CHAPTER

8 | ENSURING CYBERSECURITY FOR DIGITAL SERVICES TRADE

Lennon Yao-Chung Chang and Han-Wei Liu

8.1 Introduction

Digital technologies are not only transforming conditions for international trade but also how criminals behave. Cybercriminals are not only chasing money but also collecting data online for diverse purposes, including monetary gain, revenge, and political purposes. Cybercrime is a worldwide concern. The old criminology adage "where there's money, there's crime" is now joined by "where there is data, there is crime."

Insecurity in the global cyberspace is often in the news. In July 2022, 23 terabytes of personal data from the People's Republic of China (PRC) police agency were for sale online. The dataset includes a billion records, mostly on PRC citizens, and is the largest ever sale of data on record (Tidy 2022; Xiao 2022). In June 2021, Colonial Pipeline, the largest pipeline operator in the United States (US), providing about 45% of the nation's east coast's fuel supply, was forced to close its business due to cyberattacks (BBC News 2021). That same month, JBS, the world's largest meat processor, paid an $11 million ransom to resolve a cyberattack (Bunge and Newman 2021). Economies in Asia and the Pacific are also suffering from serious cyberattacks. For example, AXA, one of the world's biggest cyber insurance companies, suffered a serious ransomware attack at its Asian offices in May 2021 (Ikeda 2021). Kaspersky, an information security service provider, counted more than 2.7 million ransomware activities in the Association of Southeast Asian Nations (ASEAN) in the first three quarters of 2020 (Interpol 2021). In recent years, ransomware attacks have crippled critical infrastructure in the US and Asian economies and disrupted global supply chains. It shows that no firm is safe from insidious cyberattacks, especially so in least developed countries (LDCs), which do not have adequate cyber-capacity and awareness.

With the broader adoption of information and communication technology (ICT), including various emerging technologies such as artificial intelligence, big data, cloud computing, and the Internet of Things, cyberattacks are credible challenges policy makers are facing. The risks of cyberattack trigger different regulatory responses, or lack of response due to limited capacity. Insofar as regulatory interventions affect imports, exports, and foreign investment, they can raise concerns from the perspective of international trade law. Cybersecurity has emerged as a source of commercial, legal, and geopolitical conflict. It is therefore on the agenda of policy makers across areas, including trade.

A common approach can help enhance cybersecurity and facilitate digital trade. Divergent, or even protectionist approaches, can create obstacles to digital trade. Without a clear understanding of cybersecurity laws and policies, industry stakeholders can struggle to adapt to evolving restrictions. Similarly, trade policy makers need to map the issues and reconfigure the global trading system. The aim of this chapter is not to offer an account of cybersecurity governance in the digital trade context. Rather, by illustrating the overall trend in regulatory responses to cybersecurity, it seeks to identify common ground and differences and how well Asia and Pacific economies have adopted them. This inquiry could not only help reveal the implications of domestic regulations of cybersecurity for the global trading system, but more crucially, help map the differences in capacity and readiness to react to emerging threats in cyberspace. Such maps are the key for policy makers to work toward building a resilient digital economy.

The terms "cybersecurity" and "cybercrime" go beyond technical definitions and reflect how policy makers perceive concerns and react to them as a matter for regulation. This chapter provides a deeper understanding of regulatory concerns by identifying common cybersecurity threats in Asia, while offering an overview of international and national responses, in particular approaches that can disrupt the open internet and digital trade the most, such as data localization measures.

The Council of Europe's Convention on Cybercrime (Budapest Convention) is perhaps the most important international initiative to help like-minded nations manage some of these cybersecurity concerns. The Budapest Convention could serve as a good point to reflect upon the economy's readiness in developed and developing economies in the field. Key features of preferential trade agreements (PTAs) explored in this chapter can help moderate trade concerns related to cybersecurity issues, directly or indirectly, and—as also discussed in this chapter—can be supported by more informal arrangements.

8.2 Cybersecurity as a Regulatory Concern

The development of technology and the internet is a double-edged sword. On the one hand, it has transformed our everyday life, from ways we communicate with people to how we do business. The work, study, and business operated from home during the coronavirus disease (COVID-19) pandemic would not be possible without the support of new technology and the internet. However, the development of technology and the internet also provides criminals with a new tool to commit the crime. As the internet was built initially for research purposes rather than commercial use, security mechanisms were not considered in the design. The borderless characteristics of the internet also create barriers to investigating crime. Routine Activity Theory teaches that a crime happens when a potential offender meets a suitable target when capable guardians are not present. Cyberspace has created ample space where guardians are not capable most of the time due to a range of reasons illustrated below.

8.2.1 Defining Cybersecurity and Cybercrime

Defining the term "cybersecurity" can be as complex as managing trade concerns around cybersecurity. While no universally agreed definition of this term exists, from a technical and data-driven perspective, cybersecurity is often linked to the CIA Triad—*confidentiality*, *integrity*, and *availability—of* information.[1] A well-known definition along this line comes from the International Telecommunication Union, which refers to cybersecurity as a

> collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets... Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[2]

The National Institute of Standards and Technology of the US, as related in Kissel (2013) and its updates, elaborates on each of these dimensions:

- *Confidentiality*—"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."
- *Integrity*—"Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. Data integrity covers data in storage, during processing, and while in transit. Typical measures include file permissions and user access controls."

