Access Partnership

Cybersecurity Policy Developments in APEC

Lim May-Ann

Director of Data Governance
Access Partnership

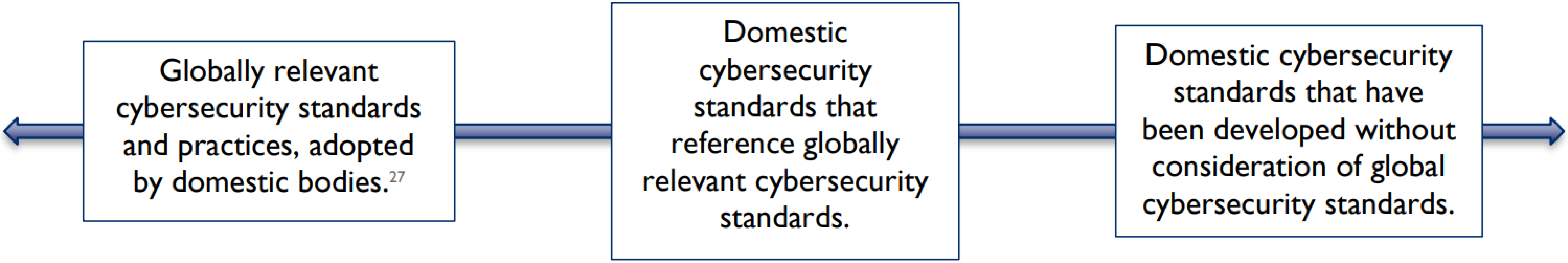
mayann.lim@accesspartnership.com

25 Jul 2024

What have we learned so far about cybersecurity policy, particularly in recent years?

- **Cybersecurity landscape has demanded different approaches.** And therefore different economies have developed different approaches towards managing cybersecurity. **State-level approaches vs universal approach.** Within individual economies, there may be a difference between state-level and whole-country approaches as well, adding another layer of complexity to alignment with other economies for interoperability
- **Best practice is globally-relevant standards.** The use of globally-relevant standards developed through open, transparent and consensus-based processes and good cybersecurity practices to better harmonize economies' cybersecurity approaches and foster interoperability.
- Best approach is one which is **flexible, nimble and responsive.**
- Any **robust cybersecurity approach** addresses five critical functions: Identification, Protection, Detection, Response, and Recovery.

Variety of Cybersec Standard Approaches in APEC economies



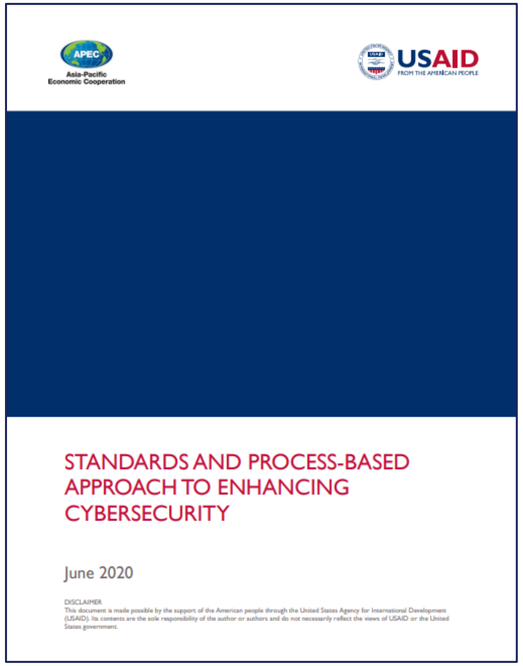
Globally relevant cybersecurity standards and practices, adopted by domestic bodies.[27]

Domestic cybersecurity standards that reference globally relevant cybersecurity standards.

Domestic cybersecurity standards that have been developed without consideration of global cybersecurity standards.

Cybersecurity Trends Observed

- Imposition of Data Localization Requirements
- Creation of domestic cybersecurity standards
- Banning of foreign content and providers/vendors
- Fragmented privacy rules and lack of harm-based data breach requirements



Asia-Pacific
Economic Cooperation

USAID
FROM THE AMERICAN PEOPLE

STANDARDS AND PROCESS-BASED APPROACH TO ENHANCING CYBERSECURITY

June 2020

DISCLAIMER
This document is made possible by the support of the American people through the United States Agency for International Development (USAID). Its contents are the sole responsibility of the author or authors and do not necessarily reflect the views of USAID or the United States government.

