop niche cybersecurity solutions which can be exported to the global market.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Special cybersecurity training is targeted at agencies maintaining critical infrastructures, those dealing with most vulnerable communities in society, law enforcement authorities, Tri-forces, government staff, and the Intelligence Services. There are also programmes that are created for grassroots organisations in the public service.

Sri Lanka has an Information and Cybersecurity Competency Framework which identifies key cybersecurity skills and competencies necessary for the country.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

In Sri Lanka, cybersecurity is incorporated into tertiary education programmes. The country also provides cybersecurity industry-oriented degree programmes and career guidance workshops. Further, subjects of information and communication technologies and cybersecurity are made part of the informatics curriculum at school. Sri Lanka also has a distance learning center, Open University of Sri Lanka, and vocational training institutes which design cybersecurity modules.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

Several activities are conducted to raise public awareness of good cybersecurity practices. These include awareness campaigns, public conferences, street dramas, and media campaigns.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

Sri Lanka is still in the process of formulating cybersecurity metrics. As part of its strategy to strengthen international presence in the cybersecurity arena, it aims to collaborate with other countries and international organisations in conducting joint cyber drills.

Sri Lanka organises multi-sector cybersecurity exercises with the involvement of the Digital Government Infrastructure

Protection Unit aiming to identify vulnerabilities arising from cross-sector interdependencies and to stress-test coordination and communication across sectors.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Sri Lanka plans to establish a Digital Forensic Lab to conduct digital forensic investigations and examinations in the areas of computer forensics, mobile forensics, audio forensics, and video forensics. It is also committed to establish a Research Unit that will develop, coordinate, and stimulate research activities in different cybersecurity fields. Sri Lanka also seeks to host an annual national cybersecurity week and a national cybersecurity conference.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

ICT Agency of Sri Lanka (ICTA) coordinates national cybersecurity activities in Sri Lanka and oversees the implementation of the cybersecurity strategy and facilitating the protection of critical national infrastructures.

Established by ICTA, Sri Lanka CERT/CC is the single trusted source of advice on the latest threats and vulnerabilities affecting computer systems and networks, charged with the responsibility of providing technical support in responding to and recovering from cyber-attacks.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

Public-private partnerships in cybersecurity are mandated in the following areas: the development of information and cybersecurity training infrastructure, multi-sector cybersecurity exercises, and the development of market opportunities to bring made-in-Sri Lanka solutions into the global market.

A mechanism to share information on cyber threats and vulnerabilities is planned to be established through the collaboration between the government and medium-sized businesses.

A collaboration between Sri Lankan militaries, police, and intelligence services is also planned to establish a joint Cyber Security Operations Centre/Defence CERT with a focus on strengthening our cyber defence and ensuring that our defence forces are able to continue to operate securely.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

Sri Lanka ratified the Council of Europe's Convention on Cybercrime (Budapest Convention) in 2015.

It seeks to partner with international organisations such as the ITU, ENISA, and APCERT for exchanging information on threats and vulnerabilities, obtaining cybersecurity products, and conducting cyber capacity-building programmes.

There is no mention of specific international fora or associations that Sri Lanka is part of. However, it seeks to enhance its presence in the global cybersecurity arena through participation in relevant international and

multilateral activities.

Sri Lanka has membership in the UN, ITU, the Commonwealth, and INTERPOL.

Sri Lanka's national CERT is a member of both FIRST and AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Children and young people, women, SME owners, rural communities, and elderly people are identified as vulnerable in the NCS.

Sri Lanka conducts interventions and activities aimed to increase women's participation in the cybersecurity workforce. Further, it engages civil society groups in its effort to raise the awareness of rural and semi-urban citizens.

There are no specific interventions targeted at young people, elderly people, and SMEs mentioned in the cybersecurity strategy.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

Sri Lanka partners with civil society groups and non-government organisations to increase the awareness of rural and semi-urban citizens on cybersecurity.

Through the online platform of Sri Lanka CERT/CC, citizens can report cybersecurity incidents.

VANUATU

HDI: MEDIUM
ASPI INDEX: 17TH OF 25
GCI: LOW

STRATEGY STATS
PUBLICATION YEAR: 2013
AVAILABLE AT: ITU, UNIDIR

THE STRATEGIC OBJECTIVES AND GUIDING PRINCIPLES OF THE NATIONAL CYBERSECURITY STRATEGY

Vanuatu aims to ensure the provision of a safe, secure, and resilient cyberspace for its stakeholders.

The formulation of the NCS is motivated by the recognition of potential benefits of ICTs and increasing risks of participation in cyberspace.