[1] International Organization for Standardization. ISO/IEC 27032:2012 (Information Technology—Security Techniques—Guidelines for Cybersecurity). https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (accessed July 2022).

[2] International Telecommunication Union (ITU). Definition of Cyberspace. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (accessed July 2022).

- *Availability*—"Ensuring timely and reliable access to and use of information. It is ensured by hardware maintenance, regular and timely system upgrades, but also disaster recovery plans."

Defining cybersecurity, however, is more than a technical issue. This term is often colored by politics, which elevates it as a geopolitical concern (Koh 2020; Meltzer and Kerry 2019). In some economies, cybersecurity is widely perceived to include any digital information that can threaten social or political stability—which could be framed as a matter of internet sovereignty and national security. The PRC and Viet Nam are prime examples.[3] Under its Cybersecurity Law, for instance, the PRC conceptualizes cybersecurity as a matter of "safeguarding the cyberspace sovereignty, national security and public interests, protecting the lawful rights and interests of citizens, legal persons, and other organizations, and promoting the sound development of economic and social information technology" (Article 1 of the PRC Cybersecurity Law). Broadly framed, cybersecurity could be seen as concerning both the traditional CIA Triad and information distributed online—including, notably, disinformation, fake news, or misinformation.[4]

While it is important to understand the linkage between cybersecurity and digital trade, one should not ignore the impact of cybercrime on digital trade. Cybercrime refers to criminal offenses that are committed using and/or targeting computers and telecommunications (Smith, Grabosky, and Urbas 2001). It is argued that "cybercrime" tends to be used "metaphorically and emotively rather than scientifically or legally" (Wall 2007). Just like the term "white collar crime" has been used for about 50 years, academia uses these terms to "delimit the scope of computer-related misconduct" (Smith, Grabosky, and Urbas 2001). On one hand, cybercrime can be conventional crime facilitated by the internet, such as online fraud and telecommunication scams. On the other hand, it can include new crimes developed out of the advancement of computing technologies, such as hacking, Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, phishing, and botnets.

[3] Cybersecurity Law of the PRC, effective 1 June 2017 (English translation available at Westlaw China); Law on Cybersecurity of Viet Nam, effective 12 June 2018 (English translation prepared by Allens Linklaters, https://www.allens.com.au/insights-news/insights/2018/06/vietnam-issues-a-stringent-new-cybersecurity-law/).

[4] Even in the Western world, it is not uncommon to see governments address the threats of fake news in the context of cybersecurity. See, for example, Buckmaster and Wils (2019).

Similar to cybersecurity, there is no universally agreed definition of cybercrime. That said, academics have classified cybercrime into three general forms (Grabosky 2016) while noting that the three types somewhat overlap:

(i) Crimes where the computer is used as the instrument of crime, such as phishing, producing, and disseminating child pornography;
(ii) Crimes where the computer is the target of crime, such as denial of service attack; and
(iii) Crimes where the computer is incidental to the offense, such as maintaining records of criminal transactions such as money laundering and drug dealing.

Indeed, remarkable overlap can be seen between the computer as instrumental and the computer as incidental. These two types of cybercrime are mainly conventional crimes facilitated by new technology, which can be called "cyber-enabled crime." On the other hand, for crimes where the computer is the target of crime, these are crimes that did not exist before the digital age and are highly dependent on new technology. Thus, they can be called "cyber-dependent crime" (McGuire and Dowling 2013).

Statistics from government and industry demonstrate the drastic increase in the number, and increasing seriousness, of cybercrime. According to the 2020 Internet Crime Report, the Federal Bureau of Investigation's Internet Crime Complaint Centre (IC3) received about 800,000 cybercrime complaints, which is 2.5 times higher than in 2016 (298,728). The financial loss from these crimes reaches $4.2 billion in 2020, about three times more than it was in 2016 ($1.5 billion). The top cybercrime types are phishing (including vishing, smishing, and pharming), nonpayment and nondelivery, extortion, personal data breach, and identity theft.

8.2.2 Identifying Emerging Threats in Cyberspace

From the definition and classification of cybercrime and cybersecurity, we can see that digital trade and services are not only impacted by weaknesses in technology and systems, but can also be impacted by users who control or use the technology. Some prevalent and emerging threats that might impact digital trade, especially for developing economies and LDCs in Asia, include the following:

- *Botnets*—These are still very popular and are used to commit cybercrime and breach cybersecurity. A botnet is a network of bot-infected computers. A bot-infected computer is a computer that contains a malicious computer program, malware, which allows the computer to be controlled remotely. Usually, the program is installed secretly without the owner's understanding. The use of botnets as springboards to launch a cyberattack or cybercrime creates barriers to crime investigation. Large botnets can contain millions of bot-infected computers and can be used to launch a DDoS, a massive attack to disrupt traffic of a targeted server or network by flooding the bandwidth. This can cause severe damage to critical infrastructure, such as online banking, and interrupt digital transactions. It has been deemed the new architecture of cyber-organized crime (Chang 2012). They are also used to disseminate *ransomware*, a type of malicious computer software used by criminals to encrypt victims' files and data and ask for a ransom payment to get codes to decrypt the file. For example, the Colonial Pipeline and the JBS USA holdings were ransomware attacks. Reports have shown that ASEAN economies are suffering from ransomware attacks (Thomas 2019).