Update 2024

- Some markets are refreshing cybersecurity laws, new threats/ war
- Some markets have faced high-profile cybersecurity breaches
- Some markets are updating data protection requirements, and/or adding "bolt-on" regulations to strengthen new aspects of cybersecurity/cybercrime online e.g. online safety laws
- Inclusion of Artificial Intelligence as a new attack vector/accelerator

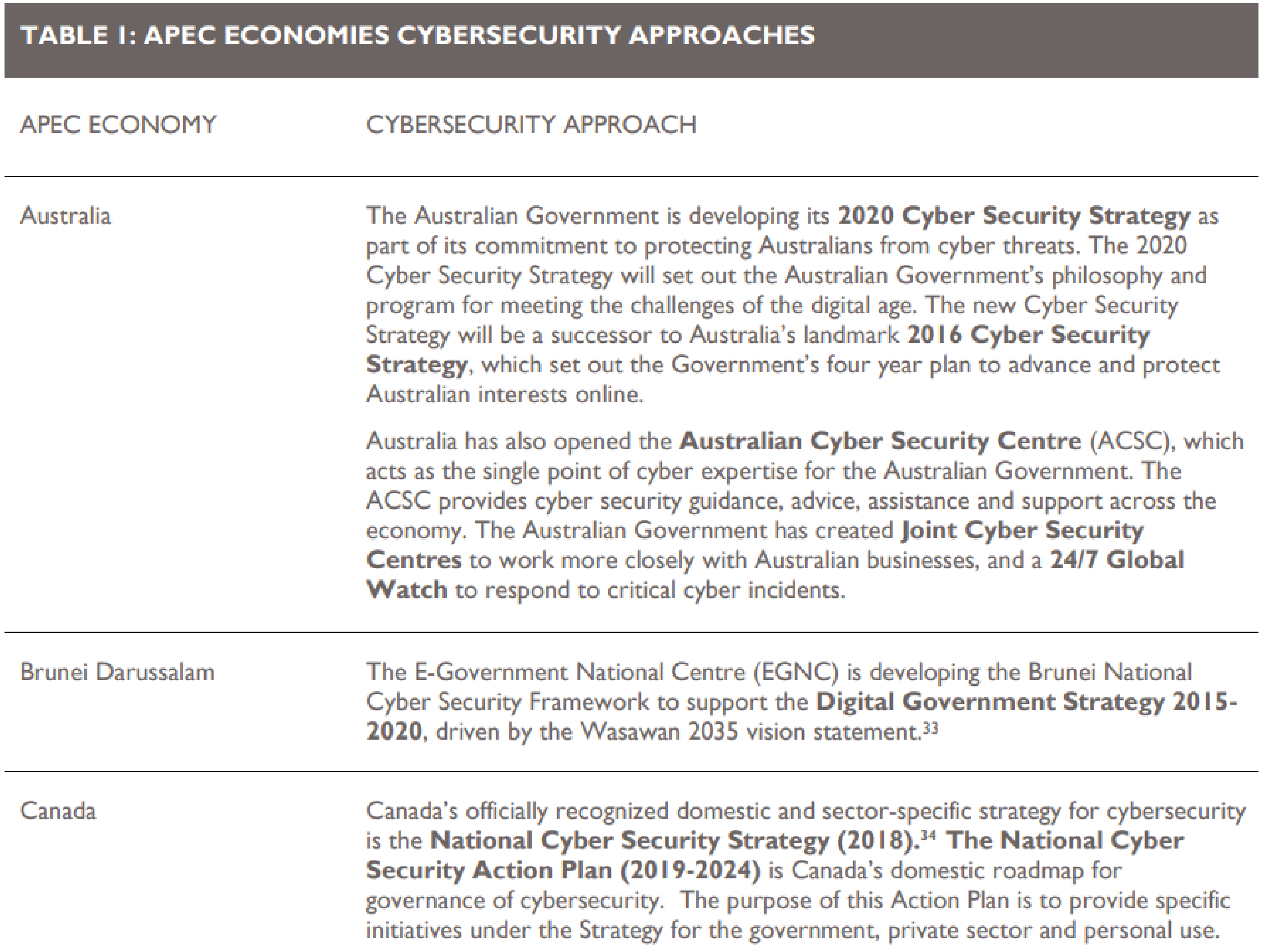


TABLE 1: APEC ECONOMIES CYBERSECURITY APPROACHES

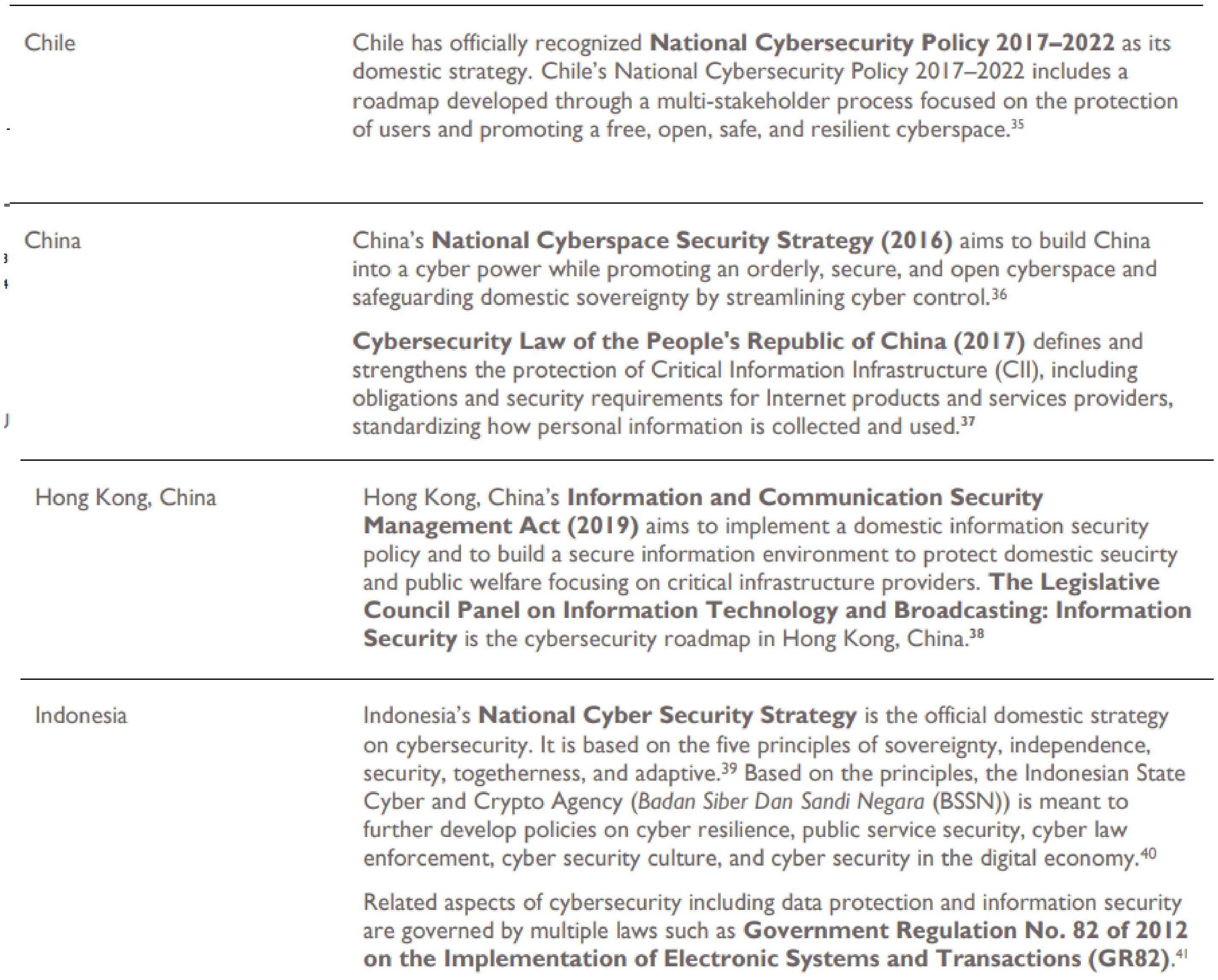
APEC ECONOMY	CYBERSECURITY APPROACH
Australia	The Australian Government is developing its **2020 Cyber Security Strategy** as part of its commitment to protecting Australians from cyber threats. The 2020 Cyber Security Strategy will set out the Australian Government's philosophy and program for meeting the challenges of the digital age. The new Cyber Security Strategy will be a successor to Australia's landmark **2016 Cyber Security Strategy**, which set out the Government's four year plan to advance and protect Australian interests online. Australia has also opened the **Australian Cyber Security Centre** (ACSC), which acts as the single point of cyber expertise for the Australian Government. The ACSC provides cyber security guidance, advice, assistance and support across the economy. The Australian Government has created **Joint Cyber Security Centres** to work more closely with Australian businesses, and a **24/7 Global Watch** to respond to critical cyber incidents.
Brunei Darussalam	The E-Government National Centre (EGNC) is developing the Brunei National Cyber Security Framework to support the **Digital Government Strategy 2015-2020**, driven by the Wasawan 2035 vision statement.[33]
Canada	Canada's officially recognized domestic and sector-specific strategy for cybersecurity is the **National Cyber Security Strategy (2018).**[34] **The National Cyber Security Action Plan (2019-2024)** is Canada's domestic roadmap for governance of cybersecurity. The purpose of this Action Plan is to provide specific initiatives under the Strategy for the government, private sector and personal use.

