BUILDING BLOCKS OF DIGITAL TRADE REGULATION SERIES
No. 2

# Cybersecurity and International Trade

## Understanding the policy landscape

IISD REPORT

Neha Mishra

IISD
International Institute for Sustainable Development



August 2025

## International Institute for Sustainable Development

The International Institute for Sustainable Development (IISD) is an award-winning, independent think tank working to accelerate solutions for a stable climate, sustainable resource management, and fair economies. Our work inspires better decisions and sparks meaningful action to help people and the planet thrive. We shine a light on what can be achieved when governments, businesses, non-profits, and communities come together. IISD's staff of more than 200 people come from across the globe and from many disciplines. With offices in Winnipeg, Geneva, Ottawa, and Toronto, our work affects lives in more than 100 countries.

IISD is a registered charitable organization in Canada and has 501(c)(3) status in the United States. IISD receives core operating support from the Province of Manitoba and project funding from governments inside and outside Canada, United Nations agencies, foundations, the private sector, and individuals.

**Head Office**

111 Lombard Avenue, Suite 325
Winnipeg, Manitoba
Canada R3B 0T4

**Tel:** +1 (204) 958-7700
**Website:** iisd.org
**𝕏:** @IISD_news

**Cybersecurity and International Trade: Understanding the policy landscape**

August 2025

Written by Neha Mishra, Assistant Professor, Geneva Graduate Institute

Photo: iStock

### Acknowledgements

Alice Tipping, Director, Trade and Sustainable Development, International Institute for Sustainable Development (IISD); Rashmi Jose, Senior Policy Advisor, Trade and Sustainable Development, IISD; Laura Cyron, Economic Affairs Officer, Digital Economy Policy Research Section, UN Trade and Development; and Shin-yi Peng, Distinguished Professor of Law & Vice President for Global Affairs at National Tsing Hua University (NTHU), reviewed and provided valuable comments on the first draft of this note.

This report was produced with support from the Swedish International Development Cooperation Agency (SIDA).


# Table of Contents



## List of Tables



## List of Boxes

# 1.0 Introduction

Cybersecurity protection is a fundamental precondition for open and trusted digital and data flows in the modern, globally interconnected economy. The importance of cybersecurity is well demonstrated by the drastic growth in the global market size of the cybersecurity industry, which increased from USD 75 billion in 2015 (Cybersecurity Ventures, 2015) to USD 193.73 billion in 2024 (Fortune Business Insights, 2025). Traditionally, cybersecurity-related discussions were limited to technical experts in internet technical bodies and standard-setting organizations. However, over the last decade, the international community and states have engaged proactively and extensively in establishing norms, standards, and best practices for cybersecurity protection. The majority of international and regional organizations now have a policy mandate to address cybersecurity concerns (International Telecommunications Union [ITU], 2021; Organisation for Economic Co-operation and Development [OECD], 2022; United Nations Joint Inspection Unit, 2021; World Bank, 2019; World Trade Organization [WTO], 2023). In addition, several countries have started implementing domestic legal and policy frameworks on cybersecurity. Unsurprisingly, cybersecurity has emerged as a public good of transnational/global importance (Cai & Zhang, 2025; World Economic Forum [WEF], 2019, 2025).

With the rapid digitalization and datafication of the economy, the WTO's multilateral framework and various regional trade bodies are also becoming important sites for discussion and engagement on cybersecurity issues (Meltzer, 2020; Mishra, 2024; Peng, 2024; Whitsitt; 2023). Consequently, the interface between trade and cybersecurity has become both important and complicated. As the paper explains in detail, although cybersecurity is fundamental to enabling secure and trusted digital trade flows, certain restrictions in domestic cybersecurity laws and regulatory frameworks can pose barriers to digital trade. Therefore, the international trade community faces the imminent challenge of balancing policy priorities at different levels of cybersecurity governance and achieving meaningful cooperation on cybersecurity issues (United Nations Office on Drugs and Crime, n.d.). Furthermore, given the transnational nature of cybersecurity threats (Huang et al., 2021), the yawning digital divide between the developed and developing countries (United Nations General Assembly, 2023) poses an additional layer of challenge in devising robust global and domestic responses to cybersecurity challenges.

Before unpacking the complex relationship of trade and cybersecurity, the paper first outlines the evolution of cybersecurity as a concept—originally the technological security of computer systems, data, and networks, it now covers myriad aspects of economic, political, military, and even social security. This section outlines examples of cybersecurity-related measures in domestic cybersecurity laws and regulatory frameworks from across the world, including data localization, organizational and technical compliance requirements, regulatory compliance requirements, and standards and certification frameworks. It then evaluates how such domestic frameworks on cybersecurity impact digital trade and the trade-offs between protection and enabling digital trade flows.

The second part focuses on how international trade law addresses the trade–cybersecurity interface, both in the multilateral context of the WTO and in recent plurilateral trade

agreements (PTAs) and digital economy agreements (DEAs). This section explains that although WTO law does not contain any specific provisions on cybersecurity, its rules nonetheless apply when cybersecurity measures have a trade-restrictive impact. In scenarios where domestic frameworks on cybersecurity breach WTO law obligations, countries are likely to justify them under the general and security exceptions contained in WTO treaties. However, given the lack of a clear, binding international consensus on cybersecurity norms and standards, the assessment of domestic cybersecurity regulatory frameworks under WTO treaties leads to legal uncertainty and political sensitivity.

Outside of the WTO, electronic commerce/digital trade chapters in several PTAs and DEAs now contain tailored provisions on cybersecurity, although the majority of these provisions remain soft, aspirational, and shallow, focusing largely on voluntary international cooperation frameworks for cybersecurity governance and cyber-capacity building. Noticeably, existing rules contained in PTAs and DEAs remain silent on facilitating cyber capacity building and technical assistance in developing countries and least developed countries (LDCs). Another observable shift is the inclusion of lenient security exceptions in some recent PTAs (including in the electronic commerce or digital trade chapters), indicating that countries are placing high importance on protecting their policy space to address (cyber)security threats within their domestic borders.

Despite the incorporation of cybersecurity-specific rules in PTAs and DEAs, fundamental aspects of international cooperation, particularly robust mechanisms for providing technical assistance and capacity-building support to developing countries on cybersecurity issues, remain under-addressed. Given the integrated nature of the digital economy, it remains urgent and critical for trade policy-makers to factor in the critical role of cybersecurity in bridging the digital divide and enabling developing countries and LDCs to integrate meaningfully in the global supply chains. Given this important link between cybersecurity and digital development, the paper concludes by unpacking the development dimension of cybersecurity and presenting opportunities and challenges for developing countries in the global digital economy. It then explores potential pathways for addressing the development-related aspects of cybersecurity both in domestic and international legal and policy frameworks.

# 2.0 Contextualizing the Relationship Between Trade and Cybersecurity: Threats and regulatory responses

Before delving deeper into the relationship between trade and cybersecurity, this section elaborates on the changing concept of cybersecurity. It then explores various examples of regulatory responses to cybersecurity threats in domestic frameworks and their potential impacts on digital trade flows. The section concludes by outlining various trade-offs in the context of fostering cybersecurity at the domestic and transnational levels while also enabling digital innovation and data flows in the global economy.

## 2.1 Cyberthreats in the Global Digital Economy

In computing terms, cybersecurity has traditionally been described as the response to various threats and attacks to computational systems and networks. It is often encompassed under the "CIA triad": "preservation of the confidentiality, integrity and availability of digital information and its underlying infrastructure" (ITU, 2018). The ITU defines 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" (ITU, 2008). The European Union's (EU's) Cybersecurity Act defines cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats," encompassing both threats to computer systems/networks and human beings affected by such threats.[1]

Cybersecurity is often confused with cybercrime: while both terms refer to the security of systems, cybercrime specifically refers to the unauthorized interference or breach of computational systems and triggers the application of punitive measures embedded in criminal laws. In contrast, cybersecurity is the broader technical approach to addressing threats and errors in computational systems adopted by internet technical bodies and companies, and, increasingly, also facilitated and regulated by states in their domestic legal frameworks (Knodell et al., 2023). This paper adopts a broader definition of cybersecurity, encompassing technological approaches and measures necessary to preserve the confidentiality, integrity, and authenticity of computational systems, and distinguishes it from related aspects, such as cybercrime.

Cybersecurity threats (or cyberthreats) are on the rise and have become more sophisticated and dangerous in recent years (OECD, 2022). Between 2014 and 2023, disclosed cybersecurity incidents (or cyber incidents, as popularly termed) grew at an average annual rate of 21% worldwide. Developing countries accounted for 30% of these cyber incidents, with the fastest growth of cyber incidents occurring in fast-expanding digital markets in

[1] Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on ICT cybersecurity certification (EU Cybersecurity Act), art. 2(1).

Latin America and the Caribbean region (Vergara Cobos, 2024). Some of the well-known cyberthreats include malware, phishing, man-in-the-middle attacks, denial-of-service attacks, zero-day attacks, ransomware, password attacks, injection attacks, and exploiting vulnerabilities in the Internet of Things (IoT) (IBM Cloud Team, 2024). These threats are directed at a variety of targets, including defence systems, critical infrastructure, businesses, and public agencies, and can seek to steal intellectual property, create disruptions, or spread distrust.