- *ATM heists*—Using sophisticated malicious computer software, international organized crime syndicates have stolen money from automatic teller machines (ATMs). This has occurred not only in developed economies like the US. It has also happened in developing and middle-income economies in Asia (Chang 2017).
- *Phishing*—This has been reported as a way criminals gain access to ATMs. When phishing, criminals obtain confidential user information, such as the login ID and password for online banking, personal data, a business login, and credit card details. Using social engineering skills, criminals masquerade as a trusted entity, luring the victim to open an e-mail, click on a link or text message and/or to fill out a fake form. It can be done by sending an e-mail, by voice message (*vishing*), by SMS text (*smishing*), and by redirecting the link to a fake website, rather than a legitimate one (*pharming*). As mentioned, phishing is on the top of IC3's list of cybercrimes. Phishing is usually not personalized or targeted, and expecting anyone to take the bait.
- *Advanced persistent threat (APT)*—This is similar to phishing but more targeted and is becoming popular. The malicious software and/or social engineering skills designed for advanced persistent threat (APT) are usually customized, targeting a specific entity or region. Also, they are designed usually for sensitive data such as government classified information, trade secrets, and intellectual property, rather than for direct financial gain. For example, PLATINUM, a malicious computer software, was designed to access sensitive government data in South and Southeast Asian economies (Microsoft 2016).
- *Business email compromise*—Such a scam can easily be launched using information about an entity/company acquired through APT. According to Trend Micro, business email compromise (BEC) is "a type of scam targeting companies who conduct wire transfers and have suppliers

> abroad." While this has been highlighted in the IC3 report as a serious issue, it is actually critical in Asia, especially for companies in economies that are under sanctions, as they usually need to use another company outside the country to accept a money transfer, which allows criminals to take the role as agents.

In response to these cybersecurity and cybercrime issues, more and more economies have introduced cybersecurity laws and personal data protection laws. While these regulatory initiatives have their merits, the free flow of information can be impeded by how each country designs and implements them, leading to a fragmented internet. The introduction of cybersecurity and data protection laws are pushing in the direction of a localized internet and are a constraint on a free and open internet. The control of data and data flow might significantly hamper the development of digital trade and services and would create barriers to trade negotiation. The power to allow a government to shut down the internet to manage damaging and uncontrollable events to the government (e.g., spreading of misinformation or information operations) also needs to be considered while developing digital trade and services. Last, digital literacy, and especially cybersecurity awareness, is key to promoting successful digital trade and services.

8.2.3 International and National Responses

Cybercrime and cybersecurity concerns are being tackled through international and national measures. The Council of Europe drafted the Convention on Cybercrime (the Budapest Convention) in 1989 to account for the "borderless" nature of cybercrime. It was opened for signature by both member and nonmember states and entered into force on 1 July 2004 after ratification by five member economies.[5] The Budapest Convention is viewed as the first international treaty focusing on combating cybercrime and has been noted by the United Nations (UN) General Assembly (resolution 56/121), which invited its member states to become signatories (Chang 2012).

The Budapest Convention aims to facilitate adoption of adequate international legal instruments against cybercrime. Computer-related offenses relating to the confidentiality, integrity, and availability of computer data are among them. They include (i) illegal access to a computer system; (ii) interception of nonpublic transmissions of computer data to, from, or within a computer system; (iii) interference with computer data; (iv) interference with

[5] According to the Council of Europe, only after ratification by five states (including at least three members) would the Convention enter into force. Albania, Croatia, Estonia, Hungary, and Lithuania were the first five states to ratify.

computer systems, such as computer sabotage; and (v) the misuse of computer-related devices (e.g., "hacker tools"), including the production, sale, procurement for use, import, or distribution of such devices. It also covers cyber-enabled crimes such as the traditional offenses of fraud and forgery when carried out through a computer system, child sexual exploitation using the internet, and offenses relating to copyright infringement. On the procedural part, it regulated real-time data sharing and asked its signatories to create 24/7 contact points for an international computer crime assistance network. While 66 economies, including Australia, Japan, the Philippines, and the US, have ratified or acceded to the Budapest Convention, the Russian Federation, supported by the PRC, is proposing a separate treaty at the UN level (Chang 2012), sharing similarities with the Budapest Convention while presenting significant differences in enforcement, with more autonomy given to states in their own investigation (ADB 2021).

Australia has promoted the Budapest Convention. In its International Cyber and Critical Technology Engagement Strategy, the Australian government supports economies in the Indo-Pacific region to build cyber resilience and promote the convention. It has also become an essential part of Australia's development cooperation program, which helps developing and least developed economies in Asia and the Pacific to improve their regulations and capacity on cybersecurity (Government of Australia, DFAT 2021).

In the past few years, while economies in Asia and the Pacific have developed cybersecurity and cybercrime laws, not all are aligned with the Budapest Convention. While most economies in the region are strongly aligned with the convention, some developing economies are weakly aligned and would benefit from developing their legal systems to improve cybersecurity and combat cybercrime (Chang 2020).