PERCEIVED THREATS THAT ARE IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Vanuatu identifies natural disasters and cyber threats targeting children as the main threats in the cybersecurity strategy.

INCORPORATION OF RESILIENCE INTO THE NATIONAL CYBERSECURITY STRATEGY

Resilience in Vanuatu's NCS refers to the resilience of the cyberspace and the ICT infrastructure in the face of natural disasters.

The vision of Vanuatu's NCS is to ensure a safe, secure, and resilient cyberspace for all of the members of the society, which will enable them to enjoy the full benefits of the cyberspace. There is no explicit definition or description of what resilience means to them. However, it can be inferred from the operationalisation of the vision to the goals that the resilient cyberspace is enabled through strengthening the national cybersecurity governance, improving the cybersecurity capacity of citizens and businesses, and participating in international cooperation on cybersecurity.

CYBERSECURITY STAKEHOLDERS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY AND THEIR ROLES

Vanuatu identifies a planned central website and portal as a mechanism to facilitate the participation of private sector actors and citizens in reporting cybersecurity incidents.

ISPs are obliged to conduct measures for the protection of children and young people when requested by the users in accordance with parameters defined by the Child Online Protection Working Group (COPWG).

Citizens, students, businesses, judiciary, and law enforcement are expected to receive cybersecurity training.

CYBER CAPACITY-BUILDING PROGRAMMES PROVIDED FOR CYBERSECURITY PROFESSIONALS

Vanuatu plans to have a sustainable cybersecurity training programme for officers in law enforcement, financial intelligence units, state law, and the judiciary.

CYBERSECURITY CAPACITY-BUILDING IMPLEMENTED IN NATIONAL EDUCATION PROGRAMMES

Apart from the inclusion of cybersecurity programmes in primary school and high school curricula, the Vanuatu government also provides support for cybersecurity capacity-building activities for teachers.

In cooperation with the future cybersecurity governing entities in Vanuatu, the Ministry of Education plans to develop the cybersecurity-related training materials, background information for teachers, and sample presentations for different age groups.

CYBERSECURITY CAPACITY-BUILDING PROGRAMMES PROVIDED FOR THE GENERAL PUBLIC

There is no specific mention of cybersecurity capacity-building programmes for the general public. However, the government plans to work with partners who could support them in reaching different population groups, including those in rural areas.

PROGRAMMES TO IMPROVE INCIDENT MANAGEMENT AND RESPONSE CAPABILITIES

Vanuatu does not identify any existing or plan to establish measures to improve cybersecurity response capabilities in the cybersecurity strategy.

CYBERSECURITY RESEARCH AND DEVELOPMENT

Vanuatu does not identify any research and development in cybersecurity in the NCS.

INSTITUTIONS COORDINATING CYBERSECURITY IN THE COUNTRY

The Office of the Government Chief Information Office develops the NCS and cybersecurity-related policy. It is currently responsible for coordinating all cybersecurity efforts.

The NCS mentions the plan to create a National Cybersecurity Steering Committee (NCSC) which will coordinate the implementation of national cybersecurity efforts. The NCSC will consist of representatives from the public and private

sectors and non-profit organisations.

Established by the Office of the Government Chief Information Office in 2018, the national CERT, CERT VU, provides basic cybersecurity services to citizens and businesses.

MULTI-STAKEHOLDER PARTNERSHIPS IN CYBERSECURITY IN THE COUNTRY

Local cybersecurity experts and scholars fill the positions in the information and communication security advisory committee through which they participate in enhancing the national cybersecurity policies and promotional strategies, and industry-government-academy research synergy on cybersecurity.

The collaboration between different cybersecurity stakeholders is planned to be coordinated by the NCSC.

COUNTRY'S ENGAGEMENT IN INTERNATIONAL DISCUSSIONS ON CYBERSECURITY

Vanuatu is still in the stage of establishing international cooperation in cybersecurity. It seeks to participate in cybersecurity-related networks, such as G8's 24/7 Cybercrime Network.

Vanuatu has membership in the UN, ITU, the Commonwealth, INTERPOL, and the PaCSON.

Meanwhile, CERT VU has no membership in FIRST or AP-CERT.

VULNERABLE GROUPS IDENTIFIED IN THE NATIONAL CYBERSECURITY STRATEGY

Vanuatu identifies primary school and high school students as groups that are vulnerable to cyber threats. To protect them from cybersecurity harms, it mandates the development of curriculum for cybersecurity training and assessment of child-specific cybersecurity risks.

