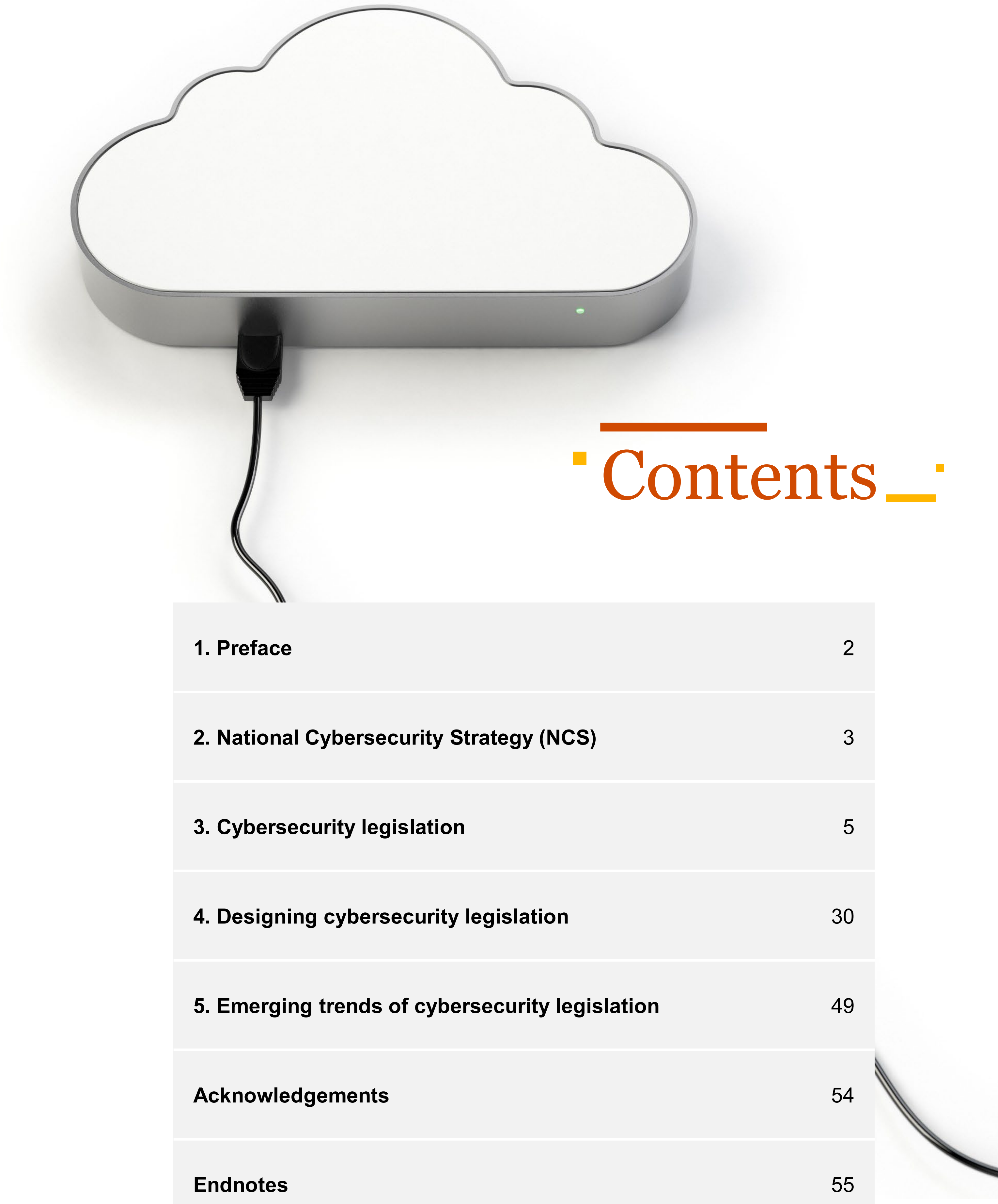
Discussion paper

# Cybersecurity legislation insights

## A comparative study and considerations for future cybersecurity legislation

**Volume 1** - **Introduction and study summary**



# Contents

# 1. Preface

The digital age is a new era of interconnectivity and innovation. People across the world have integrated information and communication technologies (ICTs) into their daily life and critical operations. Digitisation has now become an inseparable and inevitable part of global socioeconomic development. As an inevitable consequence, the increased dependency on technology has led to greater exposure to cyber threats and challenges. In response to the heightened vulnerability to cyberattacks, countries across the globe have established or are constantly having to establish and update their domestic legislations, and collaborate with their international counterparts against cyber threats.

The approaches countries have adopted in designing cybersecurity legislation vary from one to the other depending on numerous factors, such as national socioeconomic status or historical background. This paper has been written with a detailed analysis of the differences and similarities between different countries' approaches. We sampled thirteen countries (or called "subjects" hereafter) across the different continents and studied their cybersecurity environments, in particular focusing on their strategies for legislation. These sample countries are **Brazil, Chile, China, Germany, India, Mexico, Singapore, South Africa, the United Arab Emirates (UAE), the United Kingdom (UK), the United States (US), Vietnam and the European Union (EU).**

This paper intends to share observations, analysis and insights from various stakeholders, including cybersecurity and privacy policy researchers. This paper also intends to provide insights and guidance to policy makers and key stakeholders at the early stage of formulating strategy for cybersecurity legislation. In overview, this report includes the following contents.

**National Cybersecurity Strategy (NCS):** Our team first analysed the National Cybersecurity Strategy (NCS) documents, which are the foundation and cornerstone for designing national cybersecurity strategy. This section outlines our findings on common structures and components of NCS adopted by the study subjects.

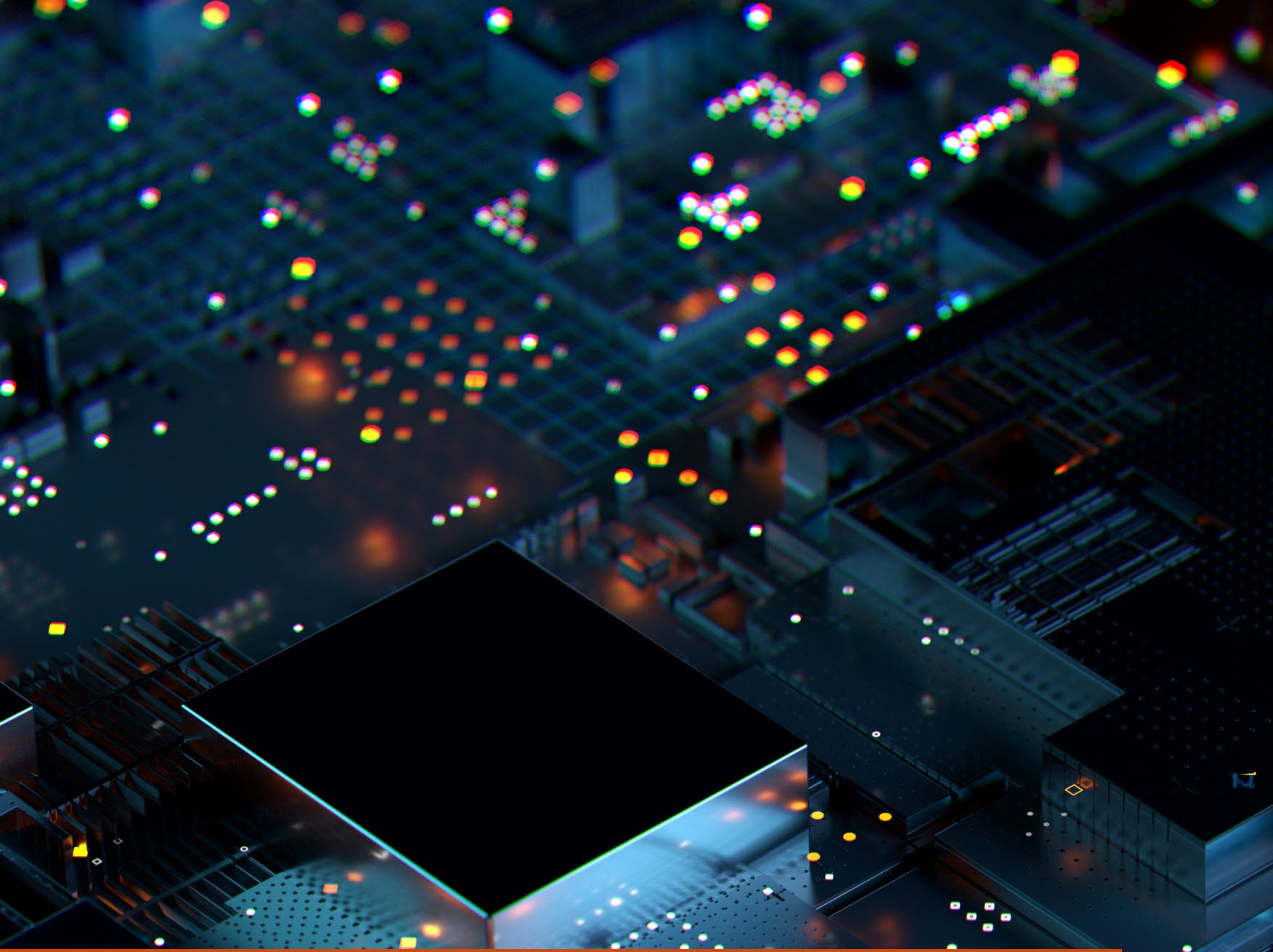
**Nine cybersecurity areas:** We conducted a thorough comparative study on our subjects' cybersecurity legislation and shortlisted nine common areas of interest:

1. Critical infrastructure (CI) protection
2. Incident response and crisis management
3. Cybercrime law
4. Personal data protection
5. Non-personal data protection
6. Information and communication technology (ICT) vulnerability management
7. Awareness and capability
8. International cooperation
9. Cybersecurity technologies and solutions marketplace

This section provides a general overview of variations and similarities in security and legislation design approaches in the nine areas of cybersecurity. This section also highlights notable observations in those areas.

**Five considerations:** After aggregating the knowledge and insights gathered during the comparative study, our team identified five considerations that countries in their early stage of developing their cybersecurity strategy (including legislation) can take into consideration.

**Future trends in legislation:** Lastly, the report sheds light on emerging cybersecurity legislation trends so that countries may better prepare themselves for a rapidly evolving digital paradigm.



# 2. National Cybersecurity Strategy (NCS)

National Cybersecurity Strategy (NCS) is a document that highlights the challenges, high-level goals, principles and priorities that guide a country in addressing its cybersecurity needs. With a clear vision, policymakers and key stakeholders can drive a more comprehensive, consistent and coherent approach. NCS shapes the strategic guidelines of a country's cybersecurity approach and plays a crucial role in its cybersecurity protocol. It is summative, and its principles will influence a country's cybersecurity legislation. One commonality that all countries share throughout their NCS is the goal of translating their nationwide vision into implementable and coherent cybersecurity legislation and regulations. Thus, an NCS should be based on an all-encompassing understanding and analysis of the overall digital environment while being tailored to the country's specific circumstances and priorities.

As mentioned above, NCS is a stepping stone for cybersecurity legislation to be developed. It articulates the cybersecurity challenges a country faces and the corresponding goals that it aims to achieve. Furthermore, it may also state specific cybersecurity issues to be addressed and actions to be carried out. Below are some of the challenges, goals and issues commonly found in the NCS of our 13 subjects.

## Challenges

- Increasing instances of cybercrimes
- Increasing level of sophistication in cyberattacks
- Increasing vulnerabilities in critical infrastructures

## Goals

- Enhance cyber resilience
- Control cybersecurity risk
- Leverage international cooperation in combating cybercrime
- Build open and connection-enabled cyberspace

## Issues to be addressed

- Domestic legislation and regulation building
- Identify and emphasise critical infrastructures (CI)
- Combat cybercrime
- International cooperation
- Expand the partnership between the public sector and private sector
- Promote the development of the cybersecurity industry
- Raise national cybersecurity maturity level
- Raise awareness and capabilities

To summarise, NCS is essential for developing a country's cybersecurity. The challenges, goals or measures proposed therein reflect the overall requirements of cybersecurity development and can act as a critical reference point.

# 3. Cybersecurity legislation

This section provides an overview and comparative analysis of the diverse approaches and subjects adopted in the nine cybersecurity areas.

# 3.1 Critical infrastructure (CI) protection

## 3.1.1 Legislative model

Critical infrastructure protection legislation has entered a mature stage. Most of our sampled countries have CI protection legislation in place; they are Brazil[1, 2], Chile[3], China[4], Germany[5], India[6], Singapore[7], South Africa[8], the UAE[9], the UK[10], the US[11], Vietnam[12], and the EU[13, 14]. There are two legislative models, one dedicated to CI protection laws and the other incorporating relevant requirements into the broader cybersecurity legislation or strategic initiatives.

## 3.1.2 Legislative framework

We observed commonalities in the writing structure and content coverage of numerous CI protection laws. The structure of the components is as follows:

1. **Introduction, definitions and scope of CI protection laws** - it covers the purpose and scope of the CI protection law.

2. **Enforcement bodies and duties** - it describes the responsibility of government bodies in CI protection, including 'enforcement bodies' and the national 'Computer Security Incident Response Team (CSIRT)'.

3. **Duties of operators** - it describes the administrative and technical requirements for CI operators, including their security and incident reporting requirements.

4. **Miscellaneous** - it includes the terms or articles that do not fit in any of the above sections but are deemed critical to the CI protection. Often, this section would cover contents related to penalties, grace periods, transitional measures, gap analysis and remediation, among others.

## 3.1.3 Definition and scope

Depending on the national priorities and circumstances of individual countries, CI may encompass a wide range of industries and sectors. In general, energy, transportation, banking and finance and telecommunications are defined as CI in most countries.

Critical infrastructure can have a different name depending on the country in question. It is commonly referred to as ‘critical infrastructure’, ‘critical entity (CE)’ or ‘essential services (ES)’. Critical information infrastructure (CII) refers to a system carried and operated based on CI and is a concept with a smaller scope. CI, CE and ES are collectively referred to as CI hereafter in this report.

## 3.1.4 Roles and responsibilities of government authorities

To continuously improve national CI protection, some countries implement the risk management cycle, including managing the vulnerability of critical infrastructure; managing critical infrastructure incident reports; conducting incident investigation; providing cybersecurity advice and support for critical infrastructure; imposing disciplinary actions; and establishing relevant standards of CI protection. There are two authority models in CI protection. One is having a central authority overseeing the entire CI protection operation, and another is delegating power to different authorities. However, numerous tasks and multiple stakeholders are involved in CI protection, and many countries in our sample nominate agencies to coordinate and be responsible for CI protection.

### 3.1.5 Incident reporting mechanism

Most countries have specified their cybersecurity incident/threat reporting requirements for their CI operator/owner. This study found that incident reporting requirements across most jurisdictions include three primary components: the reporting path, time requirements for reporting and reporting content.

#### Cybersecurity incident reporting path

Most legislation outlines the reporting path when security incidents occur, which is generally reported to the national Computer Security Incident Response Team (CSIRT) immediately. While most countries have a CSIRT as the body to report CI incidents, the US has set up CISA (Cybersecurity & Infrastructure Security Agency) to handle incident reporting from CI operators.

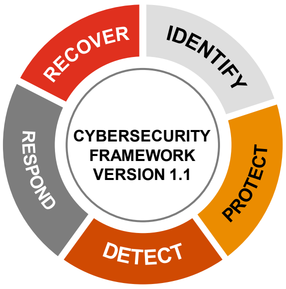
#### Time requirements for reporting

The reporting time requirement ranges from 6 to 72 hours, depending on the situation. In addition, some countries do not have a time requirement or have one that is described in vague wording such as ‘immediately’ or ‘as soon as possible’.

#### Cybersecurity incident reporting content

Countries with a higher level of cybersecurity maturity provide detailed guidelines on what content needs to be included in the incident report. The content should generally include: description of the security incident; the time when the incident occurred; the duration of the incident; the security defences that were in place; and the impact and cross-border impact of the incident. On the other hand, countries with a lower maturity level lack specifics in the content coverage guideline.

## 3.1.6 Security requirements for CI operators



Credit: N. Hanacek/NIST[15]

CI operators comply with many security requirements in the CI operation process. Most countries' CI security requirements are based on or derived from the National Institute of Standards and Technology cybersecurity framework (NIST CSF)[16]. The five core parts of the security requirements are divided by function as follows:

- **Identify** - through assessments such as security risk assessments with which the organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets and individuals.