Cyberattacks can cause a chain reaction (Chang 2012). While it is hard to stop an attack from happening, it is crucial to reduce the harm that an attack could cause to society. Therefore, besides the harmonization of laws on cybercrime and cybersecurity, a risk-based approach has also been adopted by many economies to reduce the harm caused by cyberattacks, especially cyberattacks targeting critical infrastructure. For example, the US introduced the Federal Information Security Management Act, regulating computer incident information sharing among the critical infrastructure industry. Similar approaches have been adopted by Asian economies to encourage the critical infrastructure industry to share their computer incidents so that other companies can take measures in advance. In order to protect national security and prevent cyber espionage, economies like the PRC also require software companies and service providers to make source codes available for review (Dou 2015).

Research has shown the need to help economies strengthen their laws and regulations to combat cybercrime and maintain cybersecurity. We see that cyber capacity building and raising cybersecurity awareness have become essential for aid programs and trade negotiations. For example, the Australian government recently launched the International Cyber and Critical Technology Engagement Strategy. The key for this is to support economies in the Indo-Pacific region, especially LDCs, to draft laws that meet the international standard, such as the Budapest Convention, and equip them with better cyber environments by building a risk-based approach to ensure cybersecurity.

8.3 Regulatory Cooperation: The State of Play

The lack of cybersecurity is costly and can undermine the trust of consumers and businesses in engaging in the digital context. Protecting confidence in an online world involves cross-border collaboration between the public and private sectors, as individuals, businesses, and governments that operate through the global networks can face the same threats (Meltzer and Kerry 2019). Many of the regulatory models—such as Australia, the PRC, and the US—feature the "risk-based" approach by identifying "critical infrastructure" and imposing strict obligations on the relevant operators. The PRC and others have gone even further by mandating local storage of data and obtaining source codes. Others, such as developing economies and LDCs in the ASEAN, however, are yet to maintain adequate measures.

World Trade Organization and Preferential Trade Agreements

The internet and the way we trade in terms of goods and services around it was entirely different from today when the World Trade Organization (WTO) was established in the 1990s. The WTO is therefore not well-equipped with tools to address cybersecurity explicitly—or measures in its name, except certain disciplines such as nondiscrimination (e.g., General Agreement on Trade in Services [GATS] Article II), security exception (e.g., GATS Article XIV *bis*), and general exception (e.g., GATS Article XIV) that may be applicable.[6] These exceptions, however, are far from satisfactory to manage trade conflicts that arise from cybersecurity. For one, these rules are subject to the judicial interpretation after the fact and on a case-by-case basis. There is room for WTO members to maneuver. Another, and more crucial reason, is that where a member defends itself under the security exception, WTO adjudicators may find it politically sensitive to review the disputed

[6] Marrakesh Agreement Establishing the World Trade Organization, opened for signature 15 April 1994, 1867 UNTS 3 (entered into force 1 January 1995) Annex 1A (General Agreement on Tariffs and Trade 1994 or GATT), Annex 1B (General Agreement on Trade in Services or GATS). Mitchell and Hepburn (2017) argued for instance that the former European Union (EU)–US Safe Harbor arrangement may violate the most-favored-nation (MFN) obligation under GATS Article II:1.

measures. There is significant uncertainty, as Tania Voon remarks, around the security exception (Voon 2019). Some economies, hence, attempt to reconfigure the rules to provide greater certainty and clarity for businesses and policy makers both within and outside the WTO context. Within the WTO, for instance, the consolidated negotiating text on e-commerce recently released seems to signal the willingness of some members to tackle these recurring issues in the digital age (WTO 2020). While it remains to be seen how WTO members come up with new solutions, the new development of preferential trade agreements (PTAs) is a good reference point to identify the key instruments for trade policy makers to harness trade concerns around cybersecurity. We now consider them in turn.

Cybersecurity Cooperation Clause

Recent PTAs often feature a provision dedicated to cybersecurity—under the title of "Cybersecurity,"[7] "Cooperation on Cybersecurity Matters,"[8] or "Cybersecurity Cooperation."[9]

However, given the complex nature of cybersecurity and the capacity gap among economies, the cybersecurity clauses typically take the form of "soft law" rather than "hard law"—they are not binding, enforceable commitments. Using the expressions "recognize," "shall endeavor to," or something along this line, these PTAs seek to shape the confidence in digital trade and focus on capacity building and information sharing. To illustrate, let us consider some of the US-led PTAs. Article 19.15 of the United States–Mexico–Canada Agreement (USMCA) states that:

> (a) 1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:
>
> 7.2.1.1 build the capabilities of their respective national entities responsible for cybersecurity incident response; and
>
> 7.2.1.2 strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

[7] Agreement between the United States of America, the United Mexican States, and Canada (USMCA), Chapter 28, 30 November 2018, Article 19.15; Agreement between the United States and Japan Concerning Digital Trade (US–Japan DTA), signed 7 October 2019, Article 19; Regional Comprehensive Economic Partnership Agreement (RCEP), Article 12.13.

[8] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Chapter 25, 8 March to 30 December 2018, [2018] A.T.S. 23 (incorporating, by reference, the provisions from the Trans-Pacific Partnership), Article 14.16.

[9] Digital Economy Partnership Agreement (DEPA), Chile–New Zealand–Singapore, NZTS. B2020-02, signed 12 June 2020, Article 5.1.