AVENUES PROVIDED FOR THE PARTICIPATION OF CIVIL SOCIETY ACTORS IN THE CO-PRODUCTION OF CYBERSECURITY AND CYBER RESILIENCE

The government of Vanuatu seeks to engage community-level intermediaries such as chiefs and religious leaders in rural areas to support capacity-building initiatives for rural citizens. The government will provide these intermediaries with necessary background information and training materials on cybersecurity.

Through its online portal, CERT VU receives cybersecurity incident reports, including from individuals.

CONCLUSION

Countries around the world are increasingly adopting cyber resilience in their strategies and posturing. This represents an evolution from security thinking, which is about protection from attacks and designing fail-safe systems, to a resilience thinking, which is about anticipating adverse cyber threats. The resilience thinking seeks to enable functioning despite adverse incidents and designing systems that are safe to fail. Further, cyber resilience is increasingly being recognised and understood as a multi-faceted (i.e., beyond the technical dimension) whole-of-society (i.e., multi-stakeholders and systemic) posture that enables countries and the global community to persist in their societal functioning in the face of imminent cyber threats.

In this review of the national cybersecurity strategies of several countries in Asia and the Pacific, the key findings are that:

- several countries include resilience thinking in their national cybersecurity strategies,
- however, few countries give elaborate framing and operationalisation of cyber resilience,
- all countries acknowledge cybersecurity as a shared duty of all stakeholders,
- however, there are limited avenues for citizen co-production of cybersecurity,
- citizens are largely framed as recipients of cybersecurity,
- and there remains better engagement around cybersecurity between specific sectors, for example, between the government and the private sector

As noted in the 2012 WEF 'Partnering for cyber resilience' report, and in UN SDG17 'Partnering for the goals', there is a heightened need for countries to ensure broad whole-of-society participation (i.e., to 'leave no one behind') towards the achievement of global cyber resilience goals and aspirations.

RECOMMENDATIONS

1 Define and operationalise cyber resilience in the NCS

Resilience is a broad concept. Different understandings of the concept in different sectors could pose a challenge for cross-sector cooperation. How the concept is defined determines its operationalisation. As a strategic document that constitutes the basis from which national cybersecurity posture is created, NCS needs to establish a common understanding of resilience and related terms to support a mutual understanding of the terminology across sectors.

Further, resilience needs to be operationalised into relevant instruments, including assessment frameworks and maturity models with clearly defined resilience metrics. These instruments help countries to assess various aspects of cyber capabilities, evaluate readiness, monitor progress, improve cybersecurity practices, and make progress towards cyber resilience maturity.

The Philippines and Singapore provide an example of good practice in this regard. Both countries provide elaborate description of cyber resilience and coherently operationalise the notion into relevant instruments in the NCS.

2 Enable instrumental and representative participation of civil society stakeholders in NCS development

Without the participation of civil society actors in the development of the NCS, the framing of the cybersecurity issues will be skewed and incomplete. Therefore, engaging civil society actors in the formulation of the NCS and in the associated drafting of cyber resilience-related legislation is imperative to take into consideration their substantive suggestions and concerns with regard to civil society cyber resilience in the resulting provisions.

Further, taking into account civil society's concerns can contribute to a more substantial societal buy-in and commitment to the implementation of the strategy.

A good example of this is provided by Bangladesh, which makes provision for the involvement of civil society actors in the evaluation the cybercrime law.

3 Clearly identify sites and means of engagement for civil society in the co-production of cyber resilience

It can be noted from the review that only a few countries identify and assign roles within the cybersecurity ecosystem for the civil society. In most cases, civil society is identified as the recipient of security. Simultaneously, they are regarded as the bearer of cybersecurity responsibility alongside other actors. However, compared to their private and public sector counterparts, the sites and means of engagement for civil society participation in the co-production of cybersecurity are not clearly identified in the NCS.

Several countries provide a good example in elaborating the sites of engagement of civil society (i.e. the development stage of cybersecurity-related legislation, the information-sharing network on cyber threats, the implementation of cybersecurity awareness activities, the outreach to vulnerable groups).

Additionally, civil society's participation in formal means of engagement, such as advisory committee and public consultation which function as spaces for intervention in the law and regulation of cybersecurity, needs to be explicitly encouraged as part of the strategy.

4 Facilitate civil society incident reporting

The review of NCS's reveals that only a small number of countries identify the role of national CERT in facilitating civil society incident reporting and assisting civil society in incident handling. The role of CERTs is often associated with assisting the private and public sectors.

While the civil society sector experiences cyber threats differently than their private and public sector counterparts, there is a lack of focus on the mandate of national CERTs in facilitating civil society incident reporting. This not only underestimates the vulnerability of civil society to cyber threats but also risks reducing preparedness by policymakers and the civil society itself.