- **Protect** - through programmes such as security awareness and training with which the organisation's personnel, business partners and suppliers are provided with cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities in line with related policies, procedures and agreements.

- **Detect** - through activities such as security continuous monitoring, during which information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

- **Respond** - through processes such as cyber incident response procedures, response planning, communication, analysis, mitigation and improvement.

- **Recover** - through business continuity management in cyber incidents with recovery plans or improvement, among other initiatives.

# 3.2 Incident response and crisis management

Cybersecurity incident response and crisis management are essential components of cybersecurity. It guides all levels of government and non-governmental organisations (NGOs) as well as the private sector to work together to prevent, mitigate, respond to and recover from incidents. Our study noted a global trend of increasingly mature development in cybersecurity incident response legislation, with many countries publishing their cybersecurity incident response laws, including India's CERT-IN directives[17], National Cyber Security Incident Plan of China[18] and the US's Cyber Incident Reporting for Critical Infrastructure Act of 2022[19].

Studies on our samples indicated that the framework of cybersecurity incident response law usually includes incident classification and a reporting mechanism.

## 3.2.1 Classification of a cybersecurity incident

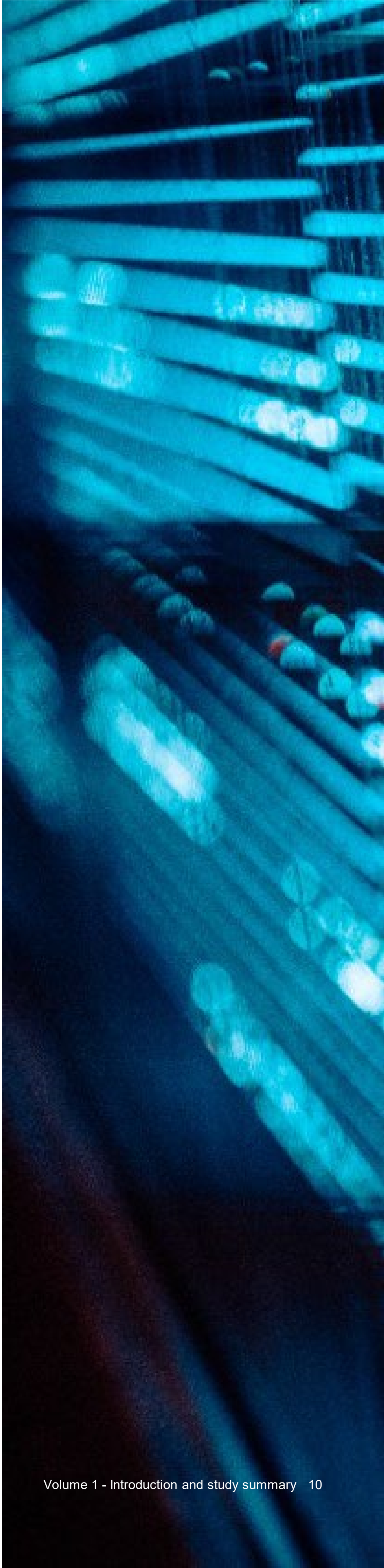
The study found that most countries have established legal requirements for classifying security incidents. For example, China's National Cyber Security Incident Plan indicates that a cybersecurity incident could be classified into one of four levels, extraordinarily significant, significant, relatively significant and general.

## 3.2.2 Reporting mechanism

### Reporting agency

All research subjects have determined the body or entity to whom cyber security incidents should be reported, e.g., the national Computer Security Incident Response Teams (CSIRTs, also known as CERTs). CSIRT's responsibilities mainly cover the following areas:

- Security incident response management
- Information sharing management
- Collaborative relationships management
- Knowledge building



However, national CSIRTs in developing countries mainly focus on dealing with security incident responses and have less emphasis on raising public awareness through regular training and awareness seminars.

## Reporting content

The legislations of most countries do not specify the report content when a security incident occurs. According to the requirements of developed countries, reporting information may include who reported the event, who experienced the event, what type of event occurred, how and when the event was initially detected, what response measures have been taken and who has been notified.

## Time requirements for reporting

Most of the legislation describes specific reporting time requirements when security incidents occur. Most countries expect cybersecurity incidents to be reported within 48-72 hours. However, in some cases the reporting requirements are relatively shorter at 6-24 hours.. At the same time, some countries do not provide a specific time limit for reporting security incidents, and only indicate that they should be reported as soon as possible or immediately after occurring.

# 3.3 Cybercrime law

In order to ensure an accurate and focused analysis, this paper focuses on cybercrimes that occur exclusively in the digital space. For example, these cybercrimes include hacking of systems or user accounts, system interference, malware, phishing and ransomware, among others. Our scope excludes traditional crimes, such as human trafficking or child pornography, that occur in non-cyber environment but uses digital space as a tool. Furthermore, based on legal characteristics, we categorised the various stages of combating cybercrime into prevention, investigation and recovery. Notably, our analysis of cybercrime legislation noted a discernible trend wherein many countries are increasingly prioritising preventive measures over investigation and punishment.

## 3.3.1 Prevention

Cybercrime prevention is a critical aspect of addressing the growing challenges in cyberspace. Cyberspace can be likened to a battleground. Thus, enhancing our 'warfare' defensive capabilities is imperative. As a widely acknowledged principle in jurisprudence, proactive measures are more effective than reactive measures in crime prevention.

Governments employ various strategies to prevent cybercrime, including enforcing the implementation of preventive measures, such as those set out in the following documents:

- **China** - Guiding Opinions on Promoting the Development of the Cybersecurity Industry (Draft for Comments)[20] and Measures for the Administration of Cybersecurity Threat Information Release (Draft for Comments)[21]

- **The US** - How to recognise & prevent cybercrime[22]

- **The EU** - Europol's cybercrime-prevention guides[23]

Additionally, governments can collaborate with private companies and other organisations to share information and resources, conduct system audits and assessments and implement robust data protection measures. By taking proactive steps to prevent cybercrime, governments can better safeguard their systems and networks and mitigate potential threats before they materialise into successful cyberattacks. Prevention is a crucial pillar in the fight against cybercrime; it plays a vital role in ensuring the security and resilience of cyber operations.

Moreover, many countries and regions have taken steps to enhance their security measures and prevent cybercrime, thereby raising the barrier to cybercrime occurrence and effectively reducing it. For instance, in 2017, numerous high-profile cyberattacks targeted organisations across different industries in Hong Kong, including licensed corporations (LCs) that are regulated by the Securities and Futures Commission (SFC). These attacks often involved hackers gaining unauthorised access to customers' internet-based trading accounts, resulting in unauthorised trades[24]. To address this issue, the SFC issued a directive mandating internet brokers to implement stricter security measures to combat cybercrime, such as the mandatory implementation of two-factor authentication for logins to clients’ internet trading accounts by licensed or registered individuals[25]. These efforts have reduced significantly the number of cyberattacks and the extent of financial losses.

## 3.3.2 Investigation

While all of the subjects have implemented legislation to combat cybercrime, there are significant differences in the legislative approaches adopted. While some countries have chosen to establish standalone legislation dedicated exclusively to cybercrime, some have opted to augment the provisions of their Penal Code by incorporating cybercrime-related contents. Notably, **South Africa, the UAE, the UK, the US** and **the EU** have legislation dedicated to cybercrime. The table below provides an overview of the dedicated laws implemented in each country.

The legislations in these countries defines the main types of cybercrime and their corresponding penalties. This legislative approach allows for supplementary provisions to be updated more effectively from a technical standpoint, offering greater adaptability to the evolving nature of cyber threats.

| | South Africa | UAE | UK | US | EU |
|---|---|---|---|---|---|
| **Law** | Cybercrimes Act of 2020[26] | Federal Decree Law Number 5/2012[27] | 1.Computer Misuse Act 1990[28]<br>2.The Data Protection Act 2018[29]<br>3.The Fraud Act 2006[30] | 1.Computer Fraud and Abuse Act<br>2.Electronic Communications Protection Act[31]<br>3.Many states have special regulations, NY Penal Law[32] | 2013/40/EU Cybercrime Directive[33] |

On the other hand, **Brazil, China, Germany, India, Mexico** and **Vietnam** have not introduced dedicated legislation for cybercrime. Instead, these countries have opted to amend their existing criminal laws or other relevant laws to address cybercrime. In Germany, cybercrime offences, jurisdiction and application are governed by a unified German Criminal Code[34], which determines the 'place of commission of the offence' for application purposes. In India, cybercrimes are covered by the Information Technology Act, 2000[35] and the Indian Penal Code, 1860 (IPC)[36]. The Information Technology Act, 2000 deals with issues related to cybercrimes and electronic commerce, and it includes stringent penalties and sanctions enacted by the Indian Parliament to protect the e-government, e-banking and e-commerce sectors. The scope of the Information Technology Act has been expanded to encompass all modern communication devices, including unauthorised access to and the damaging of a victim's computer without due permission.

**Chile** and **Singapore** adopted both approaches. In their early stages of combating cybercrime, they amended their existing penal codes. Subsequently, they enacted standalone cybercrime laws to further enhance their efforts in combatting cybercrime.

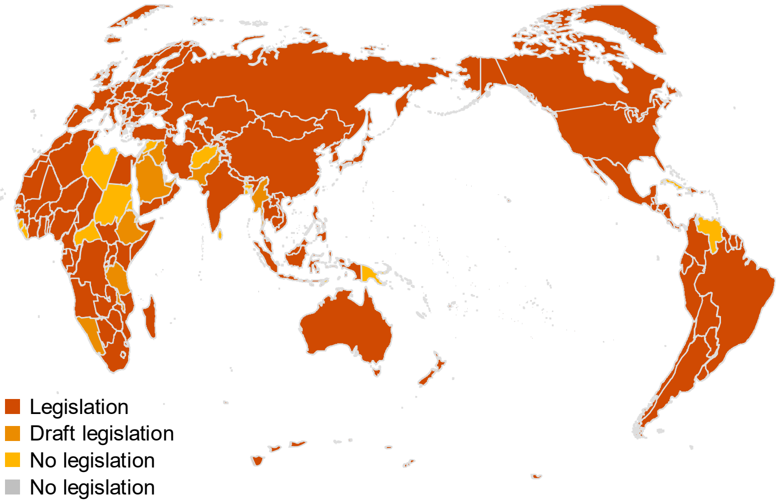
## 3.3.3 Recovery

After experiencing cybercrime, various governments would take measures to remedy and repair the situation to make up for the damage as soon as possible while paving the way for the prevention of similar losses in the future. Useful measures include cyber insurance, awareness-raising activities and post-mortem review.

# 3.4 Personal data protection

According to data from the United Nations[37], nearly 71% of countries have enacted data protection and privacy legislation. Based on our study, all subjects have enacted dedicated personal data protection laws, such as the EU's General Data Protection Regulation[38] (GDPR) and China's Personal Information Protection Law[39] (PIPL).

Data protection and privacy legislation worldwide



Source: UNCTAD, 14/12/2021

Our study found that the pathway for legislative publications in most countries is to release national cybersecurity law first, then personal data protection law. For example, the EU's cybersecurity law, Network and Information System Security Directive (NISD)[40], was implemented in 2016, while GDPR was implemented in 2018.

By studying the legislative contents of our sample, the framework for personal data protection law usually includes the following:

- Principles of handling personal data[41].
- Legal basis for data processing[42].
- Rights of the personal information subject.
- Rules for cross-border data transfer.
- Data protection authority.

### 3.4.1 Principles of handling personal data

Personal data protection laws usually include the following principles[41]: i) lawfulness, fairness and transparency; ii) purpose limitation; iii) data minimisation; iv) accuracy; v) storage minimisation; vi) integrity and confidentiality; and vii) accountability.

### 3.4.2 Legal basis for data processing

Before processing personal data, the question, ‘What is the reason for processing personal data?’ should be considered. It is clear that any processing of personal data is only lawful if it has a ‘legal basis’. At the same time, if there is no lawful basis for data processing, doing so will be unlawful. In addition, this study found that personal data protection laws in most countries stipulate six key legal bases for data processing, namely consent, the performance of a contract, compliance with a legal obligation, protection of vital interests, protection of public interest and protection of legitimate interest (which are also referred to as ‘businesses purposes for processing’).

### 3.4.3 Legislative status of personal data subject rights

Some countries’ personal data protection laws require data controllers to provide information to data subjects within a specified time frame regarding actions taken in response to their requests. However, there are also countries where their laws do not specify a response time. In addition, the study found that the personal data protection laws in certain developing countries, such as South Africa and Brazil, only grant limited rights to data subjects, which generally include the right to access, rectification and erasure/deletion.

### 3.4.4 Legislative status of cross-border data transfer

Many countries have gradually enhanced legislations to provide more details and guidance on implementing cross-border data transfer mechanisms. The current cross-border data transfer mechanisms under which personal data can be exported legally include the following two:

### 1. Transfer of data based on an adequacy decision

Most countries allow personal data to be transferred to countries where their privacy protection level can meet the provisions of the originating country's data protection law. In other words, the country or region to which the personal data is transferred has equivalent legislations in place on personal data protection to ensure the privacy and confidentiality of the personal data and enable data subjects to exercise their rights.

### 2. Transfers subject to appropriate safeguards

Personal data can also be transferred to countries that have not been recognised as having an 'adequate level of data protection'. Data can be transferred to countries that provide adequate safeguards[43] as a measure to enable cross-border data transfer to be made to a third country, ensuring adequate data protection. For example, Standard Contractual Clauses (SCC), which is a legally binding and enforceable instruments between public authorities adopted by local regulatory authority, and binding corporate rules (BCRs) can be used. This study also found that SCC and BCRs are the most commonly used data transfer tools for enterprises and businesses.

## 3.4.5 Legislation status of data protection authority

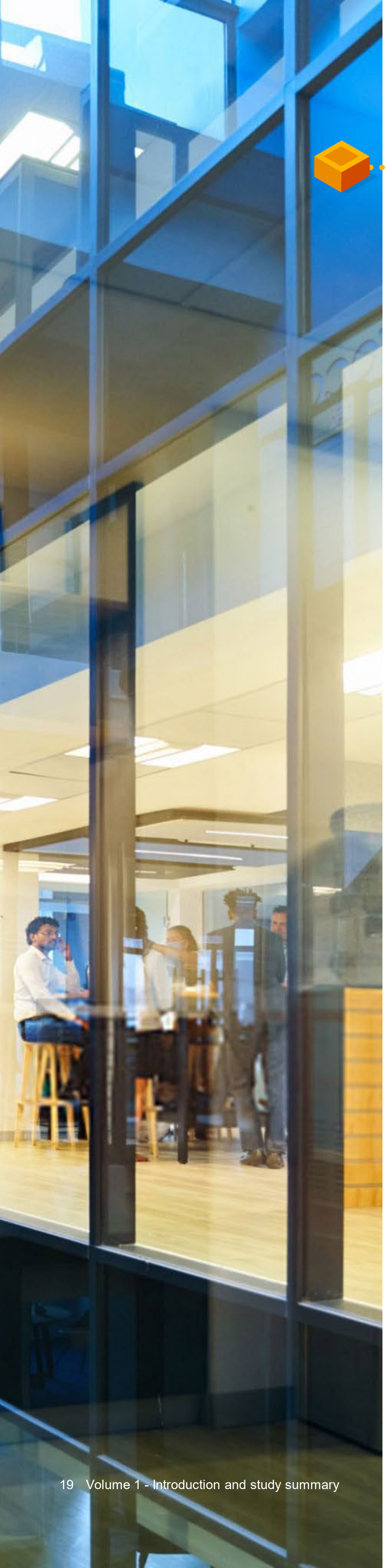
Although all samples of study strengthened supervision of personal data protection, their oversight and management method vary differently. This study found that Brazil, Germany and the EU, maintain a single privacy protection legislation with a single Data Protection Authority (DPA) entity mechanism.The DPA primarily has the following three regulatory responsibilities:

1. Investigatory: data protection audit, certification review, etc.

2. Authorisation and advisory: handle operations that require prior authorisation, approve corporate rules, etc.

3. Corrective measures and penalties: sanctions, order compliance, impose administrative fines, etc.

In contrast, the responsibilities of DPAs in Chile, China, India, Mexico and Vietnam are shared by different departments at the federal or sectoral level.