Online Safety Act 2021 https://www.legislation.gov.au/C2021A00076/latest/text

Two new industry standards under the Online Safety Act 2021 (Cth) (OSA) https://www.globalcompliancenews.com/2023/12/12/https-insightplus-bakermckenzie-com-bm-data-technology-australia-significant-new-developments-in-online-safety-regime_11272023/

Proposed (Critical Infrastructure) Bill 2020 https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Jun 2024 Critical Cyber Systems Protection Act (CCSPA) may be enacted https://www.blakes.com/insights/canadian-cybersecurity-law-update-bill-c-26-gains-momentum-in-the-house-of-commons/

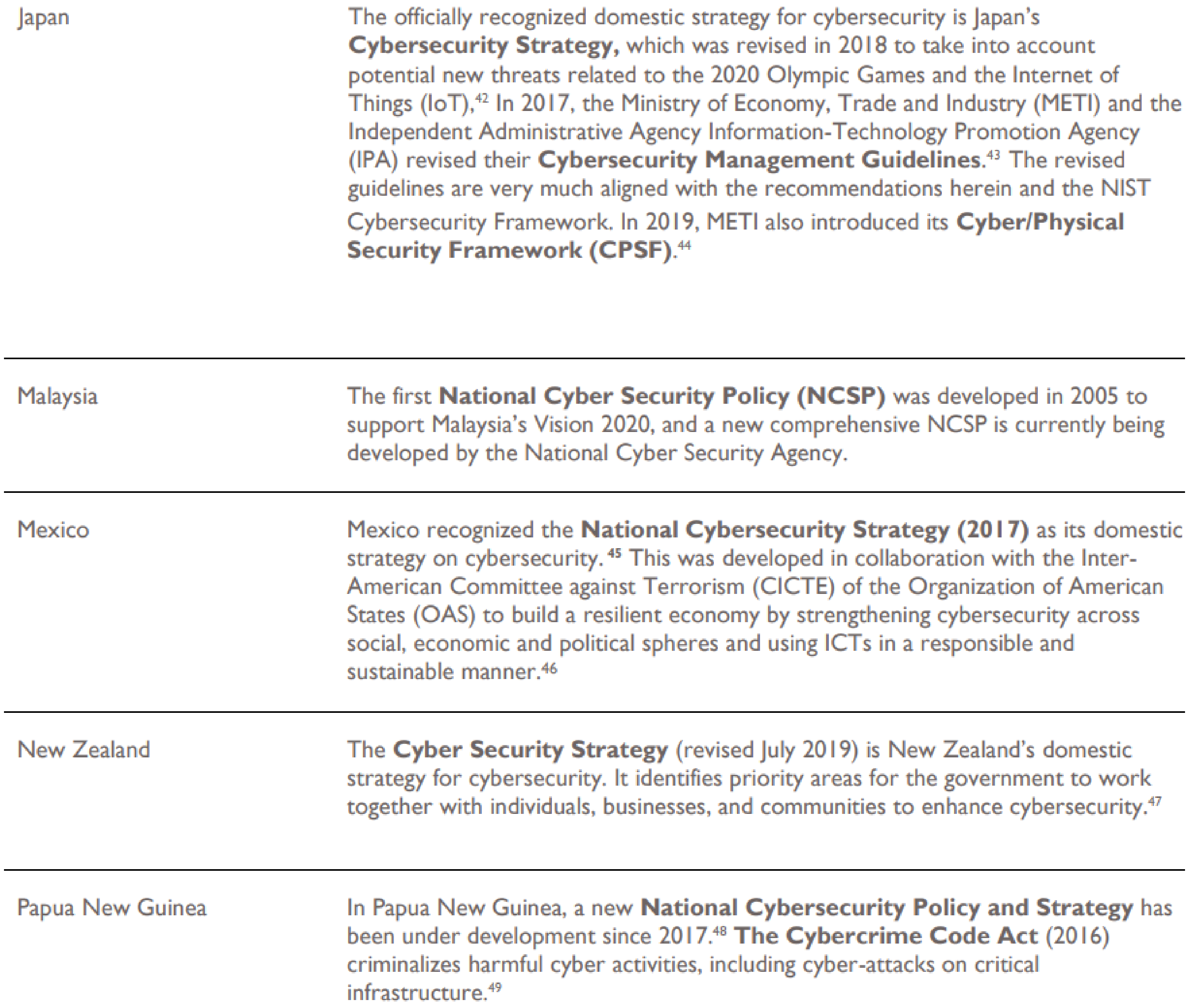


Chile	Chile has officially recognized **National Cybersecurity Policy 2017–2022** as its domestic strategy. Chile's National Cybersecurity Policy 2017–2022 includes a roadmap developed through a multi-stakeholder process focused on the protection of users and promoting a free, open, safe, and resilient cyberspace.[35]
China	China's **National Cyberspace Security Strategy (2016)** aims to build China into a cyber power while promoting an orderly, secure, and open cyberspace and safeguarding domestic sovereignty by streamlining cyber control.[36] **Cybersecurity Law of the People's Republic of China (2017)** defines and strengthens the protection of Critical Information Infrastructure (CII), including obligations and security requirements for Internet products and services providers, standardizing how personal information is collected and used.[37]
Hong Kong, China	Hong Kong, China's **Information and Communication Security Management Act (2019)** aims to implement a domestic information security policy and to build a secure information environment to protect domestic seucirty and public welfare focusing on critical infrastructure providers. **The Legislative Council Panel on Information Technology and Broadcasting: Information Security** is the cybersecurity roadmap in Hong Kong, China.[38]
