2

Data Network as Critical Infrastructure

National Security and the Digital Economy

2.1 Introduction

Digital technologies have significantly transformed the way we live our lives. The workings of both the public and private sectors have become reliant on digital infrastructure that enables data flows. The rapid development of "smart cities," in conjunction with progress in the IoT and AI, has converted more and more social and economic activities into digital data, which has in turn produced new forms of vulnerabilities: the multiplication of cybersecurity risks. Cybersecurity threats, for which digital technology suppliers can build back doors into hardware or software, have become major concerns for policymakers in this datafied era.[1] Along with digitalization, platformization, and datafication, the probability of cyberattacks against critical infrastructure increases as well. Therefore, supply chains of critical industries become intrinsically linked to broader digital and national security policies.

More specifically, the global data network has generated vulnerabilities for states in terms of protecting national security. Cyber risks in the supply chains of critical industries are specifically perceived as threats to the integrity of a state's critical infrastructure. A cyberattack to a critical national infrastructure is far beyond a mere criminal offence that the nation's judicial organs can meaningfully address.[2] Rather, it is a matter

Parts of this chapter are derived from the author's previous work: Shin-yi Peng, "Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions" (2023) 117 AJIL Unbound 122.

[1] OECD, "Reviews of Risk Management Policies Good Governance for Critical Infrastructure Resilience" (2019) <www.oecd.org/gov/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm>, at 18–24.

[2] Cyberattacks had led to approximate global annual cybercrime costs of €5.5 trillion by 2021. See European Commission, "Proposal for a Regulation of the European Parliament

of national security that affects the foundation of a sovereign.[3] Due to the relatively low cost and wide availability of digital technologies, cyberattacks and cyber terrorists now represent key methods of warfare.[4] High-profile, hostile incidents over the years[5] and the recent war in Ukraine offer lessons to other countries about the importance of a cyber defense.[6] As the backbone infrastructural sector and an interactive central nervous system for the digital economy, 5G networks face acute challenges as a result of cyber espionage, surveillance, and other cybersecurity risks, creating an intertwined relationship between data networks, cybersecurity, and national security.

In terms of national regulations, the mobile telecommunications sector has long been subject to heavy regulations. Traditional command and control mechanisms have been in place, primarily because the sector involves spectrum allocation and other public interests. More recently, controversies surrounding vulnerabilities in 5G goods and services have become a common concern, which has in turn amplified the role of state oversight. National security is now the central theme in the global 5G crisis,[7] and it is becoming more and more acute given the increasing tensions between the US and China. Taking in the entire picture, the US–China trade war has been intensified due to, or partially under the pretext of, US national security concerns. It has become a general perception that China's leading role in the 5G standardization process and Huawei's potential dominance in the global 5G market increase security risks, which could be exploited for spying and industrial espionage.[8] Facing

and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation" (2022).

[3] Sean M. Condron, "Getting It Right: Protecting American Critical Infrastructure in Cyberspace" (2007) 20(2) Harvard Journal of Law & Technology 403, at 404–407.

[4] *Ibid.*, at 407–408.

[5] See, for example, "Cyberattack Disrupts UK's NHS 111 Emergency Line" (*Economic Times*, August 8, 2022).

[6] For example, Taiwan's Ministry of Digital Development announced efforts to secure satellite Internet backup and diversify its satellite Internet services to mitigate the risks of cyberattacks. See "Taiwan Has to Secure Satellite Internet" (*Taipei Times*, October 30, 2022).

[7] See generally Berna Akcali Gur, "Cybersecurity, European Digital Sovereignty and the 5G Rollout Crisis" (2022) 46 Computer Law & Security Review 1, at 1–8.

[8] *Ibid.*, at 14. Note that Huawei, Nokia, and Ericsson are the major global suppliers of 5G telecommunications equipment, including base stations and cell towers that create the wireless broadband network through which our data pass. The dependence on Huawei products has become the key source of the claimed cybersecurity concerns.

the potential threat of a "Cyber Pearl Harbor,"[9] states have resorted to domestic regulation to protect their cybersecurity interests, leveraging their regulatory power to address such concerns, especially in critical industries in which the integrity of critical infrastructure would be in peril if not properly guarded.[10]