# 3.5 Non-personal data protection

## 3.5.1 Legislative framework

Non-personal data (NPD) protection is in its early stage of development. Only limited NPD legislations have been enacted at the time of this research, including the EU's Data Governance Act[44] and Free Flow of Non-personal Data in the EU[45], the UAE's Open Data Specifications Guidelines for the UAE Government Entities[46] and Smart Data Framework[47] and China's Data Security Law[48].

The study observed that NPD legislations generally include two components:

1. **General provision and introduction**: This section describes the definition and scope of NPD and the responsibilities of the NPD protection authority.

2. **Use of NPD**: This section describes the requirements for NPD sharing within the domestic public and private sectors, as well as cross-border transfer.

### 3.5.1.1 Scope and definition

The definition of NPD among the identified legislation is straightforward - 'data that is not personal data is NPD'. However, the scope of the identified NPD legislations varies from country to country. In China, the Data Security Law[48] applies to data processing activities within its territory. In the UAE, the Smart Data Framework[47] applies to entities wishing to use and share data originating in the UAE. In the EU, the Free Flow of Non-personal Data[45] applies to the processing of electronic data except for personal data. Regarding specific NPD legislations for regulating the government's ability to share public sector data, the UAE's Open Data Specifications Guidelines[46] and the EU's Data Governance Act[44] are examples of legislation developed to manage this aspect.

## 3.5.1.2 Roles and responsibilities for NPD authority

An NPD authority plays a key role in establishing, promoting and maintaining NPD legislations. In China, the Cybersecurity Administration is the NPD authority at the national level, providing high-level guidance to authorities and departments at the regional level on implementing NPD legislation. In the UAE, the Federal Data Management Office is in charge of implementing NPD legislation at the national level. As the EU consists of several member states, there are two levels of NPD authority within the region - the commission and the Competent Authorities. The Competent Authorities are responsible for developing and implementing the EU's NPD legislation at a state level, while the commission is responsible for being the central source of information at the EU level and overseeing the implementation of NPD legislation by the states' Competent Authorities.

Common responsibilities for the NPD authority include acting as a single official source of information for NPD legislation, establishing technical standards for the use of NPD, implementing disciplinary actions and maintaining a list of specified NPD entities. Examples include the UAE's Federal Data Management Office, which maintains a list of entities that have applied for an 'Open Data License'; the EU's Competent Authority, which maintains a list of registered data altruism organisations that provide technical advice and assistance; and China's CAC, which maintains a catalogue of essential data at the national level.

## 3.5.1.3 Use of non-personal data

We have observed three common areas regulated under the NPD legislation:

1. Domestic public sector data sharing;
2. Domestic private sector data sharing; and
3. Cross-border transfer of non-personal data.

NPD legislation also commonly features two principles for NPD usage: data interoperability and localisation.

## Domestic public sector data sharing

Based on our observation, public sector data is often shared with minimal restrictions, but the use of public sector data should adhere to the security requirements for the data classification/category it belongs to. For example, in the UAE, NPD can be classified as 'open data', 'confidential data' or 'sensitive data', with each having its own security requirement set out in the UAE's Cabinet Resolution No.21 of 2013, Regulation of Information Security at the Federal Entities, Article DC2.3 of the UAE's Smart Data Standards.

## Domestic private sector data sharing

As NPD generated in the private sector is vital to economic productivity, domestic transfer of private sector data is encouraged by NPD legislation. For example, the EU's Free Flow of Non-personal Data[45] emphasises the minimisation of data localisation. However, entities should still establish their own data security organisations to ensure data security when utilising collected data. China's Data Security Law[48], for example, requires the processors of important data to appoint a dedicated person and set up a data security organisation to ensure the data security of their daily activities.

In addition, among the legislation studied, we found that data interoperability is another key concern addressed in NPD legislation. On the one hand, countries, such as the UAE, have their Open Data Specifications Guidelines for the UAE Government Entities, which provide technical specifications that need to be followed for NPD. Hence, the data is understandable, shareable, reliable and used as intended. On the other hand, China, as well as the EU, for example, have not developed technical specifications like the UAE. However, NPD legislations in these jurisdictions outline the responsible party for supporting the implementation of data interoperability. In China, the CAC will advance the formulation of standards for data development, data utilisation technologies and data security[48]. In the EU, the European Data Innovation Board is tasked with proposing guidelines for a common European data interoperability framework[44].

## Cross-border transfer of non-personal data

Even though domestic free flow of non-personal data is broadly encouraged, some non-personal data is still considered important or critical and is prohibited from being shared with other countries. Certain requirements on cross-border NPD transfer and localisation were found within the sample. For instance, the EU has outlined the requirements for international access and transfer of NPD in Article 31 of the Data Governance Act[44]. China has set outlined rules on cross-border transfer of NPD in Article 31 of its Data Security Law[48]. In a nutshell, in terms of requirements for data localisation, data related to the government, banking and financial sector, credit status, health, critical infrastructure, and data generated from online or cloud services are, for the most part, required to be stored locally.

# 3.6 ICT vulnerability management

China[49, 50], Germany[6], the UAE[10], the UK[51, 52], the US[53, 54], Vietnam[12] and the EU[14, 55, 56], have legislations in place on ICT vulnerability management. There are two types of legislative models for ICT vulnerability management. One is established through dedicated legislation, and the other is incorporated into the broader cybersecurity legislation. ICT vulnerability management is a lifecycle process, and its legislation is often made up of four phases - identification, analysis and verification, mitigation and disclosure.

## 3.6.1 Identification

There are three ways to identify vulnerabilities - internal identification, monitoring public sources of vulnerability information and direct reporting of vulnerabilities to the organisation.

## 3.6.2 Analysis and verification

Some countries incorporate analysis and verification into their regulatory enforcement process. Using tools is a common way to assist in the analysis and verification process and includes automated testing tools, validation tools and the Common Vulnerability Scoring System.

## 3.6.3 Mitigation

Many countries have mitigation requirements in their regulations. For example, China's Cyber Product Security Vulnerabilities Management Regulations[50] state that after cyber product providers (Article 7) and network operators (Article 8) discover or have been notified that their networks, information systems or equipment have security vulnerabilities, they need to take measures to verify and remediate the known vulnerabilities in a timely manner.

## 3.6.4 Disclosure

Most countries have disclosure requirements in their regulations. Vulnerability disclosures usually include responsible disclosure, coordinated vulnerability disclosure, disclosure timeline, disclosure content and encouraged disclosure. Disclosure is the focus area of legislation on ICT vulnerability management, especially responsible disclosure. For example, the EU's NIS 2[14] states that reporters must comply with the proportionality principle - i.e. do not exploit vulnerabilities beyond what is strictly necessary to demonstrate the security problem - and reporters shall provide a clear and detailed description of the vulnerability to vendors or coordinators.

# 3.7 Awareness and capability

As a crucial component of cybercrime prevention and the development of cyber maturity, cybersecurity awareness and capacity building is of significant importance for all countries. However, the approach taken towards this issue varies among countries due to differing levels of national development and cybersecurity maturity. Some countries opt to enact dedicated legislation, such as China, the US, as well as the EU, while others have incorporated cybersecurity awareness-raising efforts within their national cybersecurity strategies or awareness campaigns.

China has placed great emphasis on raising cybersecurity awareness and has laid out specific requirements for such purpose in its cybersecurity law. The law explicitly mandates that the government and relevant departments organise and conduct regular cybersecurity awareness campaigns while also guiding and urging other entities to actively engage in cybersecurity education and publicity. Similarly, the US has addressed the importance of raising cybersecurity awareness in various laws and regulatory documents, such as the Gramm-Leach-Bliley Act[57]. The US has also issued a series of cybersecurity policies, national strategies, action plans, and presidential executive orders to help raise the cybersecurity awareness of citizens. In the EU, the recently revised NIS 2 Directive has delineated the responsibilities of government agencies and enterprises in each member state with regard to raising cybersecurity awareness. This directive provides a framework for promoting cybersecurity education and awareness at both the government and enterprise levels.

It should be noted that countries with dedicated legislation for raising cybersecurity awareness also implement complementary measures in addition to legal provisions, such as organising cybersecurity activities (such as national and/or sectoral cyberattacks drills) and issuing relevant national cybersecurity strategies to highlight its positive impact on society. Our study indicates that, with the exception of the three aforementioned countries, most countries do not yet have comprehensive legislations that specifically address cybersecurity awareness and capacity development. However, it is evident that more countries recognise the significance of raising public awareness about cybersecurity issues and have implemented other administrative measures accordingly. For instance, India does not currently have a dedicated legislation on raising cybersecurity awareness and education, yet it has implemented measures, as mentioned in its National Cyber Security Strategy 2020[59] emphasising the need to attract young talents to the field of cybersecurity through targeted awareness campaigns and enticing career opportunities. Additionally, October is declared as the Cyber Security Awareness Month (CSAM) globally[60], a range of posters and video campaigns were launched, and public surveys were conducted to assess the current level of cybersecurity awareness and identify areas for improvement.

CSAM is globally recognised as a collaborative effort between governments, industries, and individuals to foster dialogue and raise awareness about priority areas in cybersecurity. Through various awareness activities, CSAM encourages individuals, the workforce, and the community to adopt stronger security measures and work collectively towards creating a more effective security culture.

# 3.8 International cooperation

International cooperation in cybersecurity is more commonly mentioned in national cybersecurity legislation. For example, Article 42 of the EU's Cybersecurity Act states that 'ENISA may cooperate with competent authorities of third countries or with international organisations or both'[60]. Article 17 of the EU's NIS 2 Directives states that 'The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations'[14]. Article 7 of China's Cybersecurity Law states that 'the state shall actively carry out international exchange and cooperation in terms of cyberspace governance'[49].

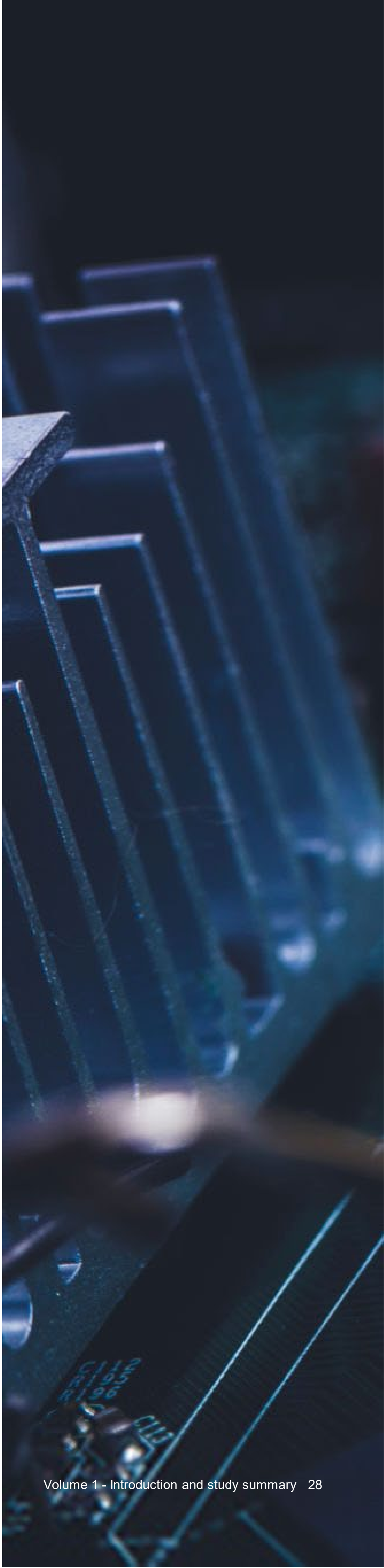
In addition, this study looks into the mechanism of international cooperation. In general, the cooperation mechanism can be defined as 'state-to-state cooperation' or 'state-to-private-sector cooperation'.

Under the 'state-to-state cooperation' mechanism, the relationship can be established through bilateral or multilateral partnerships. Currently, there are numerous bilateral agreements for international cooperation on cybersecurity among the sample with their alliance, e.g., the US-United Kingdom Cybersecurity Cooperation[61]; the UK-Australia Cyber and Critical Technology Partnership[62]; a Memorandum of Understanding (MoU) on developing capacity building of internet security and tech cooperation between China and Indonesia[63]; and an MoU for cybersecurity between China and Thailand[64].

Among the numerous multilateral cybersecurity partnerships, it is observed that partnerships are more commonly formed among countries with geographic proximity or countries that have already formed collaborative relationships in other areas. The table below is a non-exhaustive list of cybersecurity cooperation legislation and binding agreements noted within our sample.

| Legislation and binding agreements for cybersecurity cooperation within the sample | |
|---|---|
| **China** | Shanghai Cooperation Organisation: *Statement by the Heads of Member States of the Shanghai Cooperation Organisation on International Information Security*<br>The China-ASEAN Joint Declaration in the Field of Non-Traditional Security Issues of 2002 |
| **South Africa** | African Union Convention on Cyber Security and Personal Data Protection |
| **UAE** | Arab Convention on Combating Information Technology Offence |
| **US** | Organisation of American States: *Declaration Strengthening Cybersecurity in the Americas*<br>Organisation of American States*: Declaration on the Protection of Critical Infrastructure from Emerging Threats* |
| **EU** | NIS 2 Directives<br>Cybersecurity Act |
| **Global** | Convention on Cybercrime (Budapest Convention) |

For the 'state-to-private-sector cooperation' mechanism, it is a more important and widespread form of cooperation in view of a higher degree of flexibility that can be adopted. For example, the private sector has designed training for policymakers to improve their technical skills. Furthermore, enterprises have signed MoU with governments to help foster national cybersecurity capability. Under this mechanism, governments can leverage the knowledge and skills of the private sector. The partnership also provides greater opportunities for the private sector to contribute to developing national cybersecurity, efficiently enhancing the competitiveness of the cybersecurity technologies and solutions marketplace and further strengthening the overall national cybersecurity capability.



# 3.9 Cybersecurity technologies and solutions marketplace

The cybersecurity technologies and solutions market mainly includes three types of products and services – technologies (cybersecurity technologies and solutions), services and expertise and security management of outsourcing services.

## 3.9.1 Cybersecurity technologies

Some countries have stipulated cybersecurity technology control requirements in their regulations, which involve certification, risk assessment and standard security processes for cybersecurity technologies.

## 3.9.2 Cybersecurity services and expertise

Services and expertise laws and regulations often include talent training plans or arrangements at the national level. For example, in the US, the CISA[65] have three ways to build cybersecurity expertise and capacity, namely through the Cyber Career Pathways Tool, incorporating cybersecurity concepts into classrooms and advancing the cybersecurity profession with the National Initiative for Cybersecurity Education's Workforce Framework for Cybersecurity (NICE Framework) and the CISA's National Initiative for Cybersecurity Careers and Studies (NICCS). The NICE Framework is the foundation for increasing the size and capability of the US cybersecurity workforce. The NICCS is a national resource for cybersecurity awareness, education, training and career opportunities.

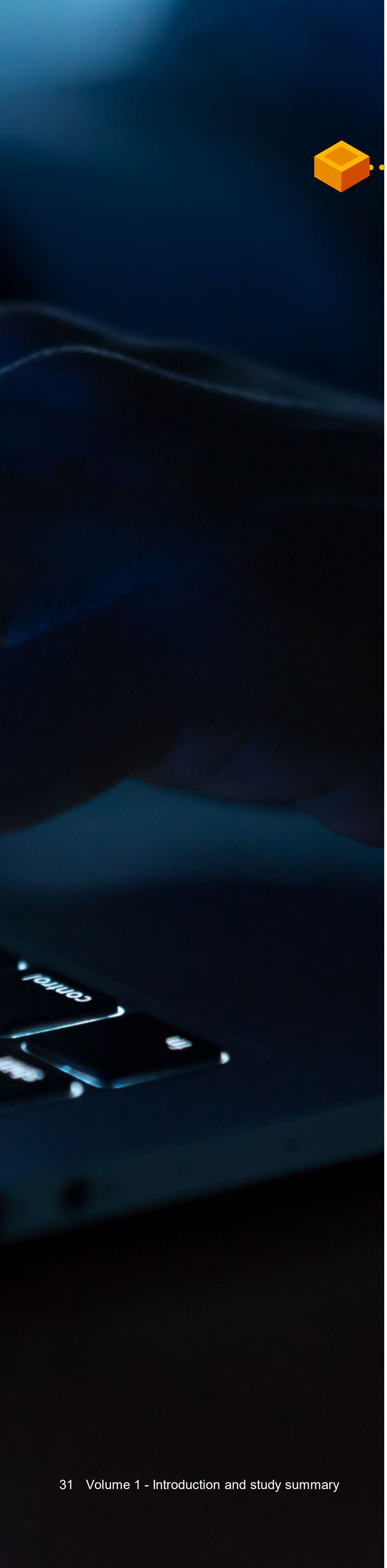
## 3.9.3 Security management of outsourcing services

The regulations in some countries cover the measures to mitigate the security impact of outsourcing. They are: conducting risk assessments; sharing responsibility; reviewing the practice of sub-tier suppliers; preparing an emergency response plan; and incorporating cybersecurity measures into contractual arrangements with suppliers and service providers.