In this regard, there is a need to extend the framing of the national CERT's role in regard to its function vis-à-vis civil society. New Zealand, for example, brings together representatives and functions from a range of stakeholders, including civil society sector in its national CERT to ensure balance in the facilitation of incident reporting.

Alternatively, the government can support the establishment of a separate CERT for the civil society sector. Malaysia and the Philippines provide an example for this. Both countries have separate national CERTs that serves the general public.

5 Undertake capacity-building for the general public

Civil society has been the weakest link in the cybersecurity ecosystem. However, the focus of NCS has been in upskilling cybersecurity professionals and preparing the future cybersecurity workforce. To build cyber resilience, the capacity of every element of the ecosystem needs to be enhanced. The capacity-building needs of the general public need to be recognised and acted upon so that well-suited programmes aimed to promote adoption of cybersecurity mindset and to provide the required level of capability to deal with cyber incidents can be devised. In this regard, engaging and partnering with civil society organisations (CSOs) is vital since CSOs possess greater grassroots understanding and proximity with the general public.

6 Provide a multi-dimensional framing of cyber threats beyond the technical

Countries still largely frame cyber threats in technical terms and with a focus on ICT systems and infrastructure. However, adverse cyber incidents are not only technical, but also include socio-technical and natural threats that not only hamper and harm individuals' everyday functioning, but that also have cascading impacts across society.

From the review, some countries recognise non-technical threats such as cyberbullying, revenge porn, and scams, however these need to be significantly foregrounded and mainstreamed because they are prevalent and pertinent for citizens.

7 Provide a whole of society framing of resilience comprising cyber resilience and other dimensions of societal resilience

Countries around the world are facing several significant risks, including natural disasters, extreme weather, biodiversity loss, social instability, fiscal crises, and adverse technological incidents. To prepare, absorb, recover, and adapt during these imminent shocks, stresses, and disasters necessitates that countries and the global community establish whole of society resilience.

Countries, therefore, need to articulate broader strategies for resilience, which invariably comprise cyber resilience as a significant component of societal resilience. Further, countries need to engage in multilateral partnerships and collaborations for resilience.

REFERENCES

[1] World Economic Forum, "Partnering for Cyber Resilience," 2012. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.
[2] World Economic Forum, "Global Risk Report 2020," 2020. [Online]. Available: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.
[3] UN General Assembly, Transforming Our World: The 2030 Agenda for Sustainable Development, 21 October 2015, A/RES/70/1. [Online]. Available: https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf
[4] UNISDR (United Nations International Strategy for Disaster Reduction), "Sendai Framework for Disaster Risk Reduction 2015-2030," 2015. [Online]. Available: http://www.wcdrr.org/uploads/Sendai_Framework_for_Disaster_Risk_Reduction_2015-2030.pdf
[5] United Nations, "The New Urban Agenda," 2017, A/RES/71/256, Habitat III and United Nations. [Online]. Available: http://habitat3.org/wp-content/uploads/NUA-English-With-Index-1.pdf
[6] D. Chandler, "Resilience and the end(s) of the politics of adaptation," Resilience, vol. 7, no. 3, pp. 304-313, Sep. 2019, doi: 10.1080/21693293.2019.1605660.
[7] I. Linkov and A. Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in Cyber Resilience of Systems and Networks, A. Kott and I. Linkov, Eds. Cham: Springer International Publishing, 2019, pp. 1-25, doi: 10.1007/978-3-319-77492-3_1
[8] T. Hellström, "Critical infrastructure and systemic vulnerability: Towards a planning framework," Safety Science, vol. 45, no. 3, pp. 415-430, Mar. 2007, doi: 10.1016/j.ssci.2006.07.007.
[9] S. Amir, Ed., The Sociotechnical Constitution of Resilience. Singapore: Springer Singapore, 2018.
[10] Internet Society, "The Internet Society Survey on Policy Issues in Asia-Pacific 2018 - Focus: IoT Security and Privacy," 2018. [Online]. Available: https://www.internetsociety.org/wp-content/uploads/
[11] International Telecommunication Union, "Global Cybersecurity Index (GCI) 2018," 2018. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[12] Australian Strategic Policy Institute (ASPI), "Creating an Asia-Pacific Cyber Maturity Metric," 2017. [Online]. Available: https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017
[13] United Nations Development Progamme (UNDP), "Human Development Report 2019", 2019. [Online]. Available: http://hdr.undp.org/sites/default/files/hdr2019.pdf
[14] A. Comninos and G. Seneque, "Cyber security, civil society and vulnerability in an age of communications surveillance," p. 10.

UNITED NATIONS UNIVERSITY
Institute in Macau

ISBN: 978-92-808-9121-8