Cyberthreats have a massive impact on the economy. In 2024, the total cost of cyberattacks was estimated to be USD 9.5 trillion, with an average cost of a breach being USD 4.62 million. The health care sector was hit the hardest, with an average loss of USD 10.93 million per incident (Keepnet Labs, 2024). Similarly, in 2023, 6.06 billion malware attacks were reported worldwide (Keepnet Labs, 2024). Several countries have also reported a massive rise in cyberattacks on critical infrastructure (Vicens, 2025). Unsurprisingly, the total loss from cyberattacks in 2025 is estimated at over USD 10.5 trillion (eSentire, 2025). In addition to monetary losses, these cyberattacks cause other disruptions, such as impacting the day-to-day operations of organizations and companies, loss of intellectual property, damage to brand reputation and public trust, and increased costs for cybersecurity measures and incident response (WEF & Accenture, 2025). Further, cyberattacks on critical infrastructure, such as transport systems, hospitals, water supply, and electricity grids, can endanger human security (Martilleni & Abaimov, 2022; Mundt & Baier, 2022).

With governments viewing cyberspace as a fifth domain of security and warfare, the responsible actors behind cyber incidents are no longer only criminal groups and hackers but also states or state-sponsored entities (Dunn Cavelty & Egloff, 2019; Medium, 2024). This has not only heightened geopolitical tensions—it has also raised difficult legal questions as to how to hold states responsible for their cyber-conduct (Delerue, 2020). Although the exact statistics are unknown (given the covert nature of cyber operations especially by state actors), the Council on Foreign Relations (2025) has reported at least 180 suspected state-sponsored cyber operations in the last 5 years, targeting government and diplomatic networks, military and defence facilities, energy grids, telecommunication networks, health facilities, transportation networks, and semiconductor manufacturers across the world.

Given the rapid increase in cyberthreats and the various ways in which both public and private sector organizations are affected, cybersecurity has morphed into a broader notion of security (Berson et al., 2014). For instance, many governments now consider cybersecurity a component of their national/political security, economic security, and even social security, and integrate these aspects into their domestic laws and regulations, as discussed further below (Ishikawa & Kryvoi, 2023). Consequently, governments adopt a range of domestic measures on the grounds of cybersecurity protection, including data localization, digital industrial policy measures such as local content requirements, stringent regulation of foreign investments in digital sectors, strict rules for the processing and encryption of data, mandatory certifications for digital products and services, and security authorizations for data transfers. The next sub-section discusses various examples of such measures and their impacts on digital trade flows.

## 2.2 Cybersecurity Measures and Their Impacts on Digital Trade

The last decade has seen the rapid adoption of cybersecurity-related laws, regulations, and policy frameworks across different countries.[2] Several aspects are common across these regulatory and policy frameworks, such as integrating a risk-based approach to cybersecurity (either in specific sectors or across the board); setting up a national coordinating agency for cybersecurity monitoring and enforcement; providing key organizational and technological baseline requirements to ensure robust compliance, quality assurance, and security of technical design and supply chains; imposing data localization or other restrictions on cross-border data transfers; incident reporting mechanisms; licensing, auditing, and testing requirements for digital products and services; and penalty/enforcement mechanisms (Burnham, 2024; Wolff, 2025).[3] Many laws contain higher baseline requirements to enable robust cybersecurity risk management for entities operating critical infrastructure within the country (OECD, 2019).

While several measures are common across cybersecurity laws, their implementation varies significantly: while some jurisdictions have opted for a market-oriented or multistakeholder approach, others have adopted a more state-centric one (Iskikawa & Kryvoi, 2023). In certain cases, the implementation of these measures poses barriers to trade flows, for instance, when the measures discriminate against foreign companies and digital technologies by imposing higher costs/compliance requirements. Huang et al. (2021) have mapped the spectrum of how cybersecurity measures impact trade flows: (i) no business impact, (ii) limited impact on businesses, (iii) pre-requirement for market access, (iv) market access limitation, (v) market prohibition, and ultimately, (vi) market decoupling. However, as discussed further below, such cybersecurity-related measures could also be related to critical public policy objectives, such as data protection and privacy and enabling data access for law enforcement authorities or other key regulators. Therefore, balancing cybersecurity protection and trade policy considerations entails a delicate and difficult balancing exercise between various policy objectives, and cybersecurity law must thus be contextualized within both the political and digital environments in each country.

Traditionally, trade policy-makers have distinguished between trade in goods and services. However, in the current world of cyber-physical systems, in which software is embedded in the majority of manufactured goods and thus part of an integrated ecosystem, the distinction between goods and services is often counterproductive and unrealistic (DeNardis & Raymond, 2017). Therefore, in most cybersecurity laws and regulations discussed below, the legal requirements apply to the relevant entities, regardless of whether they offer physical goods, virtual services, or both. Similarly, the impact of these cybersecurity-related measures can also be felt in both trade in digital goods and services.

To better analyze the trade-related impacts of cybersecurity frameworks across different countries, cybersecurity-related measures are grouped into five clusters: (1) data transfer

[2] See different databases, such as UN Conference on Trade and Development's (UNCTAD's) Global Cyberlaw Tracker and the UN Institute for Disarmament Research's Cyber Policy Portal.

[3] Penalties can range from civil fines to stringent criminal punishments in different laws and regulations.

restrictions and controls; (2) licensing, certifications, and standards; (3) bans on insecure digital technologies and services; (4) technical assistance and encryption; and (5) other technological and organizational requirements.

### 2.2.1 Data Transfer Restrictions and Controls

Several countries have adopted restrictions on data flows on the grounds of cybersecurity and data security by mandating local storage and processing of data in specific sectors, on a cross-sectoral basis, or by imposing stricter requirements for transferring data abroad, such as conducting extensive security assessments or obtaining explicit regulatory approvals. For example, operators of critical information infrastructure are required to store all personal and important data within China, and any transfers abroad of such data necessitate security assessments by the government.[4] Similarly, in Vietnam, the transfer of personal data requires an extensive impact assessment by the transferring entity and can be blocked by the government on the grounds of national security.[5] In Saudi Arabia, all cloud service providers are required to store any government data within the country.[6] Several countries have also imposed cross-border data transfer restrictions in sensitive sectors to protect sensitive data, such as health, biometric, and financial data (UNCTAD, 2023).

Certain countries have also adopted measures providing broad regulatory discretion to block data flows. For instance, in Bangladesh, the National Cybersecurity Agency is empowered to block a data flow, if it "creates threat to cybersecurity" or "if the any data-information published or propagated in digital or electronic media hampers the solidarity, financial activities, security, defence, religious values or public discipline of the country or any part thereof, or incites racial hostility and hatred."[7] The cybersecurity law in Thailand also gives the cybersecurity regulatory body the discretion to take down content deemed harmful to cybersecurity.[8]

The socio-economic and technological impacts of such data-restrictive measures are often unclear and must thus be examined from the perspective of both domestic and global economies. From a domestic perspective, data-restrictive measures can be important to achieve stronger governmental control over technology companies (especially foreign companies) and can facilitate clearer application of domestic laws to domestic data, thereby facilitating ready data access to regulators and law enforcement authorities (Selby, 2017; Serrano & Raina, 2020). Such measures can thus be seen as highly important for public security and especially safeguarding critical information and government infrastructure from foreign cyberthreats, especially those arising from jurisdictions where data security levels are

[4] Cybersecurity Law of the People's Republic of China [中华人民共和国网络安全法] (CSL), art. 37, 23–24; Cybersecurity law; Data Security Law of the People's Republic of China [数据安全法]. Promulgated June 10, 2021; effective September 1, 2021, art. 31. The definition of important data can also be difficult to interpret in practice as it can vary across sectors and free trade zones and is dependent on sub-central regulations, thus increasing legal uncertainty (USTR, 2025).

[5] Decree No. 13/2023/ND-CP on the Protection of Personal Data (Vietnam), art. 25.

[6] Cloud Computing Regulatory Framework (Version 3) (Saudi Arabia), Section 4.2.1.

[7] Cybersecurity Act 2023 (Bangladesh), Section 8.

[8] Cyber Security Act 2019 (Thailand), Section 64.

inadequate. They also prevent the transfer of data to insecure jurisdictions. At the same time, data-restrictive measures can stimulate the development of domestic data infrastructure and reduce dependence on foreign countries (Arora, 2021; Singh, 2018).

However, in certain scenarios, such domestic data facilities can be expensive and inefficient (and arguably even redundant). For instance, several studies have shown that data localization measures mandated by domestic laws can result in higher operational costs and make such markets unattractive for foreign investment, especially if the cost of building/running local data centres is higher than the expected returns from the domestic markets (Bauer et al., 2016; Chander & Lê, 2014; Van der Marel et al., 2014). Such higher costs particularly disadvantage smaller firms and render them less competitive in global markets (Giovane et al., 2023). Furthermore, enforcement of such data-restrictive measures necessitates the regulatory capacity to audit data centres and/or conduct the systematic review/authorization of data transfers (Chander et al., 2021; Giovane et al., 2023). Finally, imposing data localization requirements alongside expansive requirements for data access, especially through backdoor mechanisms (as discussed later), erodes digital trust for both users and private companies. In particular, data localization may be risky from a security/trust perspective as it concentrates data in specified data centres and thus facilitates targeted foreign surveillance of such facilities (Chander & Lê, 2014) and increases susceptibility to natural disasters and cybersecurity vulnerabilities, especially if domestic data infrastructure is not sufficiently robust (Giovane et al., 2023).

From a global digital economy perspective, data-restrictive requirements fragment global cloud/data infrastructure operations and negatively impact economies of scale due to the forced duplication of infrastructure. It could even prejudice the security of networks as a distributed global digital infrastructure is better suited for robust cybersecurity checks compared to regional/local operations (Giovane et al., 2023). Furthermore, restrictions on data flows fragment the framework for digital trade flows, increasing regulatory uncertainty and operational costs for companies operating across jurisdictions (Giovane et al., 2023). Moreover, inconsistent frameworks for data transfer across jurisdictions in data protection laws, for instance, lead to regulatory fragmentation, which is costly for all countries (Evenett & Fritz, 2022). Therefore, before imposing extensive data restrictions on the grounds of cybersecurity, a careful assessment is necessary to weigh the costs and benefits of such restrictions.