# 4. Designing cybersecurity legislation

Our comparative study on the nine areas of cybersecurity found that there is ‘no one size fits all’ method when designing cybersecurity legislation. Every country has its unique national circumstances, development priorities and exposure to cyber threats. Furthermore, varying maturity levels in cybersecurity, unique stakeholder characteristics, and different approaches to governance contribute to the notion that designing cybersecurity legislation is a unique process for each country. Through extensive analysis and academic research, however, our study identified **five considerations** that are foundational, universally applicable and significantly beneficial for countries to take into account when designing their cybersecurity legislation:

1. Designing affordable cybersecurity legislation
2. Recognising cybersecurity as a shared responsibility
3. Strengthening cybersecurity baseline requirements to prevent cybercrime
4. Collaborating to solve cybersecurity problems
5. Balancing security and development



# 4.1 Designing affordable cybersecurity legislation

Affordability refers to a country's ability and capacity to design and enforce cybersecurity legislation. On the one hand, affordability addresses whether the public and private sectors have sufficient financial or human resources to coordinate and implement measures to meet the relevant requirements set out in the laws. On the other hand, affordability refers to whether the country's social, economic, and political situations allow the required measures to be adopted realistically. The World Bank also believes affordability is an essential consideration in designing policies, stating that 'no matter how technically sound a policy is, [programmes] are likely to fail if the public sector lacks capacity and institutional support to execute them'[66] .

Our analysis indicated that most countries have established cybersecurity measures in line with their affordability. We observed that, socioeconomically, more developed countries have enforced cybersecurity legislation with more stringent requirements and wider scope of coverage.

The concept of affordability may seem fundamental and elementary, and is self-explanatory that countries with greater capacity to allocate more resources will produce a more complex and comprehensive policy. However, our analysis also observed cases where a few countries pushed forward robust legislative standards and requirements when compared to other peer countries at a similar socioeconomic development level. When governments do not consider the factors addressed under affordability during policy design, they may experience costly consequences, called the 'Policy Implementation Gap' (PIG). The gap refers to the differences in the expected outcomes during the policy design stage and the actual results after implementation. Research conducted by the University of Kent explains that the occurrence of PIG can be attributed to one of two reasons – the lack of a realistic assessment of the implementation ability and the lack of multi-stakeholder collaboration[67]. Assessing the affordability of both the government and the complying stakeholders early in the design stage through active discussions may minimise the possibility of PIG.

## One way to minimise PIG: sectoral regulation approach

During our comparative study, we observed a distinctive approach that many sampled countries adopted while designing cybersecurity legislation. The approach, known as sectoral regulation, is to create regulations and guidelines to explicitly address a single particular sector or industry.

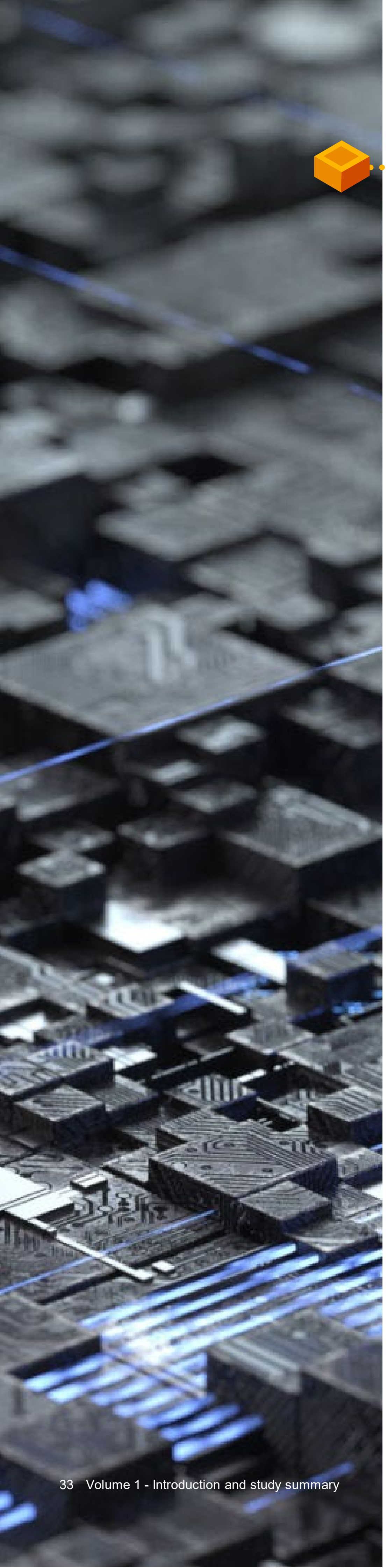
A noteworthy trend was how countries with relatively lower socioeconomic development levels enacted sectoral regulations prior to drafting national cybersecurity legislation. Research indicated that such an approach can minimise complexity and maximise efficiency.

Numerous scholars argue that the multi or cross-sector regulation approach is highly complex and runs the risk of low practicality. Schwartz and Satola, scholars from the World Bank, argue that establishing a legal framework for a multi-sector regulator (MSR) is more complex than creating one for a single-sector regulator (SSR)[68]. Moreover, the Software Alliance (BSA), a multinational technology innovation public policy group, also argues that although cybersecurity does apply to all industries, there is a need for tailored guidance to address the 'unique risks or specific operations in certain sectors based on their business needs' [69]. Laffont and Tirole, from the Massachusetts Institute of Technology Press, argue that an SSR 'may [be] better able to specialise and develop industry-specific expertise' than an MSR[70]. In other words, a sectoral regulation approach may enable lawmakers and regulatory bodies to better understand each sector's cybersecurity situation and needs. The enhanced level of understanding, in turn, may lead to policies that align with the capacity and affordability of both the enforcing regulators and the complying stakeholders. Ultimately, this would minimise policy implementation gaps.

We identified numerous sectoral regulations across a diverse range of industries within our sample. One commonality observed was the presence and comprehensiveness of cybersecurity regulations in the finance and banking sector. This might be an indicator that there is an urgent need for cybersecurity measures in that particular sector. Based on the unique national circumstances and needs, this paper does not intend to suggest a standardised order for all countries to follow when deciding which sector to prioritise their cybersecurity legislative efforts on. However, there are two factors that countries should consider when making their tailored lists.

The first factor is whether the sector contains critical infrastructures (CIs). CIs, as the backbone of a country's major operations, are increasingly digitised across the globe. Thus, strengthening the cybersecurity of CIs is of paramount importance. Complementing this first factor, governments should also consider prioritising sectors that face the highest frequency of cyberattacks. As mentioned earlier, all of the countries in our sample have put in place sectoral cybersecurity regulations in the finance and banking sector. This aligns with IBM's global cyberattack trend analysis, which identified the finance and banking sector as the recipient of the largest number of cyberattacks from 2016 to 2020[71].

Considering these two factors, countries may consider prioritising certain sectors, including but not limited to banking and finance, energy, transportation and insurance.



## 4.2 Recognising cybersecurity as a shared responsibility

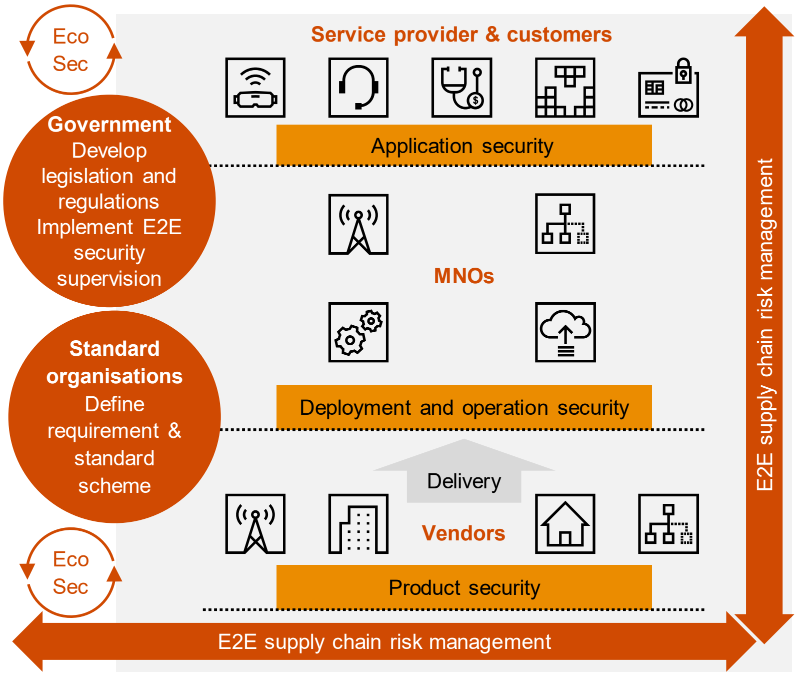
Connectivity is the foundation upon which the benefits of digitisation lie. The quick and boundless transfer of information through cyber space enable people to connect with significantly improved efficiency. The enhanced collaboration has allowed organisations to solve complex problems and create innovative solutions. However, due to high connectivity, the risks of and exposure to cyberattacks are also increased significantly. A successful attack on one channel may easily open the doors to another connected device or network. Thus, all stakeholders in society, including the government, private sector and individual citizens, have a role to play in establishing and practicing cybersecurity measures. Cooperation under the recognition of shared responsibility is the foundation of building a holistically safe and secure digital environment.

Scholars from the Centre for Strategic & International Studies argue that although there are things that only governments can do for cybersecurity, it is unrealistic to expect governments to handle all the risks and threats[72]. When guiding national cybersecurity development, governments should recognise the nature of shared responsibility for cybersecurity. Policies and regulations should reflect this and promote collaboration, discussion and reasonable sharing of responsibilities.

In many cases, stakeholders with deeper technical expertise, such as service providers or equipment vendors, are sometimes assumed to have to own more responsibilities for cybersecurity. The responsibilities should be shared among the stakeholders in a reasonable and clear manner. Governments should understand the importance of collaboration among the diverse range of industries operating in society through multi-stakeholder discussion, and through this, produce practical and accountable legislation. For example, the Groupe Speciale Mobile Association (GSMA), a renowned research institution in the telecommunications sector, produced a 5G cybersecurity shared responsibility model that illustrates the transparent and fair sharing of responsibilities among diverse stakeholders.

**Shared responsibility example**

*GSMA's shared responsibility model for 5G cybersecurity*



Eco Sec
Government
Develop legislation and regulations
Implement E2E security supervision
Standard organisations
Define requirement & standard scheme
Eco Sec
Service provider & customers
Application security
MNOs
Deployment and operation security
Delivery
Vendors
Product security
E2E supply chain risk management
E2E supply chain risk management

Source: GSMA

With the growing adoption of 5G network infrastructure globally, establishing 5G cybersecurity is also increasingly moving into the spotlight.

The Groupe Speciale Mobile Association (GSMA) produced a shared responsibility model that enables a holistic 5G cybersecurity establishment with responsibilities clearly shared among diverse stakeholders[73].

The model suggests that at the product level, vendors, such as equipment or device suppliers, should have security assurance processes throughout product development and its lifecycle. At the network level, the mobile network operators (MNOs) should ensure sound security management of the network infrastructure. At the application level, the application developers, service providers and device users should actively cooperate to protect the 5G network. Throughout all levels, governments should develop regulations to supervise each stakeholder in fulfilling their roles and responsibilities. Moreover, standard-setting organisations should provide support by clearly defining requirements for operators to follow.

According to the model, the diverse range of stakeholders should take up their corresponding roles and responsibilities throughout the entire 5G cybersecurity value chain. Not only do vendors and MNOs need to manage the technical aspects of cybersecurity, but device users, governments and standard organisations also need to be actively engaged in establishing a holistically secure 5G environment. Although the model is designed for the 5G sector only, it is an exemplary model that countries may refer to when applying the notion of shared responsibility in all areas of cybersecurity.

# 4.3 Strengthening cybersecurity baseline requirements to prevent cybercrime

The United Nations Office on Drugs and Crime (UNODC) classifies the contents of cybercrime law into Substantive, Procedural, and Preventive categories[74]. Similarly, our comparative analysis identified three components of cybercrime law: Prevention, Investigation, and Recovery (Section 3.3). Our analysis also noted that investigations and penalties were the dominant approaches governments took in the earlier stages of addressing cybercrime. However, in the recent decade, we have observed a shift in the trend for combatting cybercrime - from investigation to prevention. Such a shift could be due to a better understanding of the challenges around investigation and the high efficiency through prevention measures.

## Challenges in investigation

Our analysis identified numerous research papers[75, 76], that shed light on the challenges in investigating cybercrime. A report jointly published by Europol and Eurojust on 'Common Challenges in Combating Cybercrime' states that a key challenge investigation authorities face is collecting electronic communication data (ECD), which is 'the key to [the] successful investigation and prosecution of cybercrime'[77]. ECD is personal or non-personal information collected, usually by service providers in the private sector. Since this data is linked closely with privacy concerns, companies are often sensitive and reluctant to share this form of customer data with investigators. The fear of liability and potential privacy infringement hinders data collectors from freely supporting investigation authorities. On top of that, the rapid development of data encryption technology has further complicated the processing of ECD. Numerous communication services platforms have adopted data anonymisation and encryption policies into their service operations, which resulted in offenders exploiting these technologies. Consequently, collecting and using ECD, which is essential for investigation, 'requires many resources, incurs long delays, and carries privacy concerns'[77].

Another challenge is the absence of a unified legal framework across governments that enables the free flow of data and clarifies jurisdiction in boundless cyberspace. Cybercrime, especially large-scale attacks, usually occurs across geopolitical boundaries. Thus, investigation of cybercrime usually requires cross-border data transfer. As our analysis on cross-border data transfer (Sections 3.4-3.5) suggests, even when data evidence is available, sharing it with the country in need may require a significant amount of time and effort. Furthermore, while cybercrimes are committed in borderless cyberspace, geopolitical jurisdictions and ununified regulations give rise to confusion and conflict on who should investigate and penalise the offenders.

Investigation of cybercrime is, indeed, an essential component in the war against cybercrimes. However, it is crucial for governments and businesses, especially those with resource constraints, to recognise the limitations, affiliated risks and affordability of investing significant resources into investigating cybercrimes.

## Higher efficiency through prevention

The logic behind cybercrime prevention is increasing the difficulty and the cost of committing cyberattacks so that the return on the crime's investment is reduced and so is the incentive for cyber criminals. As mentioned earlier, governments are increasingly shifting their attention from investigating to preventing cybercrime. Numerous research and experts suggest that even a marginal increase in cyber resilience, especially among individuals or small and medium-sized enterprises (SMEs), may create a significant deterrence effect. For instance, simply adopting multi-factor authentication (MFA) for online accounts can prevent 99.9% of automated cyberattacks[78, 79, 80]. Establishing fundamental baseline requirements that raise the basic level of security across stakeholders may produce significant drops in cybercrimes. Baseline refers to fundamental procedures, guidelines or standards that establish a foundational level of cybersecurity. There are numerous approaches and methods that can establish a baseline. Below, we explain two well-recognised frameworks which countries may utilise to develop their baseline requirements.

The first is the Multi-Layered Defence (MLD) framework. It is a security approach that adopts and deploys multiple security controls and components, referred to as layers, in a system so different components may cover each other's flaws or gaps[81]. The 'layer' in this security concept does not refer to the implementation of multiple of the same security tools. The layered security approach adopts multiple types of protection mechanisms against diverse vectors of attack[82]. Some examples of security layers include firewalls, patch management, multi-factor authentication, endpoint protection, email filtering, awareness training and physical security. While there may be some overlapping characteristics among these security measures, the core area of protection for each is distinct. The different layers work together to bolster defence and establish a stronger foundation for secured cyber operations. Adopting an MLD framework as the baseline in cybersecurity would 'effectively build resilience to prepare for, respond to, and recover from cyberattacks'.