Indonesia	Indonesia's **National Cyber Security Strategy** is the official domestic strategy on cybersecurity. It is based on the five principles of sovereignty, independence, security, togetherness, and adaptive.[39] Based on the principles, the Indonesian State Cyber and Crypto Agency (*Badan Siber Dan Sandi Negara* (BSSN)) is meant to further develop policies on cyber resilience, public service security, cyber law enforcement, cyber security culture, and cyber security in the digital economy.[40] Related aspects of cybersecurity including data protection and information security are governed by multiple laws such as **Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (GR82)**.[41]

CMF begins implementation of Fintech Act
https://www.cmfchile.cl/portal/principal/613/w3-article-60379.html
Mar 2024 Chile enacts Cybersecurity and Critical Information Infrastructure Law https://www.olartemoure.com/en/cybersecurity-framework-law/

Dec 2023 - Released - Measures for the Management of Cybersecurity Incident Reports
Aug 2023 Compliance Audit of Personal Information Protection Administrative Measures (Draft for Comment)
Jan 2024 Regulations on the Protection of Minors in Cyberspace
2022-current Focus on Critical Infrastructure Security reviews

On June 20, the Indonesian Temporary National Data Centre was compromised by the hacker group Brain Cipher. The resulting data loss disrupted services for nearly 300 central and local state agencies, including immigration services and major airports. https://www.asiapacific.ca/publication/indonesian-government-under-fire-after-cyber-breaches
To take responsibility for it, Semuel Abrijani Pangerapan resigned as director general of applications and information at KOMINFO https://www.scmp.com/week-asia/politics/article/3269373/indonesias-top-communications-ministry-leader-quits-after-cyberattack-cripples-services