The US–Japan Digital Trade Agreement (US–Japan DTA) also features a cybersecurity provision (Article 19), copied nearly word for word from Article 19.15 of the USMCA. Likewise, Article 14.16 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) provides that the signatories recognize the importance of "building the capabilities of their national entities responsible for computer security incident response," and collaboration to "identify and mitigate malicious intrusions or dissemination of malicious code" that affect their electronic networks.

Arrangements of this sort can also be found in PTAs that involve Asian economies, such as the Regional Comprehensive Economic Partnership (RCEP),[10] the world's largest trading bloc with a diverse group of nations—including ASEAN states; the Digital Economy Partnership Agreement (DEPA), between New Zealand, Singapore, and Chile; [11] and the Australia–Singapore Digital Economy Agreement (DEA),[12] among others.

Notably, DEPA and the Australia–Singapore DEA have two unique features compared with others. First, while they both recognize the role of capacity building, they underscore in particular the importance of "workforce development in the area of cybersecurity, including through possible initiatives relating to mutual recognition of qualifications, diversity and equality."[13] Second, both DEPA and the Australia–Singapore DEA add a provision called "Online Safety and Security" or "Creating a Safe Online Environment" on top of a general clause on cybersecurity. [14] Article 5.2 of DEPA, for instance, reads:

> (1) The Parties recognise that a safe and secure online environment supports the digital economy.
> (2) The Parties recognise the importance of taking a multi-stakeholder approach to addressing online safety and security issues.
> (3) The Parties shall endeavour to cooperate to advance collaborative solutions to global issues affecting online safety and security.

It is also noteworthy that, while new PTAs do not require signatories to adopt specific legislation, some do highlight the "risk-based" approach as a guiding principle for parties to regulate cybersecurity. USMCA Article 19.15 states:

[10] RCEP, Article 12.13.

[11] DEPA, Article 5.1

[12] Australia–Singapore DEA, effective 8 December 2020, Article 34.

[13] DEPA, Article 5.1. Note, however, that Article 34 (2)(c) of the Australia–Singapore DEA contains similar language: "The Parties recognise the importance of (c) workforce development in the area of cybersecurity, including possible initiatives relating to mutual recognition of qualifications, diversity and equality."

[14] DEPA, Article 5.2; Australia–Singapore DEA, Article 18.

> 2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

This risk-based approach is consistent with the recommendation of the Organisation for Economic Co-operation and Development (OECD), which states that the "treatment of the risk should aim to reduce the risk to an acceptable level relative to the economic and social benefits expected from those activities while taking into account the potential impact on the legitimate interests of others" (OECD 2015). [15]

Cross-Border Data Flow and Data Localization

As noted, it is not uncommon to see economies restrict cross-border data flow or mandate local data storage in the name of cybersecurity or data protection. Consider, for instance, data localization measures. Although some cast doubt on its role in combating cybercrime (Chander and Uyên 2015), others consider data localization an effective tool for law enforcement authorities to gather evidence to identify and arrest cybercriminals (Selby 2017). For some nations, it is argued that, data localization can help resolve the practical difficulty of accessing evidence through the Mutual Law Enforcement Assistance Treaty and lessen the comparative disadvantage in intelligence agencies (Selby 2017). In recent years, trade policy makers have reacted to the growing concerns by committing to cross-border data flow—subject to certain conditions—and restricting data localization measures.

The CPTPP is, again, a prime example. Article 14.11, while recognizing there may be different regulatory approaches toward data transfer, requires that the "Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." Article 14.13 further provides that data localization measures are prohibited unless they meet certain qualifications:

[15] In this regard, regulatory frameworks of, notably, the US, the EU, and Australia also underscore the risk-based approach. See, for example, Australian Cyber Security Centre. Using the Information Security Manual. Canberra. https://www.cyber.gov.au/acsc/view-all-content/advice/using-information-security-manual (accessed 21 July 2022).

> 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, if the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

In other words, the CPTPP attempts to facilitate digital trade by balancing cross-border information flow and the public interests of the signatories. USMCA Articles 19.11 and 19.12, US–Japan DTA Articles 11 and 12, DEPA Articles 4.3 and 4.4, Australia–Singapore DEA Articles 17 and 24, and RCEP Articles 12.14 and 12.15 generally follow a similar logic, though with some variants.

Some observations are warranted. First, some of these new PTAs contain references to the principles or guidelines developed by relevant international bodies in crafting their regulatory frameworks on personal information protection or facilitating cross-border data flow. For instance, Article 17 of the Australia–Singapore DEA refers to the APEC Cross-Border Privacy Rules as a "valid mechanism to facilitate cross-border information transfer while protecting information."

Second, the US–Japan DTA extends the data localization provision to cover "Financial Services Computing Facilities for Covered Financial Services Suppliers" (Article 13). Third, while the RCEP and the CPTPP ban data localization, certain flexibility is made available to developing economies in terms of enforcement timelines.