### 2.2.2 Licensing, Certifications, and Technical Standards

An important component of cybersecurity laws and frameworks is requirements on licensing cybersecurity products and services, certification mechanisms, and the imposition of specific technical standards. Licensing and certification mechanisms are important to ensure the security and quality of digital products and services, and provide certainty to vendors while also providing clearer mechanisms for accountability. Furthermore, as some scholars have argued, technical standards, particularly those developed by international standard-setting bodies such as the International Organization for Standardization (ISO), have played an instrumental role in facilitating trade flows (Delimatsis, 2015). Where countries adhere to recognized standards or accredited certification mechanisms consistent with international

best practices, it enables an easier route toward mutual recognition and contributes to trade flows (Shang et al., 2021; Taherdoost, 2022). For instance, if a digital product/service is tested and certified using an international standard such as ISO/IEC 27001 by a laboratory in one country, it can be accepted in all other countries following the same standard.

Several countries now impose stringent requirements for registration or licensing cybersecurity products, including India (Virtual Private Network services, cloud, data centres, and crypto-exchange services),[9] Cambodia (for all cybersecurity products),[10] Saudi Arabia (for all vendors of cybersecurity products or solutions),[11] Ghana (for specified cybersecurity services),[12] Indonesia (all cybersecurity services),[13] and Malaysia (all cybersecurity services).[14] The Cyber Resilience Act, which entered into force in the EU in 2024, contains a complex framework for certification of IoT products, including CE marking for high-risk products, wherein such certifications can only be done by laboratories based in the EU.[15] Indonesia has adopted a similar framework for IoT products requiring a compliance certificate from domestic laboratories for medium- and high-risk IoT products.[16] China has developed an extensive framework for the security review of any products (software or hardware) used by critical information infrastructure operators.[17] Further, in the EU, only those certification schemes authorized in the EU are automatically considered to conform with EU law; other non-EU schemes can only be used if they have been mutually recognized.[18] Certification and standard-setting for cybersecurity products are also strictly controlled in Turkish domestic law.[19]

Several governments view cybersecurity certification and standard-setting mechanisms as critical tools to control the development and adoption of secure digital technologies within their jurisdiction. Furthermore, domestic standard-setting capabilities, especially for artificial intelligence (AI) and future emerging technologies, are considered fundamental in winning technology wars among leading digital powers and remaining a global leader in shaping

[9] Government of India, Ministry of Electronics and Information Technology, & Indian Computer Emergency Response Team, Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet (Directive No. 20(3)/2022-CERT-In). https://cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

[10] Draft Law on Cybersecurity (Cambodia), Chapter 5.

[11] National Cybersecurity Authority (Saudi Arabia), Registration and Licensing, https://nca.gov.sa/en/registration-and-licensing/.

[12] Cybersecurity Act 2020 (Ghana), Section 49(1).

[13] Draft Cybersecurity & Resilience Law (RUU KKS) (Indonesia), art. DD (Licensing of Cybersecurity Service Providers).

[14] Cybersecurity Act 2024 (Malaysia), Section 27.

[15] Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), art. 30.

[16] RUKKS, art. XXI (PDED Assessment Regime).

[17] CSL, art. 35.

[18] EU Cybersecurity Act, art. 54-55.

[19] Cyber Security Law [Siber Güvenlik Kanunu] (Law No. 7545) (Turkey), art. 5.

the future of digital transformation (Oduro, 2025).[20] Nonetheless, imposing indigenous cybersecurity standards or complex certification mechanisms is not only technologically inefficient but can be extremely costly for both domestic companies and governments to develop and implement, and results in fragmentation in the global digital economy, thus also leading to political tensions, as discussed below.

Several countries have raised concerns regarding cybersecurity laws and regulations adopted, particularly by China and the EU. For instance, the United States has argued that the EU has sidelined inputs from non-EU companies in technical standard-setting discussions under the EU Cloud Services Scheme (United States Trade Representative [USTR], 2025). Similar concerns have also been raised regarding the functioning of the national standard-setting body (TC-260) in China (USTR, 2025). In China, all network operators must classify their systems into one of the five protection levels and implement the baseline controls accordingly.[21] Some reports suggest that the Chinese government has mandatorily imposed at least 300 indigenous cybersecurity standards (Sacks & Li, 2018). The cybersecurity authorities in Ghana,[22] Malaysia,[23] Indonesia,[24] and Thailand[25] also enjoy significant discretion to set cybersecurity controls and standards. In contrast, the National Institute of Standards and Technology's Cybersecurity Framework 2.0 of the United States is largely driven by a co-regulatory approach and does not mandate specific technical standards for any entities (Gallagher, 2013; Peng, 2018).

Wide variation thus exists as to how licensing, certification, and standards requirements are implemented in practice. Stringent requirements in domestic laws can lead to potential delays, duplicate costs for vendors, and, thus, ultimately adversely impact trade flows. For instance, strict testing in domestic laboratories can be a de facto import barrier, especially for small-sized vendors of cybersecurity products and services (it can also further entrench the market position of large technology providers) (USTR, 2025). Similarly, the imposition of domestic technical standards that do not follow global best practices, such as ISO or Institute of Electrical and Electronics Engineers standards, may be expensive to implement and may become de facto trade barriers (Mishra, 2024). Furthermore, governments themselves bear economic repercussions, for instance, if they must set up several domestic laboratories/conformity assessment bodies and oversee complicated licensing mechanisms. Moreover, while imposing mandatory technical standards on domestic regimes, failing to consult private companies and not referring to international standards is economically inefficient and reduces trust in and the security of the local digital ecosystem (Kamara, 2024).

[20] See also State Council Notice on the Issuance of the Next Generation Artificial Intelligence Development Plan, July 9, 2017 (China).

[21] CSL, art. 21; MLPS 2.0 (GB/T 22239-2019).

[22] Cybersecurity Act 2020 (Ghana), Section 59.

[23] Cybersecurity Act 2024 (Malaysia), Section 25.

[24] RUU KKS, art. YY (Security Standards for PDED & CII.

[25] Cyber Security Act 2019 (Thailand), Section 13(4), Section 44.

### 2.2.3 Bans on Insecure Digital Technologies and Services

Governments often invoke cybersecurity-related rationales to ban digital technologies that they consider insecure and prejudicial to their national security concerns. These are the bluntest trade-restrictive measures as they directly block market access for specific companies and digital technologies and services. Several examples are commonly discussed in this regard, such as India's ban on hundreds of Chinese digital apps and services (Sherman, 2023). The United States has banned federal procurement of various technologies from Chinese companies, such as Huawei, ZTE, Hikvision, and Dahua (BBC, 2022; FitzGerald, 2022). In 2020, the United States announced the Clean Network Initiative to build a coalition of "trusted" partners whose 5G networks, cloud services, apps, and submarine cables would be free of "untrusted" vendors (aimed primarily at Chinese technologies) (The Clean Network, 2021). Canadian law also allows the government to prohibit or remove specified network products or services for national security reasons.[26] The 2020 Export Control Law in China regulates technical information and other data originating from outside the country.[27] Finally, although there is no explicit ban, the Turkish cybersecurity law states that preference would be given to domestic cybersecurity products.[28] Several countries have also restricted foreign investments in data-driven sectors (Knight & Voon, 2020).

### 2.2.4 Technical Assistance and Encryption

To enable stronger controls over domestic data and digital infrastructure, countries have introduced various mechanisms to enable governments to access data via backdoor mechanisms (e.g., mandatory requirements to provide technical information or decrypted data) through specific requirements in domestic laws. Further, to control the domestic use of encrypted products, governments can impose specific requirements for the export and import of encryption technologies. While these measures are often aimed at auditing software for data security and facilitating data access for domestic regulators and law enforcement agencies, especially for national security and public order reasons, they can compromise data security and digital trust for users and force companies to develop risky and insecure products, deviating from global best practices.

Some examples of the above include Australia's Assistance and Access Act, which authorizes the government to issue "technical assistance notices" that can compel any company (as long as they have Australian users) to decrypt information or provide interception capabilities.[29] A similarly broad "technical assistance" mandate exists in the Bangladesh Cybersecurity Act,[30] India's Information Technology Act,[31] Ghana's Cybersecurity Act,[32] and Cambodia's

[26] Telecommunications Act, S.C. 1993, c. 38, s 8.

[27] Standing Committee of the National People's Congress. (2020, October 10). Export Control Law of the People's Republic of China [中华人民共和国出口管制法], art. 2.

[28] Cyber Security Law [Siber Güvenlik Kanunu] (Law No. 7545) (Turkey), art. 4(1)(d).

[29] Assistance and Access Act 2018 (Australia), 317ZH–317ZL.

[30] Cybersecurity Act 2023 (Bangladesh), art. 45.

[31] Information Technology Act 2000, No. 21 of 2000 (India), Section 69(1–4).

[32] Cybersecurity Act 2020 (Ghana), Section 76.