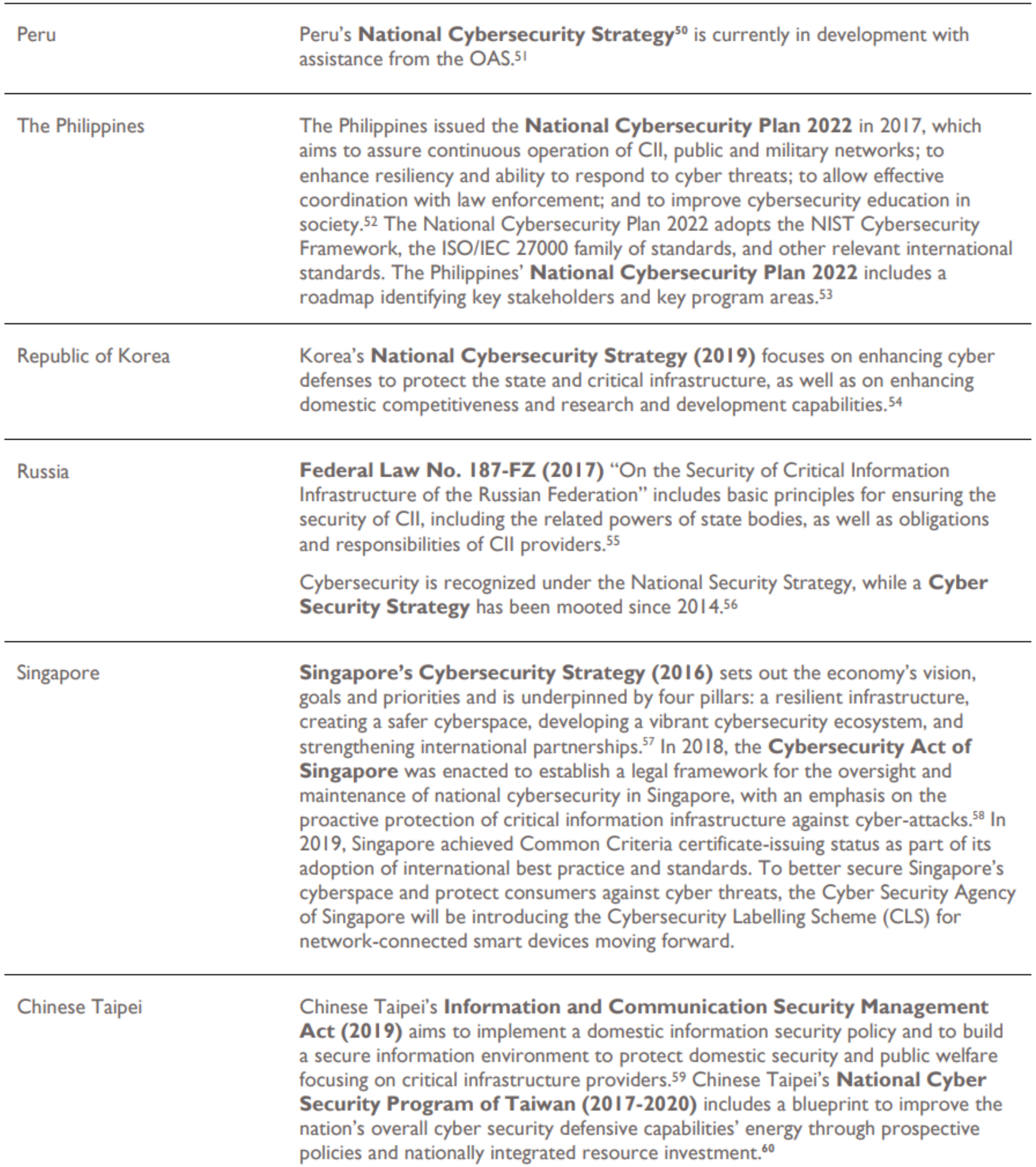
Japan	The officially recognized domestic strategy for cybersecurity is Japan's **Cybersecurity Strategy,** which was revised in 2018 to take into account potential new threats related to the 2020 Olympic Games and the Internet of Things (IoT),[42] In 2017, the Ministry of Economy, Trade and Industry (METI) and the Independent Administrative Agency Information-Technology Promotion Agency (IPA) revised their **Cybersecurity Management Guidelines**.[43] The revised guidelines are very much aligned with the recommendations herein and the NIST Cybersecurity Framework. In 2019, METI also introduced its **Cyber/Physical Security Framework (CPSF)**.[44]
Malaysia	The first **National Cyber Security Policy (NCSP)** was developed in 2005 to support Malaysia's Vision 2020, and a new comprehensive NCSP is currently being developed by the National Cyber Security Agency.
Mexico	Mexico recognized the **National Cybersecurity Strategy (2017)** as its domestic strategy on cybersecurity. [45] This was developed in collaboration with the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) to build a resilient economy by strengthening cybersecurity across social, economic and political spheres and using ICTs in a responsible and sustainable manner.[46]
New Zealand	The **Cyber Security Strategy** (revised July 2019) is New Zealand's domestic strategy for cybersecurity. It identifies priority areas for the government to work together with individuals, businesses, and communities to enhance cybersecurity.[47]
Papua New Guinea	In Papua New Guinea, a new **National Cybersecurity Policy and Strategy** has been under development since 2017.[48] **The Cybercrime Code Act** (2016) criminalizes harmful cyber activities, including cyber-attacks on critical infrastructure.[49]

In 2023, Japan's data protection law, the Act on Protection of Personal Information (APPI), was amended.
May 2023 new regulation Medical Device Cybersecurity established
Mar 2023 Japan updated it Cybersecurity Management Guidelines Ver. 3.0