Nondisclosure of Source Code

Requiring source codes can sometimes be framed as a matter of cybersecurity regulation (Meltzer and Kerry 2019). Some of the recent PTAs have addressed this concern. For instance, CPTPP Article 14.17 reads:

> 1. No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale, or use of such software, or of products containing such software, in its territory.
> 2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure.
> 3. Nothing in this Article shall preclude: (a) the inclusion or implementation of terms and conditions related to the provision

> of source code in commercially negotiated contracts; or (b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement.
> 4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorized disclosure under the law or practice of a Party.

Source code provisions also exist in other US-led PTAs, such as USMCA Article 19.16 and US–Japan DTA Article 17. It can also be found in Article 28 of the Australia–Singapore DEA. However, neither the DEPA nor the RCEP has such a clause, except a reference in Article 12.16 of RCEP that mentions "current and emerging issues, such as … source code" shall be considered when signatories have a dialogue on e-commerce.

Nondisclosure of Encryption Technologies

As in the case of source codes, forced transfer of encryption technologies can also be framed—though not necessarily justifiably—as part of cybersecurity matters. The CPTPP is the first PTA that responds to it. In Annex 8-B, Section A, entitled "Information and Communication Technology (ICT) Products that Use Cryptography," the CPTPP defines *cryptography* as "the principles, means or methods for the transformation of data to hide its information content, prevent its undetected modification or prevent its unauthorized use; and is limited to the transformation of information using one or more secret parameters, for example, crypto variables, or associated key management," and refers to *encryption* as the conversion of data (plaintext) into a form that cannot be easily understood without subsequent reconversion (ciphertext) through the use of a cryptographic algorithm."[16] It then prohibits governments from requiring transfer or access to specific technologies as a condition for market access. In the relevant part, it states:

> 3. With respect to a product that uses cryptography and is designed for commercial applications, no Party shall impose or maintain a technical regulation or conformity assessment procedure that requires a manufacturer or supplier of the product, as a condition of the manufacture, sale, distribution, import or use of the product, to:

[16] CPTPP, Annex 8-B.2. Liu (2017) provides a legal and geopolitical analysis.

> (a) transfer or provide access to a particular technology, production process or other information, for example, a private key or other secret parameter, algorithm specification or other design detail, that is proprietary to the manufacturer or supplier and relates to the cryptography in the product, to the Party or a person in the Party's territory;
> (b) partner with a person in its territory; or
> (c) use or integrate a particular cryptographic algorithm or cipher, other than where the manufacture, sale, distribution, import or use of the product is by or for the government of the Party.[17]

However, the CPTPP also considers the needs of public law enforcement by clarifying that this section "shall not be construed to prevent a Party's law enforcement authorities from requiring service suppliers using encryption they control to provide, pursuant to that Party's legal procedures, unencrypted communications."[18] USMCA Article 12.C.2, US–Japan DTA Article 21, DEPA Article 3.4, and Australia–Singapore DEA Article 7 feature similar arrangements, though there is no analogous clause in the RCEP.

Memorandums of Understanding

Beyond trade negotiations, some economies have or are currently engaging one another through an informal, nonbinding memorandum of understanding (MOU) to facilitate regulatory cooperation on cybersecurity. Australia is a notable example. It has signed MOUs with Singapore, Indonesia, Papua New Guinea, Thailand, and others in relation to cybersecurity matters.[19] These MOUs feature similar language as seen in the cybersecurity clause in recent PTAs mentioned above—though they often provide more detail.

[17] CPTPP, Annex 8-B.3.

[18] CPTPP, Annex 8-B.5

[19] Australia–Singapore MOU on Cybersecurity Cooperation. https://www.csa.gov.sg/news/press-releases/singapore-signs-mou-with-australia-to-enhance-cybersecurity-collaboration; MOU between the Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation (AU–Indonesia MOU on Cyber Cooperation). https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/mou-indonesia-australia-cyber-cooperation; MOU between the Government of Australia and the Government of Papua New Guinea Relating to Cybersecurity Cooperation (AU–PNG MOU on Cyber Security Cooperation). https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/mou-between-papua-new-guinea-and-australia-relating-to-cyber-security-cooperation; Australia–UK–Thailand MOU on Cyber and Digital Cooperation. https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/mou-on-cyber-and-digital-cooperation-australia-thailand.

The Australia–Indonesia MOU, for instance, emphasizes the significance of sharing information and best practice and capacity building. For capacity building, in particular, the MOU (paragraph 2) sets out more specific plans by stating that:

(i) Participants will support skills and knowledge development in cyber security and cyber policy through short-term training programs and long-term awards (including scholarships for master's and PhD programs);

(ii) Participants will facilitate links between institutions working in the field of cyber security including government, business, or private sector and academia;

(iii) Participants will explore linking research institutions and universities to strengthen teaching and research outcomes in cyber affairs; and

(iv) Participants will explore opportunities to promote international law, norms, and responsible behaviors in cyberspace.

Nevertheless, these MOUs go beyond the typical cybersecurity clause in the PTAs by addressing cybercrime issues or institutionalizing regulatory cooperation. On the former, for instance, the Australia–Indonesia MOU has a provision that both parties "will promote stronger cyber forensic and investigation capacities" (paragraph 2). On the latter, the MOU between Australia and Papua New Guinea states that both will work toward its objectives through a series of "Joint Cybersecurity Initiatives"—funded by Australia—including "establishment of a Cyber Security Operations Centre" to monitor threats and controls, and "enhancement of Papua New Guinea's newly established Computer Emergency Response Team," among others (paragraph 5).