Draft Cybersecurity Law.[33] The Indonesian law specifically provides that the government can demand access to source code, system logs, or decryption keys for investigation or threat response without a judicial warrant.[34] Similarly, stringent requirements are contained in Chinese and Vietnamese cybersecurity laws.[35] In the United States, the Communications Assistance for Law Enforcement Act obliges telecom and Voice over Internet Protocol providers to design equipment for court-ordered intercepts.[36] Some countries also impose restrictions on the use of encrypted products, such as India[37] and Vietnam (a trade licence is necessary for encrypted products).[38]

### 2.2.5 Technological and Organizational Requirements

Finally, cybersecurity laws and regulations contain a variety of technical and organizational requirements to facilitate risk assessment and management and include several compliance requirements for stronger monitoring and enforcement, such as mandatory incident reporting,[39] appointment of local representatives,[40] and different risk classification mechanisms, especially in the context of critical infrastructure. Further, several countries are now introducing stringent regulations to ensure data security/cybersecurity in emerging AI technologies. For instance, the EU AI Act calls for the development of new benchmarks and methodologies for "achieving appropriate level of accuracy, robustness, and cybersecurity" in high-risk AI systems, especially to address AI-specific cyber vulnerabilities.[41] The above requirements do not typically restrict trade and arguably enhance digital security in the global digital economy. However, they can be trade-restrictive when administered in highly complex ways (e.g., if different states have divergent incident reporting requirements) or where the templates vary significantly across countries (e.g., instead of using a standardized international format, countries use a specific format for the Software Bill of Materials, providing an inventory of all software products found in a digital product/service).[42] Further, in some cases, such as the Cambodian draft cybersecurity law, the risk management

[33] Draft Law on Cybersecurity [Unpublished draft] (Cambodia) https://www.accessnow.org/wp-content/uploads/2023/10/Legal-Analysis-Cambodia-Cybersecurity-Draft-Law-Final-29-Sept.pdf, arts. 19, 21, & 22.

[34] RUU KKS, art. BB (Agency Powers).

[35] CSL, art. 28; Law on Cybersecurity [Law No. 24/2018/QH14] (Vietnam), art. 26

[36] Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002 (1994), Title I, Section 102.

[37] Information Technology Act 2000, No. 21 of 2000 (India), Section 84A.

[38] Law on Cyberinformation Security [Law No. 86/2015/QH13] (Vietnam), art. 31(1).

[39] See, e.g., Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), art. 20–21; Critical Resilience Act, art. 14; Cybersecurity Act 2020 (Ghana), s.39; CSL, art. 56; Law on Cybersecurity [Law No. 24/2018/QH14] (Vietnam), art. 41.

[40] Cyber Resilience Act. art. 18(1); Law on Regulation of Publications on the Internet and Combatting Crimes Committed by Such Publications [Law No. 5651] (Turkey), Additional Article 4 (as added 29 July 2020). Resmî Gazete, No. 26530.

[41] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), art. 15.

[42] For instance, SPDX (Software Package Data Exchange) and CycloneDX are standard formats for SBOM.

compliance requirements are vaguely drafted, which can deter market entry due to legal and business uncertainty.[43]

**Table 1.** Unpacking cybersecurity measures

| Aspect of cybersecurity | Key ideas | Typical measures |
|---|---|---|
| Technical | CIA Triad: preservation of the confidentiality, integrity, and availability of digital information and its underlying infrastructure | Technical and organizational measures; licensing, auditing, and testing requirements for digital products and services |
| Military/national security | Countering the weaponization of networks, reducing dependence on foreign networks and digital technologies, protecting critical information infrastructure, enabling law enforcement measures, averting cyber threats to domestic networks/devices/services | Data localization; ban on insecure digital technologies; regulatory checks on cross-border data flows; licensing, auditing, and testing requirements for digital products and services |
| Economic | Minimizing GDP losses and impacts on the digital economy from cyber incidents, digital industrial policy-making measures addressing data/digital colonialism, and winning the technical standards race | Data localization, mandatory imposition of indigenous technical standards, and local content requirements |
| Political, social, and cultural | Regulation of harmful content, data privacy and consumer protection objectives, regulatory supervision, and strategic autonomy | Technical assistance measures; various regulatory checks on cross-border data flows; licensing, auditing, and testing requirements for digital products and services |

Source: Authors.

## 2.3 Balancing Cybersecurity and Digital Trade Concerns

As cybersecurity laws become common, governments face difficult policy choices. Table 1 demonstrates the complex choices that governments must make while deciding the nature of cybersecurity measures. On the one hand, several of these cybersecurity measures are fundamental for addressing cyberthreats and building robust digital technologies. Some requirements, such as data localization and local content/procurement requirements, facilitate not only cybersecurity but also new avenues for the growth of domestic technology companies.

[43] Draft Law on Cybersecurity [Unpublished draft] (Cambodia) art. 6.

In critical infrastructure sectors, various technological and organizational measures are essential to address cyberthreats commensurate with the level of risk they pose to the domestic economy and society. Furthermore, risk management and quality assurance mechanisms contained in several cybersecurity laws and policy frameworks are important levers to ensure that private vendors are adopting and implementing robust cybersecurity mechanisms in their products and services.

On the other hand, cybersecurity measures can be divergent and even conflicting in practice, leading to regulatory and market fragmentation, increased business/transaction costs (especially unaffordable for smaller enterprises), inefficiencies and delays, and siloed data and digital infrastructure in which security risks are amplified. Highly restrictive measures on cybersecurity, such as stringent cybersecurity licensing mechanisms and the imposition of indigenous standards, also impede the widespread adoption of global trust-based frameworks on cybersecurity. Factoring in the transnational nature of cybersecurity risks, any roadblocks to international cybersecurity cooperation, technical interoperability of cybersecurity standards, and trust-building on cybersecurity are highly undesirable for the global digital economy.

# 3.0 Cybersecurity and International Trade Law: Existing and emerging rules

This section focuses on the rules contained in international trade agreements related to cybersecurity issues. First, we look at the WTO's pre-digital era treaties and then focus on relevant rules in recent PTAs and DEAs.

## 3.1 Addressing Cybersecurity Issues in the Multilateral WTO Framework

Given that the WTO predates the current era of digitalization, WTO treaties do not contain cybersecurity-specific disciplines. However, existing WTO rules are nonetheless relevant and applicable to cybersecurity measures. For instance, provisions in the General Agreement on Trade in Services (GATS)[44] are applicable to all cybersecurity measures affecting digital services, regardless of whether they are pure services or services embedded in goods. Similarly, the General Agreement on Tariffs and Trade (GATT)[45] is relevant for any cybersecurity measures applicable to digital goods and devices, including smart technologies. The Agreement on Technical Barriers to Trade, which deals with technical regulations and standards, applies to any cybersecurity measures that impact digital goods/devices. Similarly, certain aspects of the Agreement on Trade-Related Aspects of Intellectual Property Rights are relevant, for instance, where governments demand that foreign companies provide access to source code or algorithms (i.e., trade secrets of companies) to access domestic markets.

In practice, several cybersecurity measures (as discussed in the previous section) could violate provisions in WTO treaties. For instance, a ban on digital services and technologies on the grounds of cybersecurity, especially when targeted at specific adversary states, could violate fundamental principles of non-discrimination and market access contained in WTO treaties.[46] Similarly, data-restrictive measures, which are common in many domestic cybersecurity laws, violate principles of non-discrimination and market access as they can disadvantage foreign companies and may even force them to exit the market altogether (Mishra, 2024).

Another common tool in cybersecurity laws is the imposition of mandatory technical standards. Such mandated standards may deviate from internationally recognized standards and increase the compliance burden on foreign companies and/or benefit domestic companies (especially if domestic industry lobbies have developed such standards). Furthermore, complex mechanisms for licensing or certification, or the imposition of weak, indigenous technical standards, especially if implemented in an arbitrary or discriminatory manner, could violate obligations on non-discrimination and domestic regulation.[47] In certain scenarios, governments may violate obligations on transparency and domestic regulations if insufficient

[44] https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm

[45] https://www.worldtradelaw.net/document.php?id=uragreements/gatt.pdf&mode=download

[46] For example, it could violate GATS, art. II, art. XVI, art. XVII.

[47] For example, it could violate GATS art. VI, art. XVII.

information is provided regarding how cybersecurity licences or certifications are administered or granted in the domestic framework (Mishra, 2020). Market access barriers also arise where companies are required to disclose important technical information, such as source code or encryption keys, to regulators as a precondition for selling their products and services in the domestic market (Dorobantu et al., 2021).

The WTO legal framework provides its members with policy space to impose any cybersecurity-related measures, despite their trade-restrictive impacts, if those measures can be justified under the exceptions contained in WTO treaties. The two key exceptions are the general exceptions (which apply to a range of public policy objectives) and security exceptions (applicable where national security or essential security interests are involved). The general exception could apply to cybersecurity measures that are necessary, for instance, to protect public order or public morals or to achieve compliance with specific domestic laws, such as data security or data protection laws.[48] The necessity test under the general exception is complicated and, in practice, would require trade tribunals to weigh and balance several complex factors, such as the extent to which the measure contributes to cybersecurity protection, its impact on the market, and the availability of less trade-restrictive alternatives (Mishra, 2020). Furthermore, the exception requires that the WTO panels confirm that the measure is implemented in an even-handed manner and does not create disguised or arbitrary restrictions on trade.[49]

The security exception applies when a cybersecurity measure is necessary to protect "essential security interests."[50] While this exception provides more policy space to countries to assess their cybersecurity needs as compared to the general exception, it nonetheless requires parties to establish a causal link between the measure and the cybersecurity-related rationale (Peng, 2015). It further only applies in specific scenarios, such as situations of war or emergency in international relations, or where measures relate to military or nuclear facilities. Given the absence of international consensus on several aspects of cybersecurity protection, coupled with the political sensitivity of the underlying issues, the application of this exception to real-world scenarios is likely to be legally complex and politically challenging and would not provide sufficient legal or policy certainty to countries implementing domestic laws and regulations on cybersecurity (Mishra, 2020). Therefore, several experts argue that the current provisions in WTO law neither foster an environment for international cybersecurity cooperation nor provide a well-defined policy space for countries imposing cybersecurity measures in their domestic frameworks (Meltzer, 2019; Mishra, 2024).

The issue of cybersecurity has also been broached in the ongoing plurilateral discussions on electronic commerce at the WTO. The proposed provision contains best-endeavour language for parties to build their national capabilities for cyber incident response and collaborate with each other through timely information sharing and other best practices to identify and mitigate malicious intrusions, etc.[51] The provision also acknowledges the importance of risk-based approaches to cybersecurity and the need to develop standards in a consensus-based,

[48] See, e.g., GATT art. XX; GATS art. XIV.