At the same time, the interdependencies and interconnectedness of cyberspace cannot be fully understood without considering their transnational dimension.[11] Cyber risks do not stop at national borders. Critical infrastructure resilience should therefore be examined in the cross-border context. Recent initiatives, such as the EU–US Trade and Technology Council (TTC) and the Pillar of Supply Chain of the Indo-Pacific Economic Framework (IPEF), further demonstrate policy directions to promote supply chain security and strengthen the resilience of ICT ecosystems. With regard to transatlantic allies, the impact of Russia's invasion of Ukraine on Europe's supply chains presents an urgent need to "identify and address supply chain vulnerabilities."[12] Thus, the main agenda for TTC is to cooperate on trust and security issues in the areas of ICT goods and services – namely, to prevent political and economic disruption caused by the over-concentration of resources in key supply chains. If the US is able to replicate the TTC level of cooperation and momentum under the IPEF, the transpacific allies may move forward to establish criteria, jointly identify goods and services critical to their national security, and "increase resiliency and investment in critical sectors."[13] Evidently, strengthening international cooperation toward critical infrastructure resilience is a compelling policy option among geopolitical allies.

2.2 Critical Infrastructure as the Backbone of the Digital Economy

2.2.1 Critical Infrastructure and Cyber Resilience

The concept of "critical infrastructure" is constantly evolving. In order to reflect and respond to new challenges in network security, both the

[9] See generally Lawrence J. Trautman, "Is Cyberattack the Next Pearl Harbor?" (2016) 18 North Carolina Journal of Law & Technology 233, at 233–235.

[10] Akcali Gur, supra note 7, at 14.

[11] OECD, supra note 1, at 38–39.

[12] European Commission, "EU-US Joint Statement of the Trade and Technology Council" (2022) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_7516>.

[13] USTR, "Ministerial Statement for Pillar II of The Indo-Pacific Economic Framework For Prosperity, lndo-Pacific Economic Framework for Prosperity (IPEF)-Pillar II – Supply Chains" (2022) <https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef/trade-pillar>.

number and variety of critical infrastructure are rapidly increasing. Critical infrastructure is now a term commonly used to identify services of a sensitive nature that have the potential to "cause massive disruption to dependent systems/services if they are compromised or destroyed."[14] Public utilities and emergency services, among others,[15] are most frequently associated with the concept of critical infrastructure.[16] In this datafied age, however, critical infrastructure operates across both the physical and the digital world,[17] and as a result, cybersecurity threats may originate from both the hardware and software components. Indeed, critical infrastructure is "increasingly if not exclusively controlled by computers."[18] In other words, infrastructure systems have undergone a digital transformation, with consequences to cyber risks and vulnerabilities. Cyberattacks can damage critical infrastructure in various ways, including directly taking control of industrial processes to block the functioning of energy distribution or transport services.

The complex ecosystem of critical infrastructure therefore requires a holistic and convergent security approach that protects both physical security and cybersecurity. Taking the energy sector as an example, the development of a smart grid and other innovative services means that the sector is increasingly reliant on data flows. Thus, an aggregate level of safety is necessary to mitigate both physical and cyber risks to energy systems.[19] Ultimately, critical infrastructure resilience is multifaceted. The disruption of critical infrastructure – whether 5G networks, transportation systems, water or energy supplies, or emergency hospital services – can lead to significant harm to societies and cause cascading effects across sectors. The cross-sectoral, systematically interdependent

[14] The US Patriot Act defines critical infrastructure as: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Condron, supra note 3, at 404–407.

[15] For example, there are thirteen national infrastructure sectors in the UK, including "Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water." Several sectors have defined subsectors; Emergency Services, for example, can be split into "Police, Ambulance, Fire Services and Coast Guard." See UK's National Protective Security Authority, "Critical National Infrastructure" (2023) <www.cpni.gov.uk/critical-national-infrastructure-0>.

[16] Condron, supra note 3, at 404–407.

[17] See Section 6.4.1 for more discussions in this regard.

[18] Nigel Wilson, "Australia's National Broadband Network: A Cybersecure Critical Infrastructure?" (2014) 30 Computer Law & Security 699, at 702.

[19] OECD, supra note 1, at 18–24.

nature of critical infrastructure therefore calls for a comprehensive resilience strategy through which security risks are assessed in their entirety.[20]

Notably, some infrastructure assets are the key components of a wider, complex system. In this regard, the 5G broadband infrastructure has been considered one of the most critical utilities, which "if destroyed, degraded or rendered unavailable for an extended period, would adversely impact the social or economic well-being of the nation or affect a state's ability to ensure national security."[21] Ensuring the cyber resilience of the 5G broadband infrastructure and preventing it from being either a direct target or an indirect vehicle for cyber threats has become a prominent mission of the national security efforts of most countries. That being said, such an infrastructure is generally owned and operated by the private sector. As discussed in Chapter 1, telecommunications services have undergone privatization over the last several decades, and currently, government control over telecommunications infrastructure assets has, to a large extent, decreased. The need for cyber resilience, however, has resulted in escalating governmental intervention.[22] To tackle cross-border security challenges, governments have reviewed and strengthened their national security strategies and have adopted more far-reaching regulations, with the aim of fostering a secure and resilient ICT environment against cyberattacks.