The other framework is the Zero Trust security model. As the model's name suggests, Zero Trust articulates a premise that an actor can be trusted only after being sufficiently vetted. It is based on the assumption that the source of a cyberattack can be anyone, anywhere or anything[83]. With this stringent vetting process for all actors before gaining access rights to systems, sensitive information is protected holistically from both external and internal threats.

Singapore, for instance, has adopted both frameworks in its 'Cybersecurity Code of Practice for Critical Information Infrastructure (CII)'. Under its section 3.5, 'Cybersecurity Design Principles', sub-section 3.5.2 urges CII operators to adopt, to the extent possible, MLD (Singapore uses the term 'defence-by-diversity') and Zero Trust principles 'in relation to its people, process and technologies to reduce cybersecurity risks to the CII'[84]. Incorporating concepts such as MLD or Zero Trust as baseline requirements is not solely about providing technical guidelines for stakeholders to follow. More importantly, they intend to raise awareness and shape stakeholder mindset with alert, comprehensive and defence-oriented cybersecurity ideologies. The baseline requirements, however, must ensure that stakeholders have the capability or sufficient support to fulfil their obligations. If not, the occurrence of PIG may be inevitable.

# 4.4 Collaborating to solve cybersecurity problems

As cybersecurity should be a shared responsibility, the process of establishing it involves multiple stakeholders and requires effective communication. Discussion and collaboration are essential elements of finding and enforcing solutions to address cybersecurity issues. There are two well-recognised collaboration methods - Multi-Stakeholder Partnership (MSP) and Public-Private Partnership (PPP). These modes of partnership are not only beneficial but fundamental in designing and enforcing cybersecurity legislation.

## Multi-Stakeholder Partnership (MSP)

It is vital to understand stakeholder affordability, responsibilities and needs when designing cybersecurity legislation. A well-recognised method to attain such an understanding is MSP. The Partnering Initiative (TPI), one of the global pioneers in the field, defines MSP as 'different societal players working together, sharing risks, and combining unique resources and competencies to address challenges or exploit opportunities in ways that one cannot achieve alone'[85]. Partnership 2030, a research group advocated by the United Nations' MSP Charter, identifies MSP as a partnership where the 'public sector, private sector, civil society, and academia work together as equals through an organised and long-term engagement in order to contribute to the common good'[86]. The noteworthy points under these definitions are the diversity in stakeholders, the equality among them, the sharing of risks and resources and the achievement of collective objectives.

According to Global Partners Digital (GPD), successful MSP cases ensure effective stakeholder engagement by creating an open, inclusive, transparent and accountable collaboration environment. The value of MSP is generated from the transfer of knowledge, information and resources between stakeholders. Hence, building trust and confidence among them is essential for fully realising the value of the model. MSP can produce the most desired outcomes if stakeholders are confident that their voices are heard equally and that the system is non-discriminatory, unbiased and transparent[86]. Partnership 2030 aligns with this view,

stating that the essential characteristics of a successful MSP are 'non-discriminatory identification of relevant stakeholders and an equal opportunity for stakeholders to participate and benefit from the partnerships'[87].

Adopting an MSP approach in legislation design and implementation is well-recognised by scholars across the field[88]. In the realm of cybersecurity, MSP has been a widely considered topic in international discussions. The Global Conference on Cyber Space (GCCS) has repeatedly highlighted the importance of adopting MSP in developing cybersecurity policies. The conference chair's statement articulates that 'governments are urged to ensure that cyber [policies] at [the] national, regional and international [levels are] developed through multi-stakeholder approaches [that include] civil society, the technical community, businesses and governments across the globe'[89]. Furthermore, the UN Group of Governmental Experts, in its 2015 report, also supported the use of the MSP model in addressing cybersecurity problems by stating that governments 'would benefit from the appropriate participation of the private sector, academia and civil society'[90].

When devising solutions for cybersecurity problems, different stakeholders can bring unique values and perspectives to the table. The private sector is well informed on the forms of cyber threats businesses face, products and innovations available in the market, or if there are any PIGs. The academia can introduce the latest research findings, aggregate insights from international forums or educate future talents. Civil society addresses the human rights implications of security policies, assesses the impact of policies on different members of society and draws attention to areas requiring more prioritised attention[91]. Within the public sector, relevant ministries, agencies, judiciaries, law enforcement bodies, or national defence authorities can each provide unique and diverse opinions that can be insightful for devising solutions to cybersecurity challenges[92]. The following examples from Mexico and India illustrate how an MSP can be adopted for solving cybersecurity problems.

## MSP examples

### Mexico

In the early days of cybersecurity establishment, the Mexican government and the Organisation of American States (OAS) coordinated a roundtable discussion where diverse stakeholders and experts gathered together to understand Mexico's cybersecurity status and its future direction[93]. Not only did technical specialists join the discussion, but academic scholars, businesses from the industrial and financial sectors, and stakeholders from civil society also made their voices heard. Furthermore, the government hosted a series of workshops inviting international experts from across the globe to discuss the topic with representatives from the legislative and executive branches of the Mexican public sector[94].

These discussions yielded a set of expert recommendations to guide Mexico's national cybersecurity framework and strategy. Moreover, the Mexican government gained access to greater resources and insights from the private sector for a more comprehensive and accurate assessment of the country's cyber-readiness and maturity level[94].

### India

India introduced the Indian Cyber Crime Coordination Centre (I4C) scheme in 2018 to strengthen its efforts in combatting cybercrime through multi-stakeholder cooperation[96]. The scheme is a highly comprehensive initiative encompassing projects related to crime investigation, research and development, legislative amendment and international cooperation. The National Cybercrime Threat Analytics Unit (TAU) was formed, along with numerous other projects, under the scheme to 'provide a platform for law enforcement personnel, persons from private sectors, academia and research organisations to work collaboratively on threat intelligence reports'. The scheme also founded the Cybercrime Ecosystem Management Unit, in which academia, industry experts and government authorities collaborate on cybercrime investigations[97]. Furthermore, the National Cyber Research and Innovation Centre was also established to invite diverse stakeholders from academia, the private sector, and inter-governmental organisations to leverage their expertise on emerging technological development and potential associated vulnerabilities[98].

The Mexican and Indian examples demonstrate the benefits of incorporating MSP into cybersecurity issues and the versatile ways in which MSP can find solutions to address cybersecurity issues. There is no standardised ‘correct’ method of forming an MSP. However, as mentioned earlier, the most desired outcomes of MSP can be produced under a non-discriminatory, neutral and transparent platform for dialogue where stakeholders are confident that their voices are heard with equal standings. Under the MSP model, expertise and resources can be shared, and the affordability, responsibilities, and needs of relevant stakeholders can be understood. These benefits all contribute to minimising the extent of PIG. As the central coordinator for society, governments carry the role of identifying the relevant stakeholders and creating effective channels for dialogue and discussion.

## Public-Private Partnership (PPP)

After identifying challenges, affordability and potential solutions through multi-stakeholder discussions, governments, in many cases, cooperate with the private sector to enforce the implementation of action plans. Such cooperation between the public sector and private entities is referred to as Public-Private Partnerships (PPPs). The following is a non-exhaustive list of PPP cases noted in our sample.

**PPP in national cybersecurity commitments and initiatives**

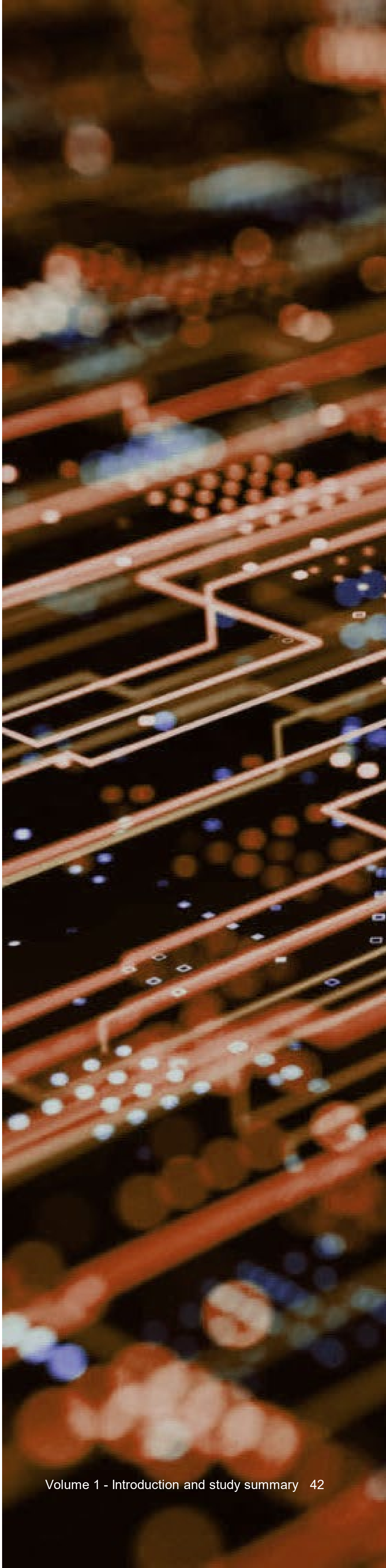
| Country/region | Documents/initiatives |
|---|---|
| Chile | First Latin American country to join Microsoft’s Government Security Program (GSP), which offers governments cybersecurity information[99].<br>The Chilean attorney general’s office signed a collaboration agreement with Microsoft to receive consultation on investigating cyber criminals[99]. |
| India | Kerala’s Cyberdome: a PPP initiated by Kerala’s police department to collaborate with private cybersecurity entities on reactive and preventive cyber incident management. The initiative has been replicated in Assam, Maharashtra, Gujarat and Tamil Nadu[100]. |
| Singapore | Singtel Cyber Security Institute - workforce development and education institution created by Singapore Telecommunications Limited in partnership with Economic Development Board, FireEye, Symantec, and Palo Alto Networks[101]. |
| South Africa | The National Cybersecurity Policy Framework (NCPF) repeatedly stresses the implementation of government-led PPP[102]. |
| UAE | Cyber Pulse Innovation Centre: a joint initiative between the UAE government, Abu Dhabi Polytechnic and Huawei for training talent on cybersecurity[103].<br>The UAE Cybersecurity Council signed an MoU with Huawei to collaborate on promoting innovation, strengthening national strategies and driving capacity development[104]. |

**PPP in national cybersecurity commitments and initiatives**

| Country /region | Documents/initiatives |
|---|---|
| UK | PPP is strongly supported by the national cybersecurity strategy. The Centre for the Protection of National Infrastructure (CPNI) conducts information exchange with private entities at a sector-specific level, which includes approximately 14 sectors. |
| US | Executive Order 13636 for Improving Critical Infrastructure Cybersecurity: the National Institute for Standards and Technology (NIST) is tasked with cooperating with private sectors in building a cybersecurity framework by identifying industry best practices and voluntary consensus standards[105].<br>The US Department of Homeland Security (DHS) implemented a cyber-threat information sharing program that automates the rapid and timely transfer of threat information between the public and private sectors[106]. |
| EU | European Public-Private Partnership for Resilience (EP3R)[107]<br>Cooperative Models for Public-Private Partnership (PPP)[108] |

The table above illustrates how governments across the world are utilising diverse forms of PPP to address different cybersecurity challenges. The PPP model has been adopted to build cybersecurity frameworks, protect national critical infrastructures, report incidents and vulnerabilities, train future talents, educate government authorities and investigate cybercrime. Governments are taking such profound and extensive PPP measures because of the inseparable nature of establishing national cybersecurity with the private sector, and the ‘synergistic effect of sharing innovative resource use and application of management knowledge” that partnering with the private sector creates[109].

Scholars such as Kruhlov, Latynin, Horban, and Petrov argue that PPP is ‘increasingly seen as addressing many of the challenges posed by cybersecurity management’ because of the ‘existing network communications, server equipment, and highly specialised professionals […] in the private businesses’[109]. From establishing ICT infrastructures and designing technical safety regulations to information exchanges to investigating and preventing cyber threats, the expertise of the private sector is needed in all areas to establish cybersecurity. Furthermore, in many countries, numerous essential services, including critical infrastructure, are handled by private entities. The following case study on Singapore part 1 explains how Singapore has privatised over 40 Government-Linked Companies (GLCs), including numerous CIs, in the past three decades. Thus, it is not just beneficial but fundamentally important for governments to cooperate with private sector bodies in addressing cybersecurity issues. Part 2 of the case study further illustrates two different approaches Singapore has taken in its cybersecurity PPP efforts.



## Case study on Singapore's Public-Private Partnership

### Part 1: The private sector presence in Singapore's CI sector

Since its independence in 1965, Singapore has adopted a state-led development approach to establish its national infrastructure and economy. The state-owned enterprises, known as Government-Linked Companies (GLCs), ran various vital sectors that served as the foundation of the country's operation. In 1985, however, an economic recession hit the country, which shed light on the need for higher operational efficiency and productivity. To address the challenge, Singapore took a deregulation and privatisation approach so that market forces may drive the country out of economic stagnation. Over the following decades, more than 40 GLCs were privatised, including numerous critical infrastructures (CI). Today, with strong private sector ownership across its CI sectors, it is not a choice but a natural course of action for the Singapore government to partner closely with private sector owners to address the cybersecurity of its CIs.

### Part 2: Singapore's Public-Private Partnership (PPP) in cybersecurity

We observed two different approaches Singapore took in establishing PPP in cybersecurity.

One approach is based on a variation of the Design-Build-Finance-Operate (DBFO) model, in which the government procures private entities to design, build, finance, and operate public projects under a contractual agreement with set terms and public grant supplements[110]. The method shares risks, responsibilities and resources in delivering public service projects with private sector contractors who have the expertise and economic incentives[111]. An example is the Cyber-Watch Centre (CWC) implemented by the Infocomm Development Authority of Singapore (IDA) in 2007. The CWC was established utilising the DBO model. IDA appointed e-Cop Pte Ltd, a managed security and monitoring services firm, to design, build and operate the CWC[112]. The Centre has successfully monitored cyber threats that the government network received and provided an early warning system for efficient prevention and remediation[112]. In 2022, the CWC was replaced with the Government Cyber Security Operations Centre (GCSOC), which is now under the commission of the Government Technology Agency (GovTech)[113]. While there are standalone cybersecurity PPPs like the CWC project, other procurement PPP projects, such as infrastructure projects, often include cybersecurity requirements as part of the overall contract[111].

Another PPP approach is establishing an MoU. An MoU is a form of agreement that outlines the common understanding of the action, partnership, commitment and outcome. However, it is not a legally binding agreement or an enforceable contract. It is a stepping stone for two parties to explore and develop a formal relationship[114]. Instead of a top-down regulation that forces the private sector into serving the needs of the public sector, Singapore's MoU approach intends to consider the opinions and affordability of the private sector partners. Only after extensive discussions and successfully establishing collaboration will the MoU progresses into a binding agreement that specifies human and financial commitments. The Cyber Security Agency of Singapore (CSA) signed numerous MoUs with a diverse range of private sector partners, including Singtel, FireEye, Microsoft, Palo Alto Networks and CheckPoint Software Technologies, on various areas of cybersecurity. These MoUs led to significant contributions to Singapore's cybersecurity research and development, information sharing and workforce development[111].

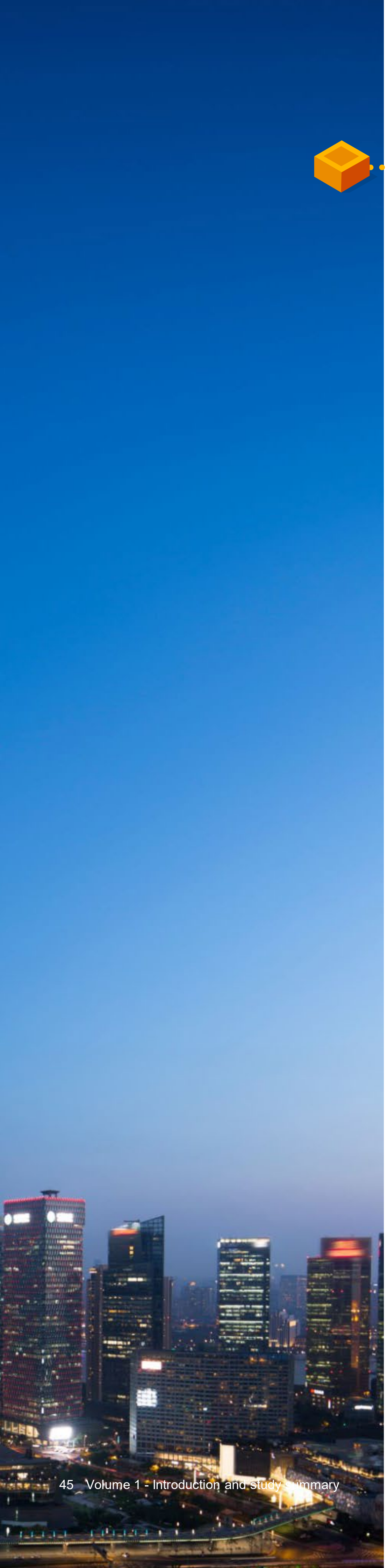
The cases under the two approaches demonstrate how PPP enabled Singapore to harness the expertise and efficiency of the private sector to be able to more effectively implement cybersecurity measures, and create a more secure digital environment in Singapore.