2024 Malaysia's cyber security act 2024 (act 854) gazetted

Apr 2024 Exposure draft of a biometric processing code of practice

2024 released National Cyber Security Strategy



Peru	Peru's **National Cybersecurity Strategy**[50] is currently in development with assistance from the OAS.[51]
The Philippines	The Philippines issued the **National Cybersecurity Plan 2022** in 2017, which aims to assure continuous operation of CII, public and military networks; to enhance resiliency and ability to respond to cyber threats; to allow effective coordination with law enforcement; and to improve cybersecurity education in society.[52] The National Cybersecurity Plan 2022 adopts the NIST Cybersecurity Framework, the ISO/IEC 27000 family of standards, and other relevant international standards. The Philippines' **National Cybersecurity Plan 2022** includes a roadmap identifying key stakeholders and key program areas.[53]
Republic of Korea	Korea's **National Cybersecurity Strategy (2019)** focuses on enhancing cyber defenses to protect the state and critical infrastructure, as well as on enhancing domestic competitiveness and research and development capabilities.[54]
Russia	**Federal Law No. 187-FZ (2017)** "On the Security of Critical Information Infrastructure of the Russian Federation" includes basic principles for ensuring the security of CII, including the related powers of state bodies, as well as obligations and responsibilities of CII providers.[55] Cybersecurity is recognized under the National Security Strategy, while a **Cyber Security Strategy** has been mooted since 2014.[56]
Singapore	**Singapore's Cybersecurity Strategy (2016)** sets out the economy's vision, goals and priorities and is underpinned by four pillars: a resilient infrastructure, creating a safer cyberspace, developing a vibrant cybersecurity ecosystem, and strengthening international partnerships.[57] In 2018, the **Cybersecurity Act of Singapore** was enacted to establish a legal framework for the oversight and maintenance of national cybersecurity in Singapore, with an emphasis on the proactive protection of critical information infrastructure against cyber-attacks.[58] In 2019, Singapore achieved Common Criteria certificate-issuing status as part of its adoption of international best practice and standards. To better secure Singapore's cyberspace and protect consumers against cyber threats, the Cyber Security Agency of Singapore will be introducing the Cybersecurity Labelling Scheme (CLS) for network-connected smart devices moving forward.
Chinese Taipei	Chinese Taipei's **Information and Communication Security Management Act (2019)** aims to implement a domestic information security policy and to build a secure information environment to protect domestic security and public welfare focusing on critical infrastructure providers.[59] Chinese Taipei's **National Cyber Security Program of Taiwan (2017-2020)** includes a blueprint to improve the nation's overall cyber security defensive capabilities' energy through prospective policies and nationally integrated resource investment.[60]

National Cybersecurity Plan 2023-2028 released https://dict.gov.ph/wp-content/uploads/2024/02/NCSP-2023-2028-FINAL.pdf

Feb 2024 Gov't unveils Nat'l Cybersecurity Strateg with new focus on N. Korea https://en.yna.co.kr/view/AEN20240201007800315