These MOUs on engagement in cybersecurity should be considered with recent regional efforts. The ASEAN's Political-Security Community Blueprint 2025 has addressed the need to combat cybercrimes through regional collaboration (ASEAN Secretariat 2016). In 2019, the ASEAN also issued a "Statement on Cybersecurity Cooperation" with the European Union,[20] and "Joint Chairs' Statement" following its Cyber Policy Dialogue with Australia.[21] More broadly, in the context of APEC, various initiatives are working toward the same goal. For instance, the APEC Cybersecurity Strategy, developed by the APEC Information Working Group in 2002, identified six issue areas—legal developments, information sharing and cooperation initiative, security and technical

[20] ASEAN Secretariat. ASEAN–EU Statement on Cybersecurity Cooperation. https://asean.org/asean-eu-statement-on-cybersecurity-cooperation (accessed July 2022)

[21] Government of Australia, Department of Foreign Affairs and Trade. Joint Chairs' Statement: ASEAN-Australia Cyber Policy Dialogue. https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/joint-chairs-statement-asean-australia-cyber-policy-dialogue (accessed July 2022).

guidelines, public awareness, training and education, and wireless security to "serve as the basis of APEC's efforts on cybercrime and critical infrastructure protection"(NATO CCDCOE 2018). This was followed by the APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment and the APEC Framework for Securing the Digital Economy (APEC 2005, 2019).

There are, of course, other instruments to help build trust in cyberspace and facilitate digital trade. Certification schemes created by the EU Cybersecurity Act[22] and the development of relevant international standards by international standard-setting bodies such as the International Organization for Standardization (ISO) (Dupendant 2016) are prime examples.

8.4 Conclusion

Ensuring cybersecurity and preventing cybercrime is essential for promoting digital trade in services. Digital trade in services will not be successful if the users and clients cannot trust each other. This is especially important for LDCs where digital services are flourishing as the internet expands. It is challenging for these economies to put more resources into issues relating to cybersecurity and cybercrime, given the many priorities competing for government expenditure.

Inquiries so far lead us to make several general recommendations. First, a consensus has formed that cybersecurity presents significant issues across the global supply chain. However, different laws and policies introduced in the name of cybersecurity—which sometimes is framed and elevated as a national security issue—have raised trade barrier concerns in recent years. Such policies not only shape cyberspace within economies, they also increase transaction and communication costs for all economies by fragmenting the internet.

Second, and relatedly, while some regulatory responses may be overreactions and unnecessary to achieve their legitimate policy purposes, one should not overlook the issues around underreaction. Developing economies and LDCs have a daunting task to grapple with the mixed opportunities of ICT. While digital technologies help accelerate social and economic development, they come with costs. Cybercrimes are borderless, as this chapter has noted. Developing economies—particularly LDCs with inadequate regulatory frameworks and limited human capacity and financial resources—find it challenging to react to these threats effectively (ITU 2022). It is problematic for economies to tap into the booming internet and maximize socioeconomic benefits unless there

[22] European Union Agency for Cybersecurity (ENISA). EU Cybersecurity Certification Framework. https://www.enisa.europa.eu/topics/standards/certification (accessed July 2021).

is a secure infrastructure to protect the organizations' assets and resources at different levels—organizational, human, financial, and technical. It is also vital to prevent the clients of digital services and digital trade from becoming victims.

Third, to tackle the ramifications of these regulatory reactions (or lack thereof) for digital trade, there is a need for a new set of rules, which will require cooperation among like-minded economies. It could occur within the existing multilateral trading system—as in the WTO e-commerce negotiations or new PTAs. These new generation trade agreements have begun to reinvent the rules—ranging from cybersecurity cooperation, cross-border information flow, data localization, source code, to encryption. Some of these new rules are "harder" than others—particularly, at cooperation on cybersecurity. Moreover, some offer a grace period for developing economies and LDCs to gradually fit into the new setting. Such arrangements are welcome because they properly acknowledge the gap between economies with different endowments in handling cybersecurity matters. However, more actions are needed. Such a gap, as well as the trade concerns in connection with cybersecurity, can be moderated through other informal arrangements such as MOUs. Of course, the gap could also be narrowed if international organizations like the Asian Development Bank or others can play a more active role in assisting developing economies and LDCs in capacity building. Proper cooperation within and outside the WTO can therefore rebuild the trust in the online environment and facilitate the sustainable growth of global digital trade in the long term.

Bibliography

Asia-Pacific Economic Cooperation (APEC). 2005. *APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment* (Inter-Sessionally Endorsed of the Senior Officials in November 2005). https://www.apec.org/-/media/Files/Groups/TEL/05_TEL_APECStrategy.pdf.

———. 2019. *APEC Framework for Securing the Digital Economy*. https://www.apec.org/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy.

Asian Development Bank (ADB). 2021. *E-Commerce in CAREC Countries: Laws and Policies*. Manila.

ASEAN Secretariat. 2016. *ASEAN Political-Security Community Blueprint 2025*. Jakarta.

BBC News. 2021. Colonial Pipeline Boss 'Deeply Sorry' for Cyber Attack. 8 June. https://www.bbc.com/news/business-57403214.