[49] See, GATT art. XX chapeau; GATS art. XIV chapeau.

[50] See, e.g., GATS art. XIVbis; GATT art. XXI.

[51] Draft text of the WTO electronic commerce agreement [INF/ECOM/86], art. 23.

transparent, and open manner.[52] There are, however, no clear commitments referring to cyber capacity building or hard mechanisms for cooperation between national cyber incident response teams.

## 3.2 Emerging Cybersecurity Disciplines in PTAs and DEAs

Outside of the WTO, several PTAs have adopted provisions pertaining to cybersecurity. As per the latest version of the TAPED dataset (which has coded all relevant provisions on e-commerce in PTAs since 2000), 67 PTAs now contain provisions on cybersecurity, underpinning its importance for digital trade. Most of these provisions are soft and aspirational in nature.

Although the language varies slightly across these PTAs, cybersecurity provisions generally focus on some common elements: (i) a general soft requirement to cooperate on cybersecurity matters,[53] with some treaties setting up established mechanisms for dialogues and information exchange;[54] (ii) building capabilities of national cybersecurity incident response teams;[55] and (iii) strengthening collaborations to "identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks."[56] Some PTAs also contain a soft provision to foster the development of the workforce in the area of cybersecurity and promote initiatives for mutual recognition of qualifications.[57]

Recent PTAs explicitly recognize the importance of a risk-based approach to cybersecurity[58] and encourage private companies to use them, as well as consensus-based standards and risk management best practices.[59] Even though this provision is not binding, it can play a critical role in fostering flexibility and coherence in cybersecurity practices (Asia-Pacific Economic Cooperation, 2020). It is also becoming common in PTAs to include a provision facilitating cooperation between national computer emergency response teams across members of the treaty.[60] Some DEAs contain a specific provision for online safety and security, acknowledging the importance of a multistakeholder approach and the need for collaborative solutions to global cybersecurity problems.[61]

---

[52] Ibid.

[53] See, e.g., Regional Comprehensive Economic Partnership Agreement (RCEP), art. 12.13.

[54] European Union–United Kingdom Trade and Cooperation Agreement (EU-UK TCA), arts. 703, 704.

[55] See e.g., Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) art. 14.16; RCEP art. 12.13; Singapore Australia Digital Economy Agreement, art. 34; US-Japan Digital Trade Agreement, art. 19.

[56] See, e.g., CPTPP art. 14.16.

[57] Comprehensive Economic Partnership Agreement between the Government of the Republic of India and the Government of the United Arab Emirates, art. 9.19; SADEA, art. 34; Digital Economy Partnership Agreement (DEPA), art. 5.1.

[58] US-Japan DTA art. 19 (with US FTAs often stating explicitly that risk-based approaches is more effective than prescriptive regulation).

[59] Agreement between the United States of America, the United Mexican States, and Canada (USMCA), art. 19.15.2; Digital Trade Agreement between the European Union and the Republic of Singapore (EU-Singapore DTA), art. 22.3.

[60] EU-UK TCA, art. 705, 706, 707.

[61] Digital Partnership Agreement between the Government of the Republic of Korea and the Government of the Republic of Singapore, art. 14.22; DEPA, art. 53.

The EU–Singapore Digital Trade Agreement contains one of the most detailed provisions on standards, conformity assessment, and technical regulations in the context of the digital economy. It recognizes that for the digital economy to function seamlessly, certain factors are critical, such as harmonizing standards and conformity assessment procedures, international cooperation to develop global standards, and mutual recognition for conformity assessment procedures.[62] The provision also sets out a broader mandate for cooperation between the private sector and joint initiatives between the EU and Singapore, and the need to improve transparency and information exchange on different aspects of cybersecurity standard setting and conformity assessment.[63]

Although the above provision is framed in best-endeavour language, it provides a robust model for cooperation and alignment on critical aspects of cybersecurity within the framework of international trade law. Another example is the Singapore–UK Digital Economy Agreement, which contains specific commitments on establishing mutual recognition of a baseline security standard for IoT products.[64] The two countries have also signed a Memorandum of Understanding on cybersecurity, establishing more detailed mechanisms for cooperation on incident response, information exchange, and skills development.[65] The private sector, including companies operating critical infrastructure, plays a critical role in cybersecurity standard setting; therefore, their expertise is relevant to developing robust standards to defend against a wide range of cyberthreats (Ishikawa & Kryvoi, 2023). By building room for multistakeholder approaches, these treaties foster a more grounded approach to cybersecurity protection.

Another interesting approach has been adopted in the African Continental Free Trade Area Digital Trade Protocol, in which parties have agreed to take into account cybersecurity standards and guidelines in relevant regional and international instruments and set out a best-endeavour provision on a wide variety of areas, including technical assistance and capacity building in cybersecurity and engaging different stakeholders in society to foster cybersecurity.[66] To date, this is the only PTA containing detailed capacity-building and technical assistance provisions on cybersecurity.

Many PTAs incorporate the general and security exceptions contained in WTO treaties by reference in PTAs. However, the Electronic Commerce or Digital Trade Chapter in recent PTAs also contain an exception for legitimate public policy reasons applicable to provisions on cross-border data flows and data localization.[67] Given that cybersecurity laws and regulations often contain data-restrictive measures, this exception is particularly relevant, as it can be read more broadly to cover several cybersecurity-related policy objectives.

---

62 EU-Singapore DTA, art. 23.

63 Ibid.

64 Singapore–UK Digital Economy Agreement, art. 8.61-L.

65 See https://www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-cyber-security-cooperation.

66 Protocol on Digital Trade to the African Continental Free Trade Area, art. 25.

67 See, e.g., CPTPP, art. 14.13; RCEP, art. 12.15(3)(a).

Several recent PTAs contain specific language regarding security threats in relation to cyberspace and have expanded the scope of security exceptions to cover scenarios pertaining to cybersecurity. In the EU–Singapore Digital Trade Agreement, the treaty enumerates different legitimate public policy objectives related to cybersecurity that can be invoked for restricting cross-border data flows, such as the protection of public security, online safety, cybersecurity, and safe and trustworthy AI.[68] EU PTAs have also typically contained some language preserving the policy space of the parties to regulate cybersecurity.[69] Furthermore, recent PTAs have incorporated self-judging language in the exceptions related to essential security interests (Peng, 2023). For instance, in the Regional Comprehensive Economic Partnership Agreement, both the provisions that prohibit data localization and require countries to enable cross-border data flows contain an explicit exception that allows countries to impose any measures that they consider necessary for their essential security interests; the same cannot be disputed by other parties.[70] In practice, such exceptions would mean that treaty parties are free to impose any cybersecurity measures, including data-restrictive measures, if they think it is necessary to protect their national security interests; the same cannot be challenged before a trade tribunal, even if it is trade-restrictive in its impact.

The discussion above indicates that countries are addressing the absence of cybersecurity-specific rules in pre-digital era WTO treaties through new rules in PTAs and DEAs. Although the WTO plurilateral agreement on e-commerce is likely to contain a dedicated provision on cybersecurity, the most tailored rules on cybersecurity currently exist outside of the multilateral framework. Despite several advances in WTO treaties, including adopting a pragmatic multistakeholder approach in relevant aspects of standard setting and online safety, these treaties contain cybersecurity provisions that remain soft and aspirational, and can only be effective if sufficient political will exists between the parties to those treaties. Furthermore, as discussed in more detail below, international trade agreements have sidelined the development dimension of cybersecurity, thus creating a lacuna in the existing frameworks.

[68] EU-Singapore Digital Trade Agreement, art. 5, fn1.

[69] Agreement between the European Union and Japan for an Economic Partnership, art. 18.8.2; EU UK TCA, art. 340(3).

[70] RCEP, art. 12.14(2)(b); art. 12.15 (2)(b). See also RCEP, art. 17.13.

# 4.0 Cybersecurity, Digital Trade, and Development

## 4.1 Unpacking the Development Dimension of Cybersecurity

Cybersecurity is a transnational policy concern impacting both developed and developing countries. In a digitalized global economy driven by the Internet, digital supply chains are inextricably interconnected, with several suppliers and manufacturers providing components embedded in digital networks, products/devices, and services (Duca, 2019). In conducting cyberattacks, hackers target and exploit the weakest links in these complex information and communications technology (ICT) supply chains, regardless of where the vulnerabilities are located (Shoemaker & Wilson, 2013). In addition to entailing economic costs, cybersecurity vulnerabilities can also prejudice basic human rights, such as by breaching the privacy of individuals (Public Knowledge, 2014). Therefore, since the Internet is a platform for trade, addressing cybersecurity concerns and vulnerabilities worldwide through robust frameworks has several characteristics of a global public good (Taddeo, 2019).

Indicators such as ITU's Global Cybersecurity Index, which scores countries based on their levels of cybersecurity protection using factors such as domestic laws, capacity-building efforts, and the availability of domestic technical infrastructure, consistently record the weak performance of LDCs and several developing countries. For instance, of the 193 countries assessed in 2024 by the ITU, a majority of LDCs were concentrated in the lower tiers with weaker scores, indicating the lack of a strong cybersecurity environment in those jurisdictions (ITU, 2024). While some developing countries, such as India, Brazil, Uruguay, and China, have been placed in the upper tiers, a majority of developing countries are also placed in the lower tiers, indicating their weaker performance on cybersecurity (ITU, 2024). As discussed earlier, as global cybersecurity is ultimately susceptible to the weakest links in digital supply chains, the weak cybersecurity performance of LDCs and a large majority of developing countries is a shared global concern.