## International cooperation

Under both the MSP and PPP cooperation models, an integral element governments must consider is expanding the scope of partnership beyond domestic stakeholders. As our comparative analysis on international cooperation (Section 3.8) suggests, forms of cooperation include inter-governmental dialogues or treaties, partnerships between governments and foreign private entities, NGO-initiated partnerships and dialogue programmes, or a combination of the above.

As we can see from Mexico's MSP example and PPP examples from Chile, governments are reaping significant benefits from inviting foreign public and private entities into the development of domestic cybersecurity solutions. Furthermore, governments are also engaging themselves in global dialogues. There are multilateral initiatives, such as the Global Conference on Cyber Space (GCCS) or the Budapest Convention, that enables the sharing of knowledge and resources within the global community. Regional or bilateral cooperation also enhances the depth of partnerships, e.g., the African Union Convention on Cybersecurity and the China-ASEAN Cybersecurity Communication and Training Centre. Especially for countries in the earlier stages of socioeconomic development, and with low cybersecurity maturity, the expertise and resources of foreign stakeholders open opportunities that cannot be otherwise harvested within the limited domestic landscape. Capacity-building cooperation provides opportunities to benchmark successful legislation, learn from past experiences of industry-leading partners and receive advisory support from a broader range of expertise.

The OECD report on 'cybersecurity policy making' states that 'capacity building of less developed countries is shared as key objectives by most strategies'[115]. Resonating with the notion of shared responsibility, incorporating international cooperation in MSP and PPP would empower nations to fulfil their roles as a member of the global cyber arena. Thus, international cooperation is essential in building comprehensive cyber resilience for both the domestic and global communities.



# 4.5 Balancing security and development

The final consideration addresses the fundamental objective and nature of establishing cybersecurity while not hindering the development of society. Technology advancement and the proliferation of digitisation opened a new chapter on how societies, businesses, and governments operate. While the growth potential spurred by cyber development is boundless, it can also be reckless if not managed carefully. Cybersecurity legislation is to set up guardrails to guide and protect people on their path of development. Government's role should be to ensure the security of their countries and its people in this rapidly expanding digital environment.

Having excessively stringent security measures, however, may produce the unintended consequence of hindering the development of societies and economies. Although the intent of protecting society from cyber threats is well-recognised, having excessively stringent security measures may shadow opportunities for innovation and progress. In the name of security enhancement, legislation may blindly place excessive responsibilities on compliance with stakeholders that they cannot afford. Such measures may be unsustainable and suppress stakeholders' ability to grow and innovate.

We must recognise that enhancing cybersecurity and attaining economic development are two sides of the same coin. We cannot accomplish one without the other. Economic development cannot be sustainable without a secure digital environment, and cybersecurity is meaningless when economic development is stagnant.

Designing good cybersecurity legislation is, thus, finding the right balance between security and development. The right balance would create a secure digital environment that stimulates sustainable ICT development - the kind of development that would allow the growth of our digital economy and enable the betterment of people's livelihoods. By placing such ideology and mindset at the core of designing cybersecurity legislation, governments may bring stakeholders together with a shared and unified vision of secure development.

# 4.6 Case study: an analysis of the Electronic Communication Services Act of Finland

The Electronic Communication Services Act of Finland well reflects some of our considerations.

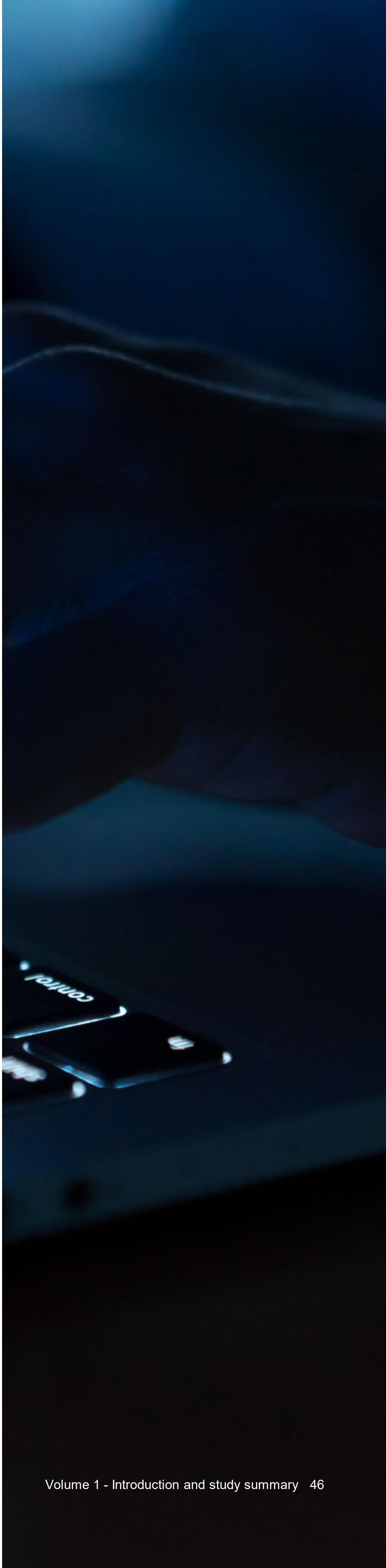
## Background

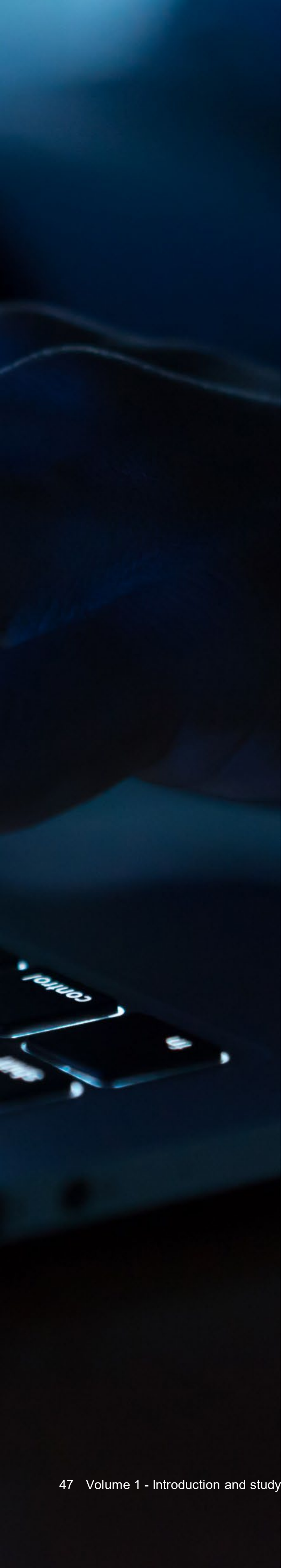
In January 2020, the European Commission published a set of ‘soft laws’ called the EU 5G Toolbox for member states to follow when designing national security measures for 5G deployment[116]. The commission left the specifics of the regulations up to each government to decide. Following the announcement, the EU member states took divergent approaches to produce 5G cybersecurity regulations and implementation frameworks based on their national circumstances[117]. As one of the earliest adopters, in December 2020, Eduskunta, the Parliament of Finland, passed the Electronic Communication Services Act, which details regulatory guidelines on the ‘who, what and how’ of managing 5G cybersecurity in Finland[118].

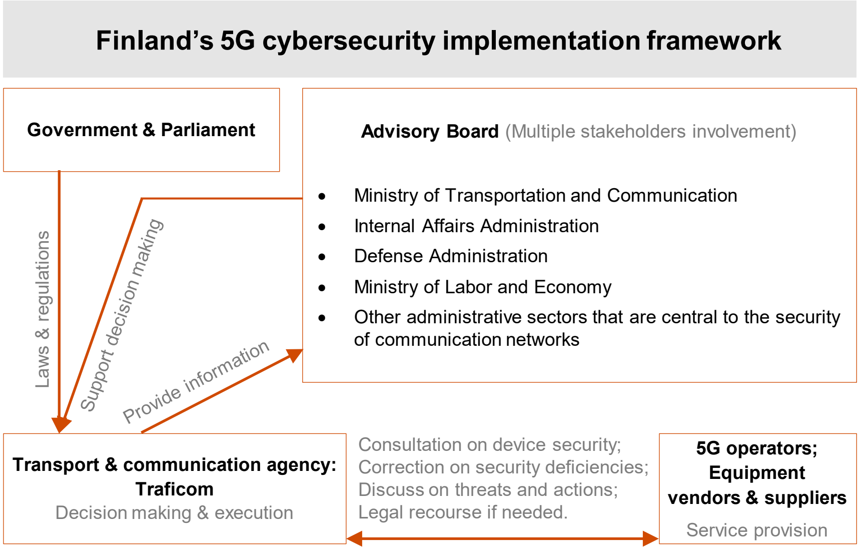
## Implication for the considerations

Finland is recognised by numerous scholars and experts as one of the pioneers of 5G technology, leading the progressive development of 5G infrastructure in the European region[119]. The Finnish Act provides a comprehensive framework for assessing ‘communication network devices used in critical parts of the public communication network’.

The following table is a visual illustration of Finland’s 5G cybersecurity implementation framework. The government and the parliament provided legal guidance and appointed the Transport & Communication Agency (Traficom) as the central decision-making body. Traficom communicates with a range of stakeholders, conducts security assessments and enforces necessary measures to ensure the security of the 5G network. Traficom has two-way communication channels with the Advisory Board, 5G operators and equipment vendors.







**Finland's 5G cybersecurity implementation framework**

**Government & Parliament**

**Advisory Board** (Multiple stakeholders involvement)

- Ministry of Transportation and Communication
- Internal Affairs Administration
- Defense Administration
- Ministry of Labor and Economy
- Other administrative sectors that are central to the security of communication networks

**Transport & communication agency: Traficom**
Decision making & execution

Consultation on device security;
Correction on security deficiencies;
Discuss on threats and actions;
Legal recourse if needed.

**5G operators; Equipment vendors & suppliers**
Service provision

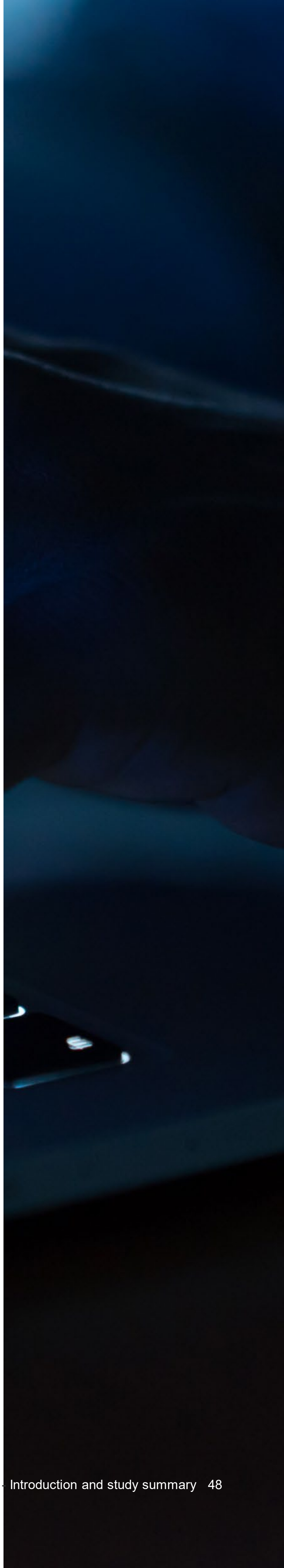
Section 244b of the Act stipulates the creation of an Advisory Board to comprehensively evaluate and monitor the development of the communication networks as well as the implementation of legislative practices regarding network security[120]. As illustrated in the above table, a wide range of stakeholders from various ministries and administrative sectors are represented on the board. Expert opinions and potential concerns from the fields of defence, foreign affairs and labour are incorporated into decision-making for 5G cybersecurity issues. The advisory board provides recommendations to Traficom on how to improve security measures and legislation[120]. Integration of multiple stakeholders with diverse backgrounds, expertise, and resources enables the decision-making body to guide the country's 5G cybersecurity legislation from a comprehensive perspective.

The Act also requires Traficom to engage in mutual discussions with 5G operators and equipment vendors. 5G in Finland is primarily operated by three major companies, namely DNA, Elisa and Telia[121]. The operators are supplied by numerous equipment vendors, most notably Finland's Nokia, to establish 5G infrastructures. The Act provides Traficom with authority to require operators to remove any devices which are deemed to threaten national security from critical parts of its network. However, the Act also states that Traficom must enter into discussion with the operators and equipment vendors prior to making any decisions[120]. Moreover, operators and vendors must be provided with opportunities to remedy any security deficiencies identified[120]. Section 301a of the Act also stipulates that full compensation may be made, under certain circumstances, by the state to the owner of the device identified to pose national security threat if Traficom made the final call to remove such devices from the system as a last resort. The circumstances include 'the device to be removed was put into use before the enforcement of the law' or 'the owner of the device could not have reasonably foreseen the deficiencies'[120]. These legal requirements intend to create a fair environment for bilateral communication between private-sector businesses and public-sector regulators. By opening the doors for operators and vendors to engage in discussion, express opinion and conduct remediation, the Act forms a public-private partnership underlined with transparency, trust and confidence.

Moving on, Section 244a of the Act states that if there are 'strong grounds to suspect that using a device would endanger national security or national defence', Traficom may 'oblige the owner to remove the device from its network'[120]. Finland's focus on the device level is noteworthy. Alkio and Rouvinen, European legal experts, pointed out that the Finnish Act 'operates at the level of a device and does not permit banning vendors outright' [122]. As the security assessment is made on devices, companies are protected from exclusion and market development is accelerated with unhindered competition. Finland recognises the importance of maintaining a confident and competitive private sector market so that the enhancement of security measures does not hinder the development of technology. Finland's target focus on the device level, as argued by scholars, could be derived from Finnish perception towards cybersecurity, where 'it is seen as a technical issue that needs a technical solution'[122].

Under the Finnish 5G cybersecurity framework, the government has incorporated a wide range of voices and opinions from both the governing and complying stakeholders. The AVANCE legal expert team describes the Finnish adoption of MSP and PPP as 'corresponding to what the International Telecommunication Union (ITU) identifies as the most desired stage of ICT regulation: collaborative, exploits synergies across sectors, and pools the expertise of diverse stakeholders'[122]. Furthermore, bilateral discussion allows policy designers and regulators to consider the affordability of both the enforcing and complying stakeholders. Thus, the extent of PIG may also be minimised through continuous adjustment and improvement.

Finally, let's look at the results produced by Finland's 5G cybersecurity initiatives. Today, over 80% of Finland's citizens have access to 5G network. The low network latency and high data transfer capacity enabled by the 5G infrastructure contributed significantly to the country's various societal functions, including healthcare, agriculture and manufacturing[123]. According to a 2021 report from The Groupe Speciale Mobile Association (GSMA), Europe's advancement in mobile networks led to an outstanding productivity increase, which is equivalent to an economic value of EUR 540 bn[124]. Finland, as one of the 5G development leaders in the region, is contributing greatly to value creation through its Electronic Communication Services Act. The Finnish government recognises how developing 5G technology could bring significant value to its economic and social operations. The Electronic Communication Services Act is to ensure the safety and security of the country while reaping the benefits of 5G proliferation. The Act is enabling Finland to take huge leaps in creating sustainable ICT development and attaining the betterment of citizens' livelihood.