Buckmaster, L., and T. Wils. 2019. *Parliamentary Library Briefing Book: Responding to Fake News*. Canberra: Parliament of Australia. https://www.aph.gov.au/

About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook46p/FakeNews.

Bunge, J., and J. Newman. 2021. Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants. *Wall Street Journal*. 11 June. https://www.wsj.com/articles/ransomware-attack-roiled-meat-giant-jbs-.

Chander, A. and P. L. Uyên. 2015. Data Nationalism. *Emory Law Journal*. 64 (3). pp. 732–733.

Chang, L. Y. C. 2012. *Cybercrime in the Greater China Region*. Cheltenham, UK: Edward Elgar.

———. 2017. Cybercrime and Cyber Security in ASEAN. In J. H. Liu, M. Travers. and L. Yao-Chung Chang , eds. *Comparative Criminology in Asia*. New York: Springer.

———. 2020. Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia. In T. Holt and A. Bossler, eds. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London: Palgrave Macmillan.

Dou, E. 2015. IBM Allows Chinese Government to Review Source Code. *Wall Street Journal*. 16 October. https://www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

Dupendant, J. 2016. *International Regulatory Co-operation and International Organisations: The Case of the International Organization for Standardization (ISO)*. Paris: Organisation for Economic Co-operation and Development / Geneva: International Organization for Standardization.

Government of Australia, Department of Foreign Affairs and Trade (DFAT). 2021. *International Cyber and Critical Technology Engagement Strategy*. Canberra.

Grabosky, P. 2016. *Cybercrime*. Oxford: Oxford University Press.

Ikeda, S. 2021. Ransomware Attack Reported at Insurance Giant AXA One Week After It Changes Cyber Insurance Policies in France. *CPO Magazine*. 25 May. https://www.cpomagazine.com/cyber-security/ransomware-attack-reported-at-insurance-giant-axa-one-week-after-it-changes-cyber-insurance-policies-in-france/.

International Telecommunication Union (ITU). 2022. *Enhancing Cybersecurity in Least Developed Countries*. Geneva.

Interpol. 2021. Interpol Report Charts Top Cyberthreats in Southeast Asia. 22 January. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia.

Kissel, R., ed. 2013. Glossary of Key Information: Security Terms. *NIST Interagency or Internal Report*. 7298 Rev. 2. Gaithersburg, MD: National Institute of Standards and Technology, US Department of Commerce.

Koh, D. 2020. The Geopolitics of Cybersecurity: Cooperation Among States Must Underpin Efforts to Create a Safer, More Secure, and Interoperable Cyberspace. *The Diplomat*. 9 December. https://thediplomat.com/2020/12/the-geopolitics-of-cybersecurity/.

Liu, H. W. 2017. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. *Journal of World Trade.* 51 (2). pp. 309–334.

———. 2019. Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism. In P. L. Hsieh and B. Mercurio, eds. *ASEAN Law in the New Regional Economic Order: Global Trends and Shifting Paradigms*. Cambridge, UK: Cambridge University Press.

McGuire, M., and S. Dowling. 2013. Cybercrime: A Review of the Evidence. *Research Report*. 75. October. London: United Kingdom Home Office.

Meltzer, J. P. and C. F. Kerry. 2019. *Cybersecurity and Digital Trade: Getting it Right*. Washington, DC: The Brookings Institution.

Microsoft. 2016. Platinum: Targeted Attacks in South and Southeast Asia. *Microsoft Security Intelligence Report*. 20. Redmond, WA.

Mitchell, A. D., and J. Hepburn. 2017. Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. *Yale Journal of Law and Technology*. 19. pp. 182–237.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2018. *APEC Cyber Security Strategy*. https://ccdcoe.org/uploads/2018/10/APEC-020823-CyberSecurityStrategy.pdf.

Organisation for Economic Co-operation and Development (OECD). 2015. *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris: OECD Publishing.

Selby, J. 2017. Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? *International Journal of Law and Information Technology*. 25 (3). pp. 213–232.

Smith, R., P. Grabosky, and G. Urbas. 2001. *Cyber Criminals on Trial*. Cambridge, UK: Cambridge University Press.

Thomas, J. 2019. Ransomware Could Cripple ASEAN. *The ASEAN Post*. 10 September. https://theaseanpost.com/article/ransomware-could-cripple-asean.

Tidy, J. 2022. Security Warning After Sale of Stolen Chinese Data. *BBC*. 9 July. https://www.bbc.com/news/technology-62097594.

Voon, T. 2019. The Security Exception in WTO Law: Entering a New Era. *AJIL Unbound.* 113. pp. 45–50.

Wall, D. S. 2007. *Cybercrime: The Transformation of Crime in the information Age*. Cambridge, UK: Polity Press.

World Trade Organization (WTO). 2020. *Negotiations on e-Commerce Continue, Eyeing a Consolidated Text by the End of the Year*. 23 October. https://www.wto.org/english/news_e/news20_e/ecom_26oct20_e.htm.

Xiao, B. 2022. Private Information of More Than 100 Australians Exposed Amid Huge China Police Data Leak. *ABC*. 8 July. https://www.abc.net.au/news/2022-07-08/australian-citizens-exposed-in-shanghai-police-data-leak/101214904.