Additionally, dealing with the economic and social risks of cyberthreats is overwhelmingly difficult for the majority of governments in developing countries and LDCs due to their limited regulatory capacity and technical expertise. This is in addition to the absence of extensive legal and regulatory frameworks on cybersecurity and organizational structures to deal with cyber incidents in most LDCs and several developing countries (although ITU's 2024 report also indicates steady improvements in many developing countries). Even if developing countries adopt cybersecurity strategies, including developing the local workforce and technical capabilities, several gaps exist in practice (ITU, 2024; Vergara Cobos, 2024). Furthermore, collaborative measures on cybersecurity between government bodies and the private sector are still uncommon in most developing countries and LDCs (ITU, 2024). Without a robust cybersecurity environment, many developing countries are unlikely to develop market readiness to integrate into the global digital economy. Furthermore, in the absence of international consensus on fundamental norms, standards, or best practices on

cybersecurity, smaller developing countries might face pressure from the digital powers to adopt specific regulatory approaches to cybersecurity protection, regardless of their developmental needs (Aaronson & LeBlond, 2018).

The conflicting regulatory frameworks for cybersecurity lead to different forms of regulatory and technological fragmentation. The costs of such fragmentation are particularly harmful for developing countries and LDCs. First, these countries are unlikely to have sufficient regulatory capacity or resources to implement complex cybersecurity frameworks domestically without adequate international cooperation mechanisms. Second, while cybersecurity laws and strategies aimed at building domestic skills and infrastructure are important, they are likely to backfire when there is a genuine dearth of local talent/resources, and any home-grown digital solutions are unlikely to match globally competitive digital products and services. Third, small and medium-sized enterprises from developing countries are unlikely to have sufficient resources to navigate diverging cybersecurity regulatory requirements across countries, ultimately leading to further fragmentation in the digital economy and widening the digital divide between the developed and developing world.

## 4.2 Policy Recommendations to Respond to Trade, Cybersecurity, and Development Considerations: From the local to the global

To better address the development implications of cybersecurity, particularly in the context of digital trade, several tailored approaches are necessary at both the national and international levels. Box 1 provides an overview of the key recommendations, followed by a detailed explanation below.

### Box 1. Overview of policy recommendations

#### Domestic Level

1. Use an evidence-based approach to develop and implement context-based domestic regulatory frameworks on cybersecurity.
2. Make cybersecurity an integral part of the domestic digital innovation strategy.
3. Build domestic talent, infrastructure, and capacities in cybersecurity protection, including regional hubs and the adoption of internationally recognized certification mechanisms.

#### International Level

1. Build a robust framework for technical assistance and capacity-building measures in FTAs, WTO treaties, and other relevant instruments.
2. Recognize multistakeholder/private/transnational cybersecurity standards in WTO law.
3. Develop mutual recognition agreements between trading partners for conformity assessment measures in relation to cybersecurity.

4. Develop clear exceptions in FTAs and WTO treaties to address cybersecurity-related measures.
5. Boost international cybersecurity cooperation in different relevant forums on critical aspects, such as cyber capacity building.

As detailed below, the following actions are important at the domestic level:

### 4.2.1 Developing Context-Specific Domestic Regulatory Frameworks

Currently, the majority of developing countries and LDCs are in the process of developing domestic legal and regulatory frameworks on cybersecurity. In building these frameworks, these countries must necessarily adopt an evidence-based approach that considers their current and future regulatory needs, the availability of technical expertise, funding and the capacity of responsible regulatory agencies, the size and structure of domestic digital markets, and the availability of local talent and resources. Adopting burdensome frameworks on cybersecurity, such as complicated data transfer authorization mechanisms or licensing processes, may not only be onerous and unrealistic but also deter foreign companies from entering these markets.

Furthermore, it is worthwhile to assess the extent to which trade-restrictive elements in domestic cybersecurity laws are helpful in fostering the domestic digital industry. As discussed earlier, in many instances, adopting international best practices (e.g., on classifying digital security risks using well-recognized global cybersecurity certification mechanisms) or international standards (e.g., ISO standards) enables the domestic digital sector more than developing local standards or licensing regimes for cybersecurity products and services. In that regard, cybersecurity must be treated as an integral part of the digital innovation and integration strategy of the country, instead of an isolated area of policy and legal action (Leibetreau, 2023).

### 4.2.2 Building Domestic Talent, Cyber Capacity, and Public–Private Partnerships

The second important lever for national policy action is building domestic talent, infrastructure, and capacities in cybersecurity protection. In practice, addressing these factors necessitates a multifaceted and experimental approach, given the pragmatic constraints faced by most developing countries and LDCs. For instance, to nurture domestic capabilities and collaborations, pilot projects and collaborations that bring together local start-ups and foreign technology companies can be encouraged. Similarly, public–private partnerships on cybersecurity might be important for governments to overcome their funding and regulatory capacity gaps.

Developing countries can also collaborate with recognized accreditation bodies (such as security certification laboratories) to build domestic capabilities. For the large majority of

developing countries, regional hubs (e.g., a regional testing centre in Africa or Latin America) will operate better than building expensive domestic facilities in each country. Developing countries could also push to join frameworks such as the Common Criteria Recognition Agreement, an agreement that promotes the Common Criteria Certificate for ICT products. Once a laboratory issues such a certificate for a digital product, the same certificate is valid in all countries that are members of the agreement. Such solutions enable more interoperability and scalability of security standards across countries (Asia-Pacific Economic Cooperation, 2020).

At the international level, particularly from the perspective of international trade agreements, several actions as discussed below, may further strengthen cybersecurity protection in the developing world:

### 4.2.3 Developing Tailored Cybersecurity Mechanisms in Digital Trade Agreements

International trade agreements have so far not addressed the development implications of cybersecurity. First, robust mechanisms for technical assistance and capacity building are necessary to enable developing countries to build their cyber capabilities. Such mechanisms are no longer simply moral obligations for developed countries, but a necessity to build a global framework for cybersecurity. Second, for developing countries and LDCs to engage in liberalized frameworks for cross-border data flows and commit to obligations on developing national cyber capacity, this support can become a part of the reciprocal bargaining process, leading to more equitable and realistic outcomes in the long run. Third, developing countries should push for more extensive disciplines in trade agreements to support digital small and medium-sized enterprises, including through dedicated information exchange programs and the provision of contact points.

Trade bodies such as the WTO can play an important role in fostering transparency on cybersecurity measures by enforcing provisions regarding the transparency of domestic regulations. Furthermore, given that cybersecurity measures are often discussed in WTO committees and other trade forums, a new work program aims to map cybersecurity measures to provide more clarity regarding the digital trade repercussions of such measures.

Several aspects of standard setting, particularly in the context of trade in services, remain unclear at the WTO. For instance, although cybersecurity standard setting is now commonplace in many private bodies, no clear criteria exist under the GATS to consider the legal relevance of multistakeholder and private cybersecurity standards. Most FTAs and DEAs, as discussed earlier, are also largely silent on this matter. To develop a global framework for digital standards, future digital trade rules (especially for trade in services) can incorporate a provision on the recognition of technical standards that are open, secure, representative of developing country interests, efficient, and affordable for the developing world.

Finally, another untapped potential under international trade law is the negotiation of mutual recognition agreements (MRA), agreements signed by countries that accept each other's conformity assessment measures as being equivalent to their own. Currently, most MRA

discussions related to cybersecurity are limited to some leading digital powers.[71] However, MRAs can be explored on a wider scale in different regional hubs in Africa, Asia, and Latin America, as well as by using the Common Criteria Recognition Agreement. Both WTO law and several PTAs already contain mechanisms to allow countries to discuss MRAs. In the future, developing countries must utilize such mechanisms to reduce various trading costs in the global digital economy.

In the context of various ongoing debates related to the trade-restrictiveness of cybersecurity measures at the WTO and other trade bodies, we have already seen a shift toward more flexible and cyber-specific exceptions in recent PTAs and DEAs. Clarifying the scope of security and general exceptions, and their applicability to the cyber context, is critical to provide policy space for the developing world. Furthermore, at least for LDCs, a moratorium can be implemented to avoid such disputes for the next several years to provide them more time to develop their regulatory frameworks and digital infrastructure. Alternate mechanisms to address cybersecurity-related trade disputes can also be considered, such as political solutions for security-related disputes (Lester & Zhu, 2019), compensatory mechanisms (Voon & Burri, 2023), or allowing specific waivers for critical infrastructure protection (Gagliani, 2020).

### 4.2.4 Strengthening Global Mechanisms for Cybersecurity Cooperation and Capacity Building

The second lever at the international level is developing a clear and comprehensive agenda for cybersecurity cooperation and identifying the right institutional frameworks to implement it. Cyber capacity building initiatives are popularly discussed in the international community, for instance by the Open-Ended Working Group of the UN (Hakmeh et al., 2024) but have been implemented sporadically by different international organizations. Experts have demonstrated that cyber capacity-building capabilities are primarily determined by the domestic cyber capabilities of a country rather than in response to external cyber threats (Calderaro & Craig, 2020). Thus, providing support to developing countries is fundamental to enabling them to strengthen their cyber capabilities.