# 5. Emerging trends of cybersecurity legislation

# 5.1 Legislation of new technology

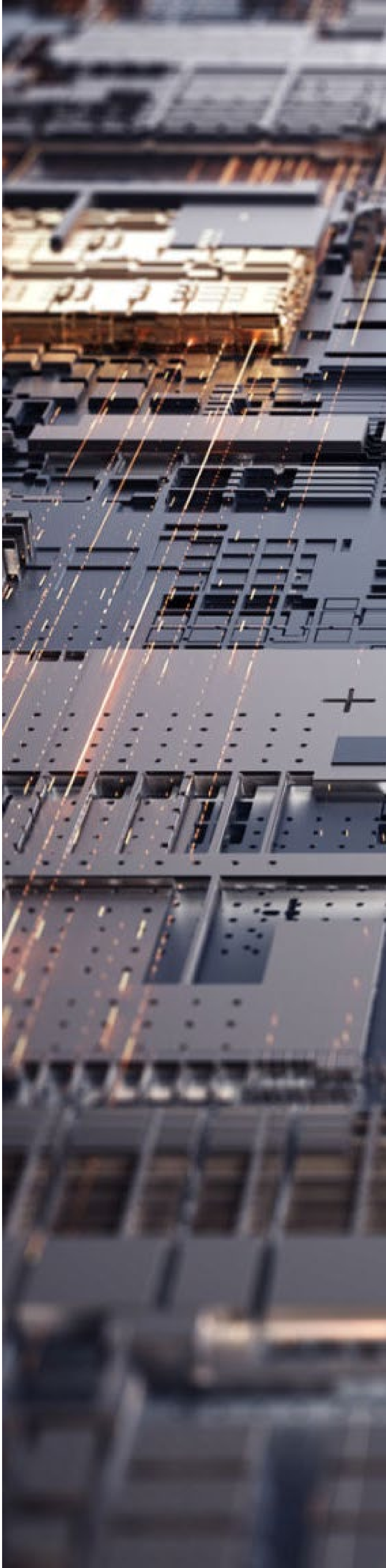
In the past few years, many developed countries have made significant progress in the development of AI and introduced policies in different ways. The EU's AI regulatory framework has built on the original intention and experience of GDPR while actively promoting AI legislation through a unified legislative model based on the principle of protecting individual rights. Similarly, the US actively promotes AI legislation based on promoting industrial development. On a national level, the US Congress enacted the National AI Initiative Act in January 2021, creating the National AI Initiative, which provides 'an overarching framework to strengthen and coordinate AI research, development, demonstration and education activities across all the US Departments and Agencies'[125]. Furthermore, China released the Administrative Provisions on Algorithm Recommendation of Internet Information Services in 2021, emphasising that China is committed to making technological development as important as national security in its AI legislation. Based on the understanding of the current status of legal supervision of AI in China, the US and the EU, it is predicted that the security, privacy and ethical issues of AI applications will be considered in the legislative process in the near future. In other words, a risk-based approach will be leveraged to implement AI legislation.

Blockchain is the next emerging new technology, a decentralised ledger of all transactions across a peer-to-peer network. It is the technology that enables the existence of cryptocurrency, such as Bitcoin. In the US, the Financial Crimes Enforcement Network (FinCEN), the Federal Reserve Board (FRB) and the Commodity Futures Trading Commission (CFTC) have issued their interpretations and guidance on cryptocurrencies[126]. On the other hand, in 2013, the People's Bank of China banned financial institutions from dealing in cryptocurrencies and later expanded the ban to cover crypto exchanges and ICOs. Furthermore, China banned bitcoin mining in May 2021, forcing many engaging in the activity to close operations entirely or relocate to jurisdictions with a more favourable regulatory environment[127]. Based on the current status of legal supervision of AI in China and the US, it can be predicted that legislation on blockchain will continue to encourage the development and implementation of blockchain technology, with an emphasis on cybersecurity risks stemming from the use of cryptocurrencies.

## 5.2 Greater emphasis on cross-border data transfer

The cross-border data flow has become an important area of competition among countries. Looking at the legislation of developed countries in the field of cross-border data transfer, we can see that some countries are also tightening their legislative requirements and guidelines related to cross-border transfer of personal data. The EU has stipulated the requirement of more stringent protection standard for the governance of cross-border data transfer, while supporting the free flow of personal data between member states in the EU through a unified legislative model that protects human rights and strengthens internal data flow. At the same time, conditional cross-border data transfer rules have been established for personal data flowing out of EU member countries to ensure the safe transmission of personal data. On the contrary, the US has established restrictive rules for transmitting personal data through a decentralised (industry-based) legislative model based on the main principle of economic interest. For example, the National Security and Personal Data Protection Act of 2019[128], which has not come into effect yet, explicitly prohibits the transmission and storage of data to specific countries.

Through legislation and promotion trends of cross-border data transfer in the countries and regions above, countries prefer to promote a regional, data-free transfer model while continuously refining the requirements of cross-border data transfer. Therefore, on the issue of cross-border data transfer, countries should consider the relationship between the development of their data economy and national security, which is a key issue they will need to consider for a long time to come.



## 5.3 Cybersecurity insurance

Cybersecurity insurance is a speciality insurance product intended to protect businesses from risk events arising from the use of information technology infrastructure, the internet and related activities. Cybersecurity insurance does not simply protect users from financial damages caused by cyberattacks. Instead, it is also a mechanism to indirectly encourage and motivate organisations to strengthen their cybersecurity by leveraging insurance premiums. Currently, China, the US and the EU have legislation on cybersecurity insurance.

As mentioned in the earlier sections, cybersecurity insurance is one of the areas of attention many countries carry in the realm of cybersecurity legislation. Diverse forms of insurance products are being created in the market.

## 5.4 ICT supply chain

More and more countries are increasingly paying attention to supply chain security due to the increasing number of related issues reported in the past few years. The SolarWinds cyberattack[129] is one of the most significant supply chain attacks reported in recent years. Even though SolarWinds was recognised as one of the trusted IT management solution suppliers, a catastrophic cyberattack still occurred. As a result, countries are beginning to reconsider the current status of supply chain security and the required legislation to mitigate supply chain security risks. The US, China and the EU have legislation on supply chain management. The US has the US Executive Order on Securing the Information and Communications Technology and Services Supply Chain[130] and the Federal Acquisition Supply Chain Security Act[131]. As for China, the government has published the Measures for Cloud Computing Service Security Assessment[132] and Measures for Cybersecurity Review[133]. In the EU, the NIS 2[14] and ENISA-published Threat Landscape for Supply Chain Attacks (2021)[134] are in place.

The core components of ICT supply chain cybersecurity are (1) vendor risk management and (2) security of underlying products and services. Supply chain security is a complex issue that not only includes suppliers' security review and product or service certification requirements but also addresses the security of the underlying products and services themselves. ICT supply chain legislation shall involve these two core components. Only focusing on either one of these two is deemed insufficient, and it will lead to a false sense of security. Last but not least, a number of principles should be considered in supply chain management, including evaluation and competition, resilience and stability of the supply chain and trustworthy assessment of products and technologies.

## 5.5 Legislation for non-personal data protection

Data is commonly recognised as the fuel for the digital economy - it is estimated that open data can contribute over 3 trillion USD to the global economy annually[135]. As such, governments have emphasised the sharing of NPD to serve the development of the digital economy. However, regulating the use of NPD is still in its early development phase at a global level, and consensus for this is yet to be achieved.

However, based on the experience of regulating personal data use, many concerns have been expressed about promoting the sharing of NPD. First, building a robust infrastructure for data transmission is a prerequisite to ensure the secure and reliable sharing of NPD[136]. Constructing a resilient, secure and highly-accessible infrastructure to support the sharing of large amounts of data concurrently is one of the challenges that need to be addressed. Second, determining the ownership and pricing of NPD data is another challenge. Unlike the ownership of personal data, which can be linked back to the data subjects, the ownership of non-personal data is difficult to be determined. Furthermore, the value of NPD is highly subjective to the user. When it comes to data assertion, standardising the pricing model to determine the monetary value of NPD would be another struggle for governments.

# Acknowledgements

The contributors of this discussion paper wish to thank our partners, Mr Kenneth Wong, Ms Lisa Li and Mr Danny Weng, who gave us a chance to work on this project. We are very grateful and appreciative of their valuable suggestions that improved the project outcome.

We are also grateful for the contributions of our team members: Mr Duncan Ding, Ms Sara Qu, Ms Vivian Tong, Ms Frances Lin, Ms Levana Qi and Mr Tory Kim.

The project has been hard work, but we couldn't have done it without the support and guidance of experts and professionals. We want to thank Ms Xi Gelian and Dr Annie Xue from Gen Law Firm in Beijing; Associate Professor Ding Hao, Associate Professor Chen Xing, and Associate Professor Shang Xuejiao from the Guangdong University of Foreign Studies in Guangzhou; Dr. William J. Drake from the Columbia Institute for Tele-Information at Columbia Business School in New York for their help with this project. They provided us with professional insights and expert opinions essential to producing this paper.

Last but not least, we would like to send our warmest appreciation to all those who contributed to writing this paper in any form, either direct or indirect.

# Endnotes

1 Decreto nº 9.573, de 22 de Novembro de 2018 <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm> [Accessed 27 March 2023].

2 Decreto nº 11.200 de 15 de Setembro de 2022 <https://www.in.gov.br/en/web/dou/-/decreto-n-11.200-de-15-de-setembro-de-2022-430035293> [Accessed 27 March 2023].

3 Chile Cybersecurity 2023 <https://practiceguides.chambers.com/practice-guides/cybersecurity-2023/chile> [Accessed 27 March 2023].

4 Regulations on the Security Protection of Critical Information Infrastructure <http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm> [Accessed 27 March 2023].

5 Act on the Federal Office for Information Security (BSI Act - BSIG) <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile > [Accessed 27 March 2023].

6 The Information Technology Act <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=> [Accessed 27 March 2023].

7 Singapore Cybersecurity Act 2018 <https://sso.agc.gov.sg//Act/CA2018> [Accessed 27 March 2023].

8 Critical Infrastructure Protection Act <https://static.pmg.org.za/220422interim-critical-infrastructure-protection-regulations.pdf> [Accessed 27 March 2023].

9 UAE Information Assurance Regulation <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/uae-information-assurance-regulation> [Accessed 21 February 2023].

10 The Network and Information Systems Regulations 2018 <https://www.legislation.gov.uk/uksi/2018/506/made> [Accessed 27 March 2023].

11 Cybersecurity and Infrastructure Security Agency Act of 2018 <https://www.govinfo.gov/content/pkg/COMPS-15296/pdf/COMPS-15296.pdf> [Accessed 27 March 2023].

12 Vietnam Law on Cybersecurity <https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf> [Accessed 27 March 2023].

13 CER Directives <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557&from=EN> [Accessed 27 March 2023].

14 NIS 2 Directives <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1679369866848&from=en> [Accessed 27 March 2023].

15 N. Hanacek, NIST < https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework > [Accessed 27 March 2023].

16 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> [Accessed 21 February 2023].

17 No. 20(3)/2022-CERT-In <https://regmedia.co.uk/2022/06/28/supplied_cert_india_extension.pdf> [Accessed 28 March 2023].

18 National Cyber Security Incident Plan of China <http://www.cac.gov.cn/2017-06/27/c_1121220113.htm> [Accessed 28 March 2023].

19 H.R.2471 - Consolidated Appropriations Act, 2022 <https://www.congress.gov/bill/117th-congress/house-bill/2471/text> [Accessed 27 March 2023].

20 Guiding Opinions on Promoting the Development of the Cybersecurity Industry (Draft for Comments) <http://www.cac.gov.cn/2019-09/27/c_1571114011459248.htm> [Accessed 22 February 2023].

21 Measures for the Administration of Cybersecurity Threat Information Release (Draft for Comments) <http://www.npc.gov.cn/npc/c30834/201911/507f3d238d3a49c4846168dd8b07a96e.shtml > [Accessed 22 February 2023].

22 How to recognize & prevent cybercrime <https://www.cisa.gov/sites/default/files/publications/Week3TipCard-%20508%20compliant_0.pdf> [Accessed 22 February 2023].

23 Europol's cybercrime-prevention guides <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides> [Accessed 22 February 2023].

24 Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading <https://apps.sfc.hk/edistributionWeb/api/consultation/openFile?lang=EN&refNo=17CP4> [Accessed 22 February 2023].

25 Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading <https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading> [Accessed 22 February 2023].

26 Cybercrimes Act of 2020 <https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf> [Accessed 23 February 2023].

27 Federal Decree Law Number 5/2012 <https://tdra.gov.ae/-/media/About/Legal-References/LAW/LAW-English/Federal-DecreeLaw-no-5-of-2012-on-combating-Cybercrimes.ashx> [Accessed 23 February 2023].

28 Computer Misuse Act 1990 <https://www.legislation.gov.uk/ukpga/1990/18/contents> [Accessed 23 February 2023].

29 The Data Protection Act 2018 <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> [Accessed 23 February 2023].

30 The Fraud Act 2006 <https://www.legislation.gov.uk/ukpga/2006/35/contents> [Accessed 23 February 2023].

31 Electronic Communications Protection Act <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285> [Accessed 23 February 2023].

32 N.Y. Penal Law <https://ypdcrime.com/penal.law/> [Accessed 23 February 2023].

33 2013/40/EU Cybercrime Directive <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040> [Accessed 22 February 2023].

34 German Criminal Code <https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html> [Accessed 23 February 2023].

35 the Information Technology Act, 2000 <https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf> [Accessed 23 February 2023].

# Endnotes

36 The Indian Penal Code, 1860 <https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362> [Accessed 23 February 2023].

37 UNCTAD, Data Protection and Privacy Legislation Worldwide <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> [Accessed 28 February 2023].

38 General Data Protection Regulation <https://gdpr-info.eu/https://gdpr-info.eu/> [Accessed 28 February 2023].

39 Personal Information Protection Law (PIPL) <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml?xxgkhide=1> [Accessed 28 February 2023].

40 ENISA, Supporting the implementation of Union policy and law regarding cybersecurity <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new> [Accessed 28 February 2023].

41 One Trust, Understanding the 7 Principles of the GDPR <https://www.onetrust.com/blog/gdpr-principles> [Accessed 28 February 2023].

42 ICO, Lawful basis for processing <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> [Accessed 28 February 2023].

43 Thomson Reuters, Appropriate safeguards <https://uk.practicallaw.thomsonreuters.com/w-014-8166?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true> [Accessed 28 February 2023].

44 Data Governance Act <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0868&from=EN> [Accessed 27 March 2023].

45 Free Flow of Non-personal Data <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1807&from=EN> [Accessed 27 March 2023].

46 Open Data Specifications Guidelines for UAE Government Entities <https://u.ae/-/media/Documents-2023/Open-Data-Specifications-Guidelines-for-UAE-Government-Entities--2022-Eng.ashx > [Accessed 27 March 2023].

47 UAE Smart Data Framework <https://bayanat.ae/-/media/UAE-Smart-Data-Framework-EN---Part-2-Implementation-Guide.ashx> [Accessed 27 March 2023].

48 Data Security Law <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml> [Accessed 27 March 2023].

49 Cybersecurity Law <http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm> [Accessed 28 March 2023].

50 Cyber Product Security Vulnerabilities Management Regulations <http://www.gov.cn/zhengce/zhengceku/2021-07/14/content_5624965.htm> [Accessed 21 February 2023].

51 NCSC Vulnerability Management Guidance <https://www.ncsc.gov.uk/guidance/vulnerability-management> [Accessed 21 February 2023].

52 NCSC Vulnerability Reporting Guidance <https://www.ncsc.gov.uk/information/vulnerability-reporting> [Accessed 21 February 2023].

53 CISA Coordinated Vulnerability Disclosure (CVD) Process <https://www.cisa.gov/coordinated-vulnerability-disclosure-process> [Accessed 21 February 2023].

54 NIAC Vulnerability Disclosure Framework (2004) <https://www.cisa.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf> [Accessed 21 February 2023].

55 Coordinated Vulnerability Disclosure Policies (CVD Policies) <https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu> [Accessed 21 February 2023].

56 EU The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 (2022) <https://www.digital-operational-resilience-act.com/> [Accessed 23 February 2023].

57 Gramm-Leach-Bliley Act <https://www.congress.gov/bill/106th-congress/senate-bill/900> [Accessed 23 February 2023].

58 National Cyber Security Strategy 2020 <https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20submission.pdf> [Accessed 26 March 2023].

59 DSCI Promoting Data Protection <https://www.dsci.in/content/CSAM/2022> [Accessed 26 March 2023].

60 Cyber Security Act <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN> [Accessed 17 March 2023].

61 Factsheet: U.S.-United Kingdom Cybersecurity Cooperation <https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation > [Accessed 16 January 2015].