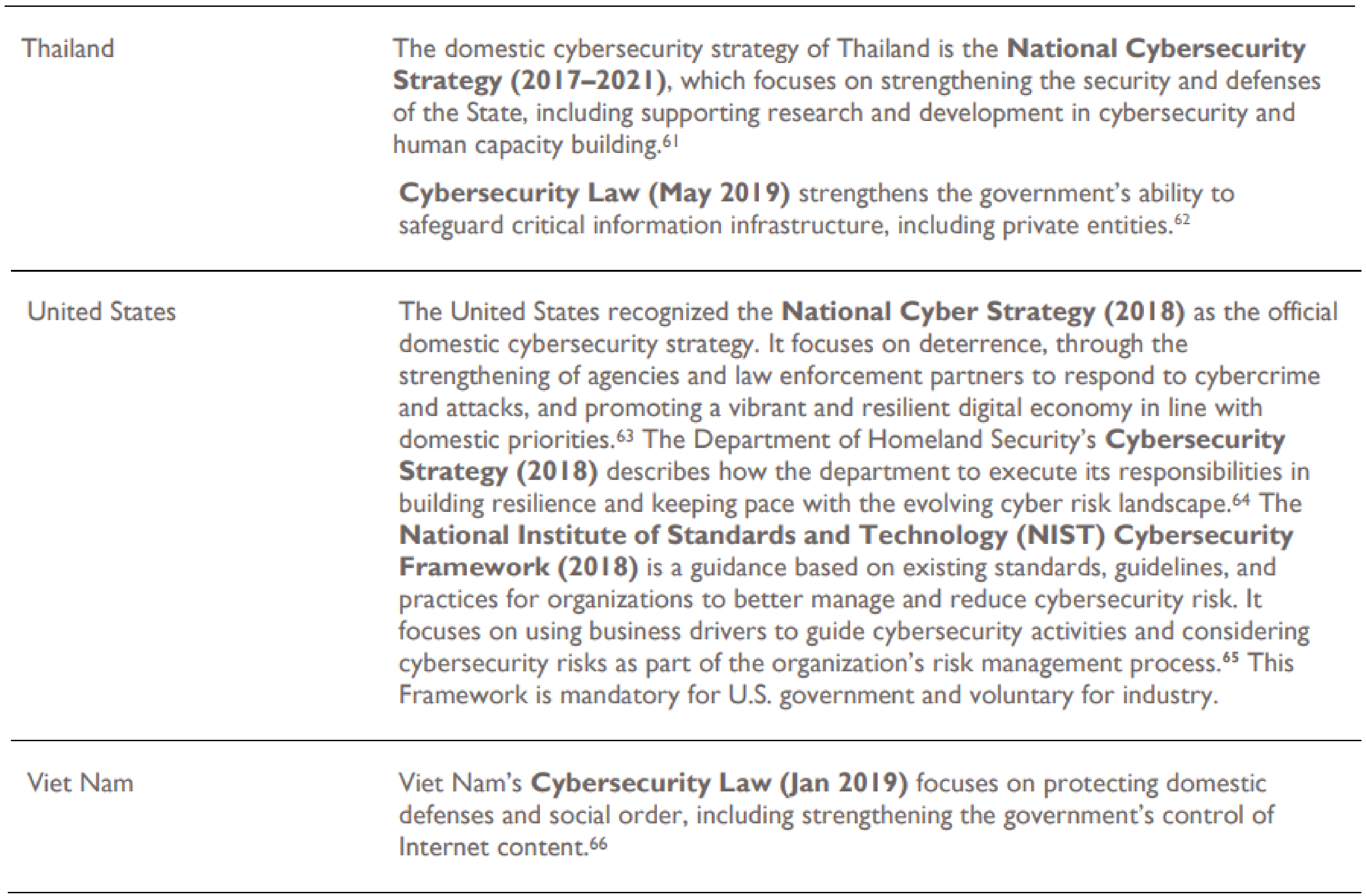
4 Jun 2024 Easy to use AI cloud… Easing financial 'netwo separation' regulations https://www.hankyung.com/article/2024070430251

Apr 2024 Cybersecurity (Amendment) Bill

https://www.channelnewsasia.com/singapore/cybersecurity-critical-information-infrastructure-csa-parliament-4238971

Also 2023-2024 – Operational Technology Masterplan being updated

Cyber Security Management Act (CSMA) may be updated in 2024 or 2025



Thailand	The domestic cybersecurity strategy of Thailand is the **National Cybersecurity Strategy (2017–2021)**, which focuses on strengthening the security and defenses of the State, including supporting research and development in cybersecurity and human capacity building.[61] **Cybersecurity Law (May 2019)** strengthens the government's ability to safeguard critical information infrastructure, including private entities.[62]
United States	The United States recognized the **National Cyber Strategy (2018)** as the official domestic cybersecurity strategy. It focuses on deterrence, through the strengthening of agencies and law enforcement partners to respond to cybercrime and attacks, and promoting a vibrant and resilient digital economy in line with domestic priorities.[63] The Department of Homeland Security's **Cybersecurity Strategy (2018)** describes how the department to execute its responsibilities in building resilience and keeping pace with the evolving cyber risk landscape.[64] The **National Institute of Standards and Technology (NIST) Cybersecurity Framework (2018)** is a guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management process.[65] This Framework is mandatory for U.S. government and voluntary for industry.
Viet Nam	Viet Nam's **Cybersecurity Law (Jan 2019)** focuses on protecting domestic defenses and social order, including strengthening the government's control of Internet content.[66]

June 2024 -- Thailand Prepares Criteria for Personal Data Deletion, Destruction, and De-Identification

7 May 2024 Biden-Harris Administration Releases Version 2 of the National Cybersecurity Strategy Implementation Plan https://www.whitehouse.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/

29 Apr 2024 NIST AI Risk Management Framework launched https://www.nist.gov/itl/ai-risk-management-framework

Jun 2024 – draft decree on administrative sanctions for cybersecurity violations expected to take effect https://www.vietnam-briefing.com/news/vietnams-latest-draft-decree-on-sanctions-for-cybersecurity-violations.html