Several programs by leading international organizations and initiatives, including those of the G7 and China's Digital Silk Road program, are dedicated to building cyber capabilities in the developing world. For instance, the World Bank has been implementing a Global Cyber Security Capacity Program for a decade (World Bank, 2025). The role of the Forum of Incident Response and Security Teams, a global forum of incident response and security teams, could be strengthened further to enable the better exchange of intelligence on cyber threats and best practices for cyber defence (Nye, 2014). Multistakeholder initiatives, such as the Paris Call for Trust and Security in Cyberspace, launched in November 2018, also facilitate cooperation on cybersecurity (Ciglič, 2023; Laudrain, 2018). The G7 group of countries has established flagship programs for cybersecurity capacity building, including training programs for officials and local experts in developing countries and programs to

[71] See, e.g., https://digital-strategy.ec.europa.eu/en/news/eu-and-united-states-enhance-cooperation-cybersecurity.

facilitate private investments in many developing countries.[72] Similar initiatives have been promoted by the Chinese government under the Digital Silk Road initiative, although there are some concerns, especially among Western countries, that such programs may be used to embed Chinese cyber sovereignty values in LDCs and developing countries (Wang, 2024).[73]

The above capacity-building initiatives, funded by leading digital powers, offer both challenges and prospects for developing countries. On the one hand, leading digital powers have a stronger interest and incentive to invest in cybersecurity capacity building in developing countries, as they have become the fastest-growing digital markets. On the other hand, developing countries inevitably face challenges navigating the pressures of adopting a specific model of digital and data governance that is aligned with that of the digital power offering the funding and capacity-building support. As noted earlier, developing countries must carefully assess and develop their cybersecurity regulatory frameworks and infrastructure so they are consistent with their strategic socio-economic and political needs. In that regard, they must also make judicious policy choices in accepting funding and other forms of capacity building from different international and regional bodies.

Technical assistance and capacity-building programs implemented under the framework of the WTO and other international organizations, such as UNCTAD, must not only focus on providing support to domestic regulators in LDCs and developing countries to build their domestic cyber capabilities but also provide training to their trade negotiators to deal with critical aspects of cybersecurity in future digital trade rulemaking. Further, as discussed previously, the soft law framework provided under FTAs and DEAs on various aspects of cybersecurity cooperation can develop into informal arrangements between trading partners to collectively deal with cybersecurity capacity-building challenges. As an example, certain countries that have signed DEAs have already developed Memoranda of Understanding on cybersecurity cooperation.[74] Especially in regional FTAs, such as the African Continental Free Trade Area Digital Trade Protocol, such informal understandings can be crucial in boosting strong regional cooperation on cybersecurity-related issues. Thus, a multi-pronged approach is necessary for international cybersecurity cooperation, which in turn would require stronger coordination between international, regional, and multistakeholder bodies.

[72] See, e.g., https://www.jica.go.jp/english/information/topics/2023/20230518_21.html; https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/06/13/fact-sheet-partnership-for-global-infrastructure-and-investment-at-the-g7-summit-2/.

[73] See, e.g., https://english.news.cn/20241220/022aa76882b044c8a58528412195ddd7/c.html

[74] See, e.g., https://www.csa.gov.sg/news-events/press-releases/singapore-renews-mou-on-cybersecurity-cooperation-with-australia.

# References


Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law, 21*(2), 245–272. https://doi.org/10.1093/jiel/jgy019

Arora, K. (2021, June 16). *India as archetype: What emerging data powerhouses need effective information sharing.* Heinrich Böll Stiftung North America. https://us.boell.org/en/2021/06/16/india-archetype-what-emerging-data-powerhouses-need-effective-information-sharing

Asia-Pacific Economic Cooperation. (2020). *Standards and process-based approach to enhancing cybersecurity* (Report). Committee on Trade and Investment, Sub-Committee on Standards and Conformance. https://www.apec.org/docs/default-source/publications/2020/7/standards-and-process-based-approach-to-enhancing-cybersecurity/220_scsc_standards-and-process-based-approach-to-enhancing-cybersecurity.pdf

Bauer, M., Ferracane, M. F., & van der Marel, E. (2016). *Tracing the economic impact of regulations on the free flow of data and data localization* (Global Commission on Internet Governance Paper Series No. 30). Centre for International Governance Innovation & Chatham House. https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization/

BBC News. (2022, November 26). *US bans sale of Huawei, ZTE tech amid security fears.* https://www.bbc.com/news/world-us-canada-63764450

Berson T., Clark, D., & Lin, H. S. (Eds.). (2014). *At the nexus of cybersecurity and public policy: Some basic concepts and issues.* National Academic Press. https://www.govinfo.gov/content/pkg/CHRG-114hhrg95373/pdf/CHRG-114hhrg95373.pdf

Burnham, K. (2024, September 17). *5 new cybersecurity regulations businesses should know about.* MIT Sloan Ideas Made to Matter. https://mitsloan.mit.edu/ideas-made-to-matter/5-new-cybersecurity-regulations-businesses-should-know-about

Cai, C. & Zhang, R. (2025). Fragmentation of global cybersecurity governance: Quasi-public goods and multi-level conflicts. *Global Political Economy, 4*(1), 32–50. https://doi.org/10.1332/26352257Y2024D000000016

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly, 41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). *Achieving privacy: Costs of compliance and enforcement of data protection regulation* (Policy Research Working Paper No. 9594). World Bank. https://documents1.worldbank.org/curated/en/890791616529630648/pdf/Achieving-Privacy-Costs-of-Compliance-and-Enforcement-of-Data-Protection-Regulation.pdf

Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal, 64*(3), 677–739. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

Ciglič, K. (2023). *Reflecting on five years of the Paris Call for Trust and Security in Cyberspace*. LinkedIn. https://www.linkedin.com/pulse/reflecting-five-years-paris-call-trust-security-kaja-ciglic-g2kuf

Council on Foreign Relations. (2025). Cyber operations tracker. https://www.cfr.org/cyber-operations/

Cybersecurity Ventures. (2015). *Cybersecurity market report, Q4 2015*. https://cybersecurityventures.com/cybersecurity-market-report-q4-2015/#:~:text=The%20worldwide%20cybersecurity%20market%20is,to%20%24170%20billion%20by%202020

Delerue, F. (2021). *Cyber operations and international law*. Cambridge University Press.

Delimatsis, P. (2015). Introduction: Continuity and change in international standardisation. In P. Delimatsis (Ed.), *The law, economics and politics of international standardisation* (pp. 1–16). Cambridge University Press. https://doi.org/10.1017/CBO9781316423240.001

DeNardis, L., & Raymond, M. (2017). The Internet of Things as a global policy frontier. *UC Davis Law Review, 51*(2). https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/51-2_DeNardis_Raymond.pdf

Dorobantu, C., Ostman, F., & Hitrova, C. (2021). Source code disclosure: A primer for trade negotiators. In I. Borchert & L. A. Winters (Eds.), *Addressing impediments to digital trade* (pp. 105–140). CEPR Press

Duca, S. (2019, June 13). *Supply chain, the weakest link in cybersecurity* [Video]. EC-Council. YouTube. https://www.youtube.com/watch?v=s7SryAK3-C0

Dunn Cavelty, M., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review, 15*(1), 37–57. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf

eSentire. (2024). *Cybersecurity Ventures report on cybercrime*. https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime

Evenett, S., & Fritz, J. (2022). *Emergent digital fragmentation: The perils of unilateralism*. https://www.hinrichfoundation.com/research/wp/digital/emergent-digital-fragmentation-the-perils-of-unilateralism/

FitzGerald, D. (2022, November 25). U.S. expands bans of Chinese security cameras, network equipment: FCC move blocks Dahua, Hikvision and other Chinese manufacturers from selling new equipment. *The Wall Street Journal*. https://www.wsj.com/articles/u-s-expands-bans-of-chinese-security-cameras-network-equipment-11669407355

Fortune Business Insights. (2025). *Cybersecurity market analysis 2032*. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Gagliani, G. (2020). Cybersecurity, technological neutrality, and international trade law. *Journal of International Economic Law, 23*(3), 723–745. https://doi.org/10.1093/jiel/jgaa006

Gallagher, P. D. (2013). *Testimony of Patrick D. Gallagher, Ph.D.: The cybersecurity partnership between the private sector and our government: Protecting our national and economic security* [Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation and Committee on Homeland Security and Governmental Affairs]. U.S. Senate. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Gallagher-2013-03-07.pdf

Giovane, C., Ferencz, J., & López-Gonzalez, J. (2023). *The nature, evolution and potential implications of data localisation measures* (OECD Trade Policy Paper No. 278). OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/the-nature-evolution-and-potential-implications-of-data-localisation-measures_249df37e/179f718a-en.pdf

Hakmeh, J., Sawli, A., & Collett, R. (2024). *A principles-based approach to cyber capacity-building (CCB): Understanding and operationalizing the OEWG CCB principles.* Chatham House. https://www.chathamhouse.org/2024/06/principles-based-approach-cyber-capacity-building-ccb

Huang, K., Madnick, S., Choucri, N., & Zhang, F. (2021). A systematic framework to understand transnational governance for cybersecurity risks from digital trade. *Global Policy, 12*(5), 625–638. https://doi.org/10.1111/1758-5899.13014

IBM Cloud Team. (2024). *Types of cyberthreats.* IBM. https://www.ibm.com/think/topics/cyberthreats-types

International Telecommunications Union. (2008). *Overview of cybersecurity* (ITU-T Recommendation X.1205). https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items

International Telecommunications Union. (2018). *Explainer: Cybersecurity* (ITU Explainers). https://www.gp-digital.org/wp-content/uploads/2018/08/ITU_Explainers_cybersecurity.pdf

International Telecommunications Union. (2021). *Global cybersecurity index 2021* (D-STR-GCI.01-2021-PDF-E). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

International Telecommunications Union. (2024). *Global cybersecurity index 2024.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Ishikawa, T., & Kryvoi, Y. (2023). Introduction. In T. Ishikawa & Y. Kryvoi (Eds.), *Public and private governance of cybersecurity: Challenges and potential* (pp. 1–11). Cambridge University Press.