62 Statement on the UK-Australia Cyber and Critical Technology Partnership <https://www.internationalcybertech.gov.au/node/156> [Accessed 20 January 2023].

63 Announcement on signing MoU for developing capacity building of internet security and tech cooperation between China and Indonesia <http://www.cac.gov.cn/2021-01/15/c_1612286687720936.htm> [Accessed by 15 January 2021].

64 Announcement on signing MoU for cybersecurity between China and Thailand <http://www.cac.gov.cn/2022-07/05/c_1658638472372340.htm> [Accessed 5 July 2022].

65 Cybersecurity Education & Career Development <https://www.cisa.gov/cybersecurity-education-career-development> [Accessed 21 February 2023].

66 NORMAN LOAYZA & MICHAEL WOOLCOCK, Designing good policies is one thing, implementing them is another (2020) <https://blogs.worldbank.org/developmenttalk/designing-good-policies-one-thing-implementing-them-another> [Accessed 23 February 2023].

67 Bob Hudson, David J Hunter & Stephen Peckham, Policy failure and the policy-implementation gap: can policy support programs help? (2019) <https://www.researchgate.net/publication/331369599_Policy_failure_and_the_policy-implementation_gap_can_policy_support_programs_help> [Accessed 23 February 2023].

68 Tim Schwarz & David Satola, Telecommunications Legislation in Transitional and Developing Economies (2000) <https://elibrary.worldbank.org/doi/pdf/10.1596/0-8213-4823-X> [Accessed 23 February 2023].

# Endnotes

[69] BSA, Asia-Pacific Cybersecurity Dashboard A Path to a Secure Global Cyberspace (2015) <https://www.bsa.org/reports/apac-cybersecurity-dashboard> [Accessed 23 February 2023].

[70] Jean-Jacques Laffont & Jean Tirole, Competition in Telecommunications (2001) <https://mitpress.mit.edu/9780262621502/competition-in-telecommunications/> [Accessed 23 February 2023].

[71] IBM, X-Force Threat Intelligence Index 2022 (2022) <https://www.ibm.com/downloads/cas/ADLMYLAZ> [Accessed 23 February 2023].

[72] Eugenia Lostri, James Andrew Lewis, & Georgia Wood, A Shared Responsibility Public-Private Cooperation for Cybersecurity (2022) <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220322_Lostri_Public_Priatev_Cooperation.pdf?aoeH8eOs0uhaBPp8HPVgi.qkEXFmj2yX> [Accessed 23 February 2023].

[73] GSMA, 5G Cybersecurity Knowledge Base <https://www.gsma.com/security/5g-cybersecurity-knowledge-base/> [Accessed 23 February 2023].

[74] United Nations Office on Drugs and Crime, The role of cybercrime law <https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html> [Accessed 23 February 2023].

[75] European Cybercrime Centre (EC3), Internet Organized Crime Threat Assessment (2019) <https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf> [Accessed 23 February 2023].

[76] United Nations Office on Drugs and Crime (UNODC), Obstacles to Cybercrime Investigations <https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html> [Accessed 23 February 2023].

[77] Europol & Eurojust, Common challenges in combating cybercrime (2019) <https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf> [Accessed 23 February 2023].

[78] Bojan Jovanovic, Two-Factor Authentication Statistics: A Good Password is Not Enough (2023) <https://dataprot.net/statistics/two-factor-authentication-statistics/> [Accessed 23 February 2023].

[79] Zain Malik, 8 Benefits of Multi-Factor Authentication (MFA) (2021) <https://www.pingidentity.com/en/resources/blog/post/eight-benefits-mfa.html> [Accessed 23 February 2023].

[80] Jeffrey Julig, Why Multi-Factor Authentication (MFA) is a Business Imperative (2021) <https://blog.swbc.com/businesshub/why-multi-factor-authentication-mfa-is-a-business-imperative> [Accessed 23 February 2023].

[81] Amy Mersch, What is Layered Security & How Does it Defend Your Network? (2021) <https://blog.totalprosource.com/what-is-layered-security-how-does-it-defend-your-network> [Accessed 23 February 2023].

[82] Apotheon, Understanding layered security and defense in depth (2008) <https://www.techrepublic.com/article/understanding-layered-security-and-defense-in-depth/> [Accessed 23 February 2023].

[83] Axiad, Zero Trust vs. Defense-In-Depth: What's the Difference? (2022) <https://www.axiad.com/blog/zero-trust-vs-defense-in-depth-whats-the-difference/> [Accessed 23 February 2023].

[84] Cyber Security Agency of Singapore, Cybersecurity Code of Practice for Critical Information Infrastructure – Second Edition Revision One (2022) <https://www.csa.gov.sg/docs/default-source/legislation/ccop---second-edition_revision-one.pdf?sfvrsn=421a71ab_1> [Accessed 23 February 2023].

[85] The Partnering Initiative, An introduction to multi-stakeholder partnerships (2016) <https://www.thepartneringinitiative.org/wp-content/uploads/2017/03/Introduction-to-MSPs-Briefing-paper.pdf> [Accessed 24 February 2023].

[86] Global Partners Digital, Multistakeholder Approaches to National Cybersecurity Strategy Development (2018) <https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf> [Accessed 24 February 2023].

[87] Partnerships 2030, What is an MSP? <https://www.partnerschaften2030.de/en/what-is-a-msp/> [Accessed 24 February 2023].

[88] Md Nurul Momen, Multi-stakeholder Partnerships in Public Policy (2019) <https://www.researchgate.net/publication/337685913_Multi-stakeholder_Partnerships_in_Public_Policy> [Accessed 24 February 2023].

[89] Global Conference on Cyberspace, Chair's Statement (2015) <https://www.mofa.go.jp/mofaj/files/000076862.pdf> [Accessed 24 February 2023].

[90] UN. Secretary-General and UN. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General (2015) <https://digitallibrary.un.org/record/799853> [Accessed 24 February 2023].

[91] GLOBAL PARTNERS DIGITAL, Multistakeholder Approaches to National Cybersecurity Strategy Development (2018) <https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf> [Accessed 24 February 2023].

[92] Nabila Rahal, UAE's Cybersecurity Council and Huawei ink MoU to strengthen local cybersecurity strategies (2022) <https://www.arabianbusiness.com/industries/technology/uaes-cybersecurity-council-and-huawei-ink-mou-to-strengthen-local-cybersecurity-strategies> [Accessed 24 February 2023].

[93] Saul Mauricio Rodriguez-Hernandez & Nicolas Velasquez, Mexico and cybersecurity: policies, challenges, and concerns <https://ebrary.net/173531/political_science/mexico_cybersecurity_policies_challenges_concerns> [Accessed 24 February 2023].

[94] Cristos Velasco, Cyber Law in Mexico, Fourth edition (2019) <https://law-store.wolterskluwer.com/s/product/cyber-law-in-mexico-4e/01t0f00000NY5cAAAT> [Accessed 24 February 2023].

[95] GLOBAL PARTNERS DIGITAL, Multistakeholder Approaches to National Cybersecurity Strategy Development (2018) <https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf> [Accessed 24 February 2023].

[96] Details about Indian Cybercrime Coordination Centre (I4C) Scheme (2022) <https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme> [Accessed 24 February 2023].

# Endnotes

97 Balsing Rajput, Cyber Economic Crime in India: An Integrated Model for Prevention and Investigation (2020) <https://books.google.com.hk/books?id=CJreDwAAQBAJ&pg=PA173&lpg=PA173&dq=INDIAN+National+Cybercrime+Threat+Analytics+Unit+(TAU)+multistakeholder&source=bl&ots=Oyof3P4eUN&sig=ACfU3U2BJs2K6Rx6Cc2dMK3yBPC_vyyfhw&hl=zh-TW&sa=X&ved=2ahUKEwjf1YqAhvb8AhV-r1YBHQxH> [Accessed 24 February 2023].

98 I4C: Indian Cyber Crime Coordination Centre (2022) <https://simplifiedupsc.in/i4c-indian-cyber-crime-coordination-centre/> [Accessed 24 February 2023].

99 Bnamericas, Microsoft allies with Chile government to fight cybercrime (2017) <https://www.bnamericas.com/en/news/microsoft-allies-with-chile-government-to-fight-cybercrime> [Accessed 24 February 2023].

100 Kerala Police Cyberdome <https://cyberdome.kerala.gov.in/> [Accessed 24 February 2023].

101 Singtel, Singtel launches first-of-its-kind cyber security institute in Asia Pacific to hone cyber skills and preparedness (2016) <https://www.singtel.com/about-us/media-centre/news-releases/singtel-launches-first-of-its-kind-cyber-security-institute-in-asia-pacific-t> [Accessed 24 February 2023].

102 Mbangiseni David Mahlobo, The National Cybersecurity Policy Framework (NCPF) (2015) <https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf> [Accessed 24 February 2023].

103 Scott Birch, UAE creating cybersecurity fortress for a safer world (2022) <https://cybermagazine.com/cyber-security/uae-creating-cybersecurity-fortress-for-a-safer-world> [Accessed 24 February 2023].

104 Nabila Rahal, UAE's Cybersecurity Council and Huawei ink MoU to strengthen local cybersecurity strategies (2022) <https://www.arabianbusiness.com/industries/technology/uaes-cybersecurity-council-and-huawei-ink-mou-to-strengthen-local-cybersecurity-strategies> [Accessed 24 February 2023].

105 Cybersecurity — Executive Order 13636 (2013) <https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636> [Accessed 24 February 2023].

106 Cyber Information Sharing and Collaboration Program <https://www.cisa.gov/ciscp> [Accessed 24 February 2023].

107 EP3R 2009-2013 Future of NIS Public Private Cooperation (2015) <https://www.enisa.europa.eu/publications/ep3r-2009-2013> [Accessed 24 February 2023].

108 Public Private Partnerships (PPP) - Cooperative models (2018) <https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models> [Accessed 24 February 2023].

109 Vitalii Kruhlov, Mykola Latynin, Alina Horban and Anton Petrov, Public-Private Partnership in Cybersecurity (2020) <https://ceur-ws.org/Vol-2654/paper48.pdf> [Accessed 24 February 2023].

110 Gini Services Tunisie Design Build Finance Operate <http://www.giniengineering.com/index.php?option=com_content&view=article&id=150&Itemid=191> [Accessed 24 February 2023].

111 National University of Singapore, Policy Analysis: Singapore's Public-Private Partnerships for Cybersecurity in the Critical Infrastructure Sectors — Challenges and Opportunities <https://lkyspp.nus.edu.sg/docs/default-source/case-studies/entry-1594-cybersecurity_weichieh_v3_tt.pdf?sfvrsn=e1e7970b_2> [Accessed 24 February 2023].

112 Infocomm Media Development Authority, Real-Time Response to Cyber-Threats by Government (2006) <https://www.imda.gov.sg/content-and-news/press-releases-and-speeches/archived/ida/press-releases/2006/20050906111323> [Accessed 24 February 2023].

113 Smart Nation Singapore, Factsheet - Government Cyber Security Operations Centre (GCSOC) (2023) <https://www.smartnation.gov.sg/media-hub/press-releases/gcsoc-factsheet/> [Accessed 24 February 2023].

114 Will Kenton, Memorandum of Understanding (MOU) Defined, What's In It, Pros/Cons, MOU vs MOA (2023) <https://www.investopedia.com/terms/m/mou.asp> [Accessed 24 February 2023].

115 OECD, Cybersecurity Policy Making at a Turning Point (2012) <https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf> [Accessed 24 February 2023].

116 European Union, The EU toolbox for 5G security (2021) <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security> [Accessed 24 February 2023].

117 Samuel Stolton, EU nations divided on 5G security, auditors say (2021) <https://www.euractiv.com/section/5g/news/eu-nations-divided-on-5g-security-auditors-say/> [Accessed 24 February 2023].

118 Morgan Lewis, The Approach of the EU and Selected Member States to 5G Network Cybersecurity (2021) <https://www.morganlewis.com/-/media/files/publication/morgan-lewis-title/white-paper/2020/morgan-lewis-white-paper_theapproachoftheeuandselectedmemberstatestocybersecurityof5gnetworks.pdf> [Accessed 24 February 2023].

119 International Trade Administration, Information and Communication Technologies (2022) <https://www.trade.gov/country-commercial-guides/finland-information-and-communication-technologies> [Accessed 24 February 2023].

120 Act on Electronic Communications Services (2020) <https://www.finlex.fi/en/laki/kaannokset/2014/20140917> [Accessed 24 February 2023].

121 Francesco Rizzato, Finland 5G Experience Report (2021) <https://www.opensignal.com/reports/2021/12/finland/mobile-network-experience-5g> [Accessed 24 February 2023].

122 Mikko Alkio & Petri Rouvinen, Implementing the 5G toolbox: Could Finland serve as a model for the other EU countries? (2021) <https://www.avance.com/wp-content/uploads/2021/05/AVANCE-Insight-01-2021.pdf> [Accessed 24 February 2023].

123 Sari Laine-Lassila, Finland is at the forefront of 5G technology (2021) <https://ficom.fi/news/finland-is-at-the-forefront-of-5g-technology/> [Accessed 24 February 2023].

124 GSMA, The Mobile Economy Europe 2022 (2022) <https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/10/051022-Mobile-Economy-Europe-2022.pdf> [Accessed 24 February 2023].

125 Dr. Lynne Parker, National Artificial Intelligence Initiative (2022) < https://www.uspto.gov/sites/default/files/documents/National-Artificial-Intelligence-Initiative-Overview.pdf> [Accessed 28 February 2023].

# Endnotes

126 Thomson Reuters Institute. 2022, Cryptocurrency regulations by country <https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf> [Accessed 2 January 2023].

127 Kelvin George, Cryptocurrency Regulations Around the World (2022) <https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122> [Accessed 2 January 2023].

128 Congress. GOV, S.2889 - National Security and Personal Data Protection Act of 2019 <https://www.congress.gov/bill/116th-congress/senate-bill/2889> [Accessed 28 February 2023].

129 The White House, Statement by Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger on SolarWinds and Microsoft Exchange Incidents <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/19/statement-by-deputy-national-security-advisor-for-cyber-and-emerging-technology-on-solarwinds-and-microsoft-exchange-incidents/> [Accessed 22 March 2023].

130 The White House, US Executive Order on Securing the Information and Communications Technology and Services Supply Chain <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/> [Accessed 23 February 2023].

131 Federal Acquisition Supply Chain Security Act <https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act > [Accessed 23 February 2023].

132 Measures for Cloud Computing Service Security Assessment <http://www.gov.cn/xinwen/2019-07/22/content_5412625.htm> [Accessed 21 February 2023].

133 Measures for Cybersecurity Review <http://www.gov.cn/zhengce/2022-11/26/content_5728942.htm> [Accessed 21 February 2023].

134 ENISA, Threat Landscape for Supply Chain Attacks (2021) <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks> [Accessed 23 February 2023].

135 How Government Can Promote Open Data and Help Unleash over $3 Trillion in Economic Value <https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/how%20government%20can%20promote%20open%20data/how_govt_can_promote_open_data_and_help_unleash_over_$3_trillion_in_economic_value.pdf> [Accessed 28 February 2023].

136 Kapoor, A., Nanda, A. Non-personal data sharing: Potential, pathways and problems. CSIT 9, 165-169 (2021). <https://doi.org/10.1007/s40012-021-00336-5> [Accessed 16 January 2023].

# Contact us

## China South

### Kenneth Wong

Mainland China and Hong Kong Digital Trust & Risk - Cybersecurity and Privacy Leader
PwC Hong Kong
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

### Danny Weng

Mainland China Digital Trust & Risk - Cybersecurity and Privacy Partner
PwC China
+86 (20) 3819 2629
danny.weng@cn.pwc.com

## China Central

### Chun Yin Cheung

Mainland China Digital Trust & Risk - Cybersecurity and Privacy Leader
PwC China
+86 (21) 2323 3927
chun.yin.cheung@cn.pwc.com

## China North

### Lisa Li

Mainland China Digital Trust & Risk - Cybersecurity and Privacy Leader
PwC China
+86 (10) 6533 2312
lisa.ra.li@cn.pwc.com

The information contained in this publication is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of legal, tax or other professional advice or service by PricewaterhouseCoopers Mainland China and Hong Kong ("PwC"). PwC has no obligation to update the information as law and practices change. The application and impact of laws can vary widely based on the specific facts involved. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual PwC client service team or your other advisers.

The materials contained in this publication were assembled in April 2023 and were based on the law enforceable and information available at that time.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.