2.2.2 *Trade-Restrictive Critical Infrastructure Security Measures*

The cyber arms race and digital tit-for-tat have intensified geopolitical frictions. The major geopolitical players in the digital economy have adopted increasingly comprehensive security measures at the national level. By stressing that the backbone of the digital economy must be trusted and reliable, the Biden administration has accelerated the implementation of a set of trade measures to diversify supply chains and thereby secure the infrastructural resilience of 5G networks.[23] In fact, under both Trump and Biden, 5G supply chain security has been at the center of the national security strategy of the US. At the data network

[20] *Ibid.*, at 38–39.
[21] Wilson supra note 18, at 702.
[22] OECD, supra note 1, at 42.
[23] The US White House, "National Security Strategy" (2022) <www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>, at 33–35.

level, following Trump's "Clean Network" and "Clean Path" initiatives,[24] the current FCC of the Biden administration, citing the same national security grounds, has continued to order US telecommunications companies to remove Huawei equipment from their networks.[25] At the digital platform level, although the Biden administration has withdrawn Trump's executive orders that banned transactions with eight Chinese software applications,[26] the current FCC proceeded to request that US digital platforms remove TikTok from their app stores.[27] Overall, the government has been actively engaged and has closely scrutinized transactions in the ICT sector. Among other measures, the Committee on Foreign Investment in the United States (CFIUS)[28] ordered ByteDance, a Chinese startup, to divest in TikTok due to national security concerns. Although that order was not enforced by the Biden administration, the CFIUS has continued to monitor whether TikTok's partnership with Oracle can sufficiently resolve national security issues.[29]

Across the Atlantic, recognizing that digital technologies are now a vulnerable target, protecting resilience against cybersecurity threats has been placed at the center of the EU's cybersecurity policies. The adoption of the "5G Toolbox of Risk-Mitigating Measures" (the "5G Toolbox"),[30]

[24] The US Department of State, "The Clean Network" (2021) <https://2017–2021.state.gov/the-clean-network/index.html>.

[25] David Shepardson, "U.S. FCC Set to Ban Approvals of New Huawei, ZTE Equipment" (*Reuters,* October 13, 2022) <available at www.reuters.com/technology/us-fcc-set-ban-all-us-sales-huawei-zte-equipment-axios-2022-10-13/>.

[26] The US White House, "Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries" (June 9, 2021) <www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/>.

[27] Brian Fung, "FCC Commissioner Calls on Apple and Google to Remove TikTok from Their App Stores" (*CNN*, June 29, 2022).

[28] CFIUS is an interagency committee tasked to "block or suspend proposed or pending foreign mergers, acquisitions, or takeovers of persons engaged in interstate commerce in the U.S. that threaten to impair the national security." Defense Production Act of 1950, 50 USC §4565 (2018). See Lizzie Knight and Tania Voon, "The Evolution of National Security at the Interface Between Domestic and International Investment Law and Policy: The Role of China" (2020) 21 Journal of World Investment and Trade 104, at 139.

[29] The US Congress, "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms" (March 23, 2023) <www.congress.gov/event/118th-congress/house-event/115519?s=1&r=18> (TikTok chief executive Shou Chew testified before the US Congressional Hearing explaining the platform's business practices and defending the company from charges that it poses national security threats).

[30] On January 29, 2020, the EU adopted Cybersecurity of 5G networks EU Toolbox of risk mitigating measures (the "5G Toolbox"). European Commission, "Cybersecurity of 5G

which delineates potential areas of risk and remedial measures connected with suppliers of 5G infrastructure, sought to achieve diversity among suppliers and reduce Chinese companies' (especially Huawei's) participation in the 5G rollout.[31] In practice, one important category in the 5G Toolbox is the risks connected with suppliers of 5G infrastructure. Among all possible strategic remedial measures, the 5G Toolbox underscores the importance of restricting or excluding "high risk suppliers" to ensure that dependencies on certain suppliers do not "negatively affect the security of networks and/or services."[32] Along this policy path, the proposed EU Cyber Resilience Act is expected to "bolster cybersecurity rules to ensure more secure hardware and software products."[33]