Kamara, I. (2024). European cybersecurity standardisation: A tale of two solitudes in view of Europe's cyber resilience. *Innovation: The European Journal of Social Science Research*, 1–20. https://doi.org/10.1080/13511610.2024.2349626

Keepnet Labs. (2024, September 11). *171 cyber security statistics: 2025's updated trends and data.* Keepnet Labs. https://keepnetlabs.com/blog/171-cyber-security-statistics-2024-s-updated-trends-and-data

Knight, L., & Voon, T. (2020). The evolution of national security at the interface between domestic and international investment law and policy: The role of China. *Journal of World Investment & Trade, 21*(1), 104–139. https://doi.org/10.1163/22119000-12340169

Knodel, M., Kumar, S., & Degezelle, W. (2023, January 20). *Mythbusting: Cybercrime versus cybersecurity* [Blog post]. TechPolicy.Press. https://techpolicy.press/mythbusting-cybercrime-versus-cybersecurity

Laudrain, A. P. B. (2018, December 4). *Avoiding a world war web: The Paris Call for trust and security in cyberspace.* Lawfare. https://www.lawfaremedia.org/article/avoiding-world-war-web-paris-call-trust-and-security-cyberspace

Liebetrau, T. (2024). Problematising EU cybersecurity: Exploring how the single market functions as a security practice. *Journal of Common Market Studies, 62*(3), 705–724. https://doi.org/10.1111/jcms.13523

Lester, S., & Zhu, H. (2019). A proposal for "rebalancing" to deal with "national security" trade restrictions. *Fordham International Law Journal, 42*(5), 1451–1474. https://ir.lawnet.fordham.edu/ilj/vol42/iss5/5

Martellini, M., & Abaimov, S. (2022). Physical security, cyber security, and critical infrastructure: An introduction. In A. J. Masys (Ed.), *Handbook of security science* (pp. 1133–1143). Springer.

Medium. (2024, January 16). Cybersecurity as the fifth domain of warfare: Navigating the digital battlefield [Blog post]. https://medium.com/@cyber-news/cybersecurity-as-the-fifth-domain-of-warfare-navigating-the-digital-battlefield-55686deef9f2

Meltzer, J. P. (2019). *Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rules.* Brookings Institution. https://www.brookings.edu/articles/cybersecurity-digital-trade-and-data-flows-re-thinking-role-for-international-trade-rules/

Mishra, N. (2019). Privacy, cybersecurity, and GATS Article XIV: A new frontier for trade and Internet regulation? *World Trade Review, 19*(3), 341–364. https://doi.org/10.1017/S1474745619000120

Mishra, N. (2024). *International trade law and global data governance.* Hart Publishing.

Mundt, M., & Baier, H. (2023). Mapping cyber-physical threats for critical infrastructures. In B. Hämmerli, U. Helmbrecht, W. Hommel, L. Kunczik, & S. Pickl (Eds.), *Critical information infrastructures security* (pp. 164–179). Springer.

Nye, J. S., Jr. (2014, May). *The regime complex for managing global cyber activities* (Global Commission on Internet Governance Paper Series No. 1). Centre for International Governance Innovation & Chatham House. https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities/

Oduro, S. (2025, June 16). Shaping AI standards to protect America's most vulnerable: Tech innovators. *TechPolicy.Press.* https://www.techpolicy.press/shaping-ai-standards-to-protect-americas-most-vulnerable-tech-innovators/

Organisation for Economic Co-operation and Development. (2019). *Good governance for critical infrastructure resilience* (OECD Reviews of Risk Management Policies). OECD Publishing. https://doi.org/10.1787/02f0e5a0-en

Organisation for Economic Co-operation and Development. (2022). *OECD policy framework on digital security.* https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf

Peng, S. (2015). Cybersecurity threats and the WTO national security exceptions. *Journal of International Economic Law, 18*(2), 449–478. https://doi.org/10.1093/jiel/jgv025

Peng, S. (2018). "Private" cybersecurity standards? Cyberspace governance, multistakeholderism, and the (ir)relevance of the TBT Regime. *Cornell International Law Journal, 51*(2), 445–469. https://scholarship.law.cornell.edu/cilj/vol51/iss2/4?utm_source=scholarship.law.cornell.edu%2Fcilj%2Fvol51%2Fiss2%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages

Peng, S. (2023). Digital economy and national security: Contextualizing cybersecurity-related exceptions. *AJIL Unbound, 117*, 122–127. https://doi.org/10.1017/aju.2023.18

Peng, S.Y. (2024). *International trade law in the era of datafication.* Cambridge University Press.

Public Knowledge. (2014). *Cybersecurity and human rights.* https://publicknowledge.org/cybersecurity-and-human-rights/

Sacks, S., & Li, M. (2018). *How Chinese cybersecurity standards impact doing business in China* (CSIS briefs). https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china

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), 213–232. https://doi.org/10.1093/ijlit/eax010

Serrano, H. S., & Raina, A. (2020). *Legal problems with data localisation requirements: The case of the Russian Federation* (KU Leuven Working Paper no 223). https://ghum.kuleuven.be/ggs/publications/working_papers/wp223-hernandez-raina.pdf

Shang, T., Zhang, J.Y., Dawson, J., & Klonoff, D. C. (2021). Benefits of conformity assessment for cybersecurity standards of diabetes devices and other medical devices. *Journal of Diabetes Science and Technology, 15*(4), 727–732. https://doi.org/10.1177/19322968211018186

Sherman, J. (2023, March 27). *The problem with India's app bans.* SouthAsiaSource. Atlantic Council. https://www.atlanticcouncil.org/blogs/southasiasource/the-problem-with-indias-app-bans/

Shoemaker, D., & Wilson, C. (2013). The weakest link: The ICT supply chain and information warfare. *Journal of Information Warfare, 12*(2), 10–18. https://www.jstor.org/stable/26486851

Singh, P. J. (2018). *Data localisation: A matter of rule of law and economic development.* IT for Change. https://itforchange.net/data-localisation

Taddeo, M. (2019). Is cybersecurity a public good? *Minds and Machines, 29*, 349–354. https://doi.org/10.1007/s11023-019-09507-5

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics, 11*(14), 2181. https://doi.org/10.3390/electronics11142181

The Clean Network. (2021). [Archived]. https://2017-2021.state.gov/the-clean-network/

United Nations Conference on Trade and Development. (2023). *G20 members' regulations of cross-border data flows.* https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf

United Nations General Assembly. (2023). *Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels: Report of the Secretary-General* (A/78/62–E/2023/49). https://docs.un.org/en/A/78/62

United Nations Joint Inspection Unit. (2021). *Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit* (JIU/REP/2021/3). United Nations. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

United Nations Office on Drugs and Crime. (n.d.). International cooperation on cybersecurity matters. In Module 8: Cybersecurity and Cybercrime Prevention Strategies, Policies and Programmes (UNDOC Teaching Module Series: Cybercrime). https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

United States Trade Representative. (2025). *2025 national trade estimate report on foreign trade barriers.* https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf

van der Marel, E., Lee-Makiyama, H., & Bauer, M. (2014). *The costs of data localisation: A friendly fire on economic recovery* (ECIPE Occasional Paper). European Centre for International Political Economy. https://ecipe.org/publications/dataloc/

Vergara Carbos. E. (2024). *Cybersecurity economics for emerging markets.* World Bank. https://openknowledge.worldbank.org/entities/publication/4ec1bf22-3658-4d69-b9d3-43122254bc66

Vicens, A. J. (2025, April 23). *Complaints about ransomware attacks on US infrastructure rise 9%, FBI says.* Reuters. https://www.reuters.com/world/us/complaints-about-ransomware-attacks-us-infrastructure-rise-9-fbi-says-2025-04-23/

Voon, T., & Burri, M. (2024). Security exceptions, including cybersecurity (University of Melbourne Legal Studies Research Paper No. 24, Paper No. 964). Forthcoming in C. L. Lim & J. P. Trachtman (Eds.), *Cambridge companion to world trade law* (2025). https://digitaltradelaw.ch/wp-content/uploads/2025/01/Burri-and-Voon_Security-Exceptions.pdf

Wang, Z. (2024, January 5). China's Digital Silk Road (DSR) in Southeast Asia: Progress and challenges. *ISEAS Perspective, 2024*(1). https://www.iseas.edu.sg/wp-content/uploads/2024/01/ISEAS_Perspective_2024_1.pdf

Whitsitt, E. (2023). International trade law and cybersecurity: Balancing market-oriented and domestic state regulation. In T. Ishikawa & Y. Kryvoi (Eds.), *Public and private governance of cybersecurity: Challenges and potential* (pp. 161–184). Cambridge University Press.

Wolff, J. (2024). *Harmonizing U.S. cybersecurity regulations: Opportunities & challenges* (SSRN Scholarly Paper No. 5044551). SSRN. https://doi.org/10.2139/ssrn.5044551

World Bank. (2019). *Global Cybersecurity Capacity Program: Lessons learned and recommendations towards strengthening the program.* https://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf

World Bank. (2025, January 29). *Enhancing cyber resilience in developing countries* [Results brief]. https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries.

World Economic Forum. (2019). *We must treat cybersecurity as a public good. Here's why.* https://www.weforum.org/stories/2019/08/we-must-treat-cybersecurity-like-public-good/

World Economic Forum. (2025). *The growing complexity of global cybersecurity: Moving from challenges to action.* https://www.weforum.org/stories/2025/01/growing-complexity-global-cybersecurity-from-challenges-action/

World Economic Forum & Accenture. (2025). *Global cybersecurity outlook 2025* [Report]. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

World Trade Organization. (2023). *Members discuss cybersecurity, intangible digital products, raise over 60 trade concerns.* https://www.wto.org/english/news_e/news23_e/tbt_23jun23_e.htm

Published by the International Institute for Sustainable Development

**Head Office**

111 Lombard Avenue, Suite 325
Winnipeg, Manitoba
Canada R3B 0T4

**Tel:** +1 (204) 958-7700
**Website:** www.iisd.org
**𝕏:** @IISD_news

IISD

iisd.org