Other striking cases of trade-restrictive security measures surrounding 5G and its applications include the Australian government's ban on Huawei's participation in building the nation's broadband infrastructure and India's decision to block access to dozens of mobile applications originating in China, including WeChat.[34] It should also be noted that after joining the so-called Five Eyes intelligence-sharing network, which consists of the US, Canada, the UK, Australia, and New Zealand, Canada decided to ban Huawei/ZTE 5G equipment to protect its national security. Retroactively, Canadian telecommunications operators that already have this equipment installed are required to remove it by June 2024.[35]

At the same time, from "Great Firewall" to direct virtual private network (VPN) blocking,[36] VPN traffic is generally filtered in China to ensure compliance with its social stability and national security agendas.

Networks – EU Toolbox of Risk Mitigating Measures" (2020) <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

[31] *Ibid.*

[32] *Ibid.*

[33] European Commission, "Cyber Resilience Act" (September 15, 2022) <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>.

[34] WeChat is Tencent's flagship social media platform, providing messaging, online shopping, payments, and other digital services. The app's more than one billion users are based in China, and it is also used by millions of people, mainly Mandarin speakers, around the globe.

[35] Andy Blatchford, "Canada Joins Five Eyes in Ban on Huawei and ZTE" (*Politico,* May 19, 2022).

[36] The Great Firewall of China restricts users within the country from accessing certain websites. Virtual private networks (VPNs) are one of the most popular tools to bypass the firewall. For commentaries on the trade aspects of the Great Firewall, see Henry Gao, "E-commerce Joint Statement Initiative Negotiation and China" in Shin-yi Peng et al. (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge University Press, 2021), at 295, 316.

China's cybersecurity regime has become even more complex and strict since its Cybersecurity Law was implemented,[37] primarily due to its lack of tailored definitions and transparent guidance. The vague language and broad scope of China's Cybersecurity Law accord the government even wider latitude to facilitate its political and economic agendas.[38] The Chinese government has issued implementation measures for its cybersecurity law, including the "cybersecurity review," which imposes restrictions on foreign ICT goods and services based on "potential national security risks" related to the reliability of supply chains. Moreover, the Chinese Cryptography Law contains trade-restrictive requirements for encryption products that involve national security.[39] Under the Chinese regulatory framework, loosely defined "encryption products," which encompass a wide range of ICT goods and services, must mandatorily undergo a cybersecurity risk assessment.[40]

2.2.3 *The Inherent Clash with International Trade Rules*

Through a broader lens, security-related trade restrictions – regardless of whether or not they directly address critical infrastructure – have the potential to clash with international trade rules in many ways, at both the multilateral and regional levels. Country-specific bans on ICT goods and services may violate the most-favored-nation principle, given the fact that the competitors of other countries will be the beneficiaries of such restrictions.[41] Security measures may be inconsistent with national treatment obligations if the domestic ICT goods or services and the banned foreign goods or services are "like products" or "like services."[42] Moreover, non-discrimination provisions in the Electronic Commerce/Digital Trade Chapters of the FTAs also require the parties to ensure

[37] *Zhonghua Renmin Gongheguo Wanglao Anquan Fa* (China's Cybersecurity Law), effective June 1, 2017.

[38] USTR, "Report to Congress on China's WTO Compliance" (2021) <https://ustr.gov/sites/default/files/files/Press/Reports/2021USTR%20ReportCongressChinaWTO.pdf>, at 34.

[39] *Zhonghua Renmin Gongheguo Mima Fa* (China's Cryptography Law), effective January 1, 2020.

[40] USTR, supra note 38, at 35.

[41] Most-favored-nation (MFN), for example, GATT, Article I; GATS, Article II. Arguably, major competitors of Huawei from Europe (Nokia and Ericsson) and South Korea (Samsung) will be the beneficiaries of the Huawei ban in the US.

[42] The National Treatment (NT), for example, GATT, Article III; GATS, Article XVII.

non-discriminatory treatment of "like digital products."[43] In other words, a violation could be found by comparing domestic and foreign digital products. If they are "like" digital goods or services, the adverse treatment of foreign digital products may be considered discrimination. Furthermore, security measures can simultaneously constitute quantitative restrictions on international trade in goods and violate the obligations to eliminate such restrictions.[44] Similarly, when a state undertakes market access commitments in relevant services sectors, these measures may restrict ICT services and violate relevant market access obligations.[45] Additionally, security-related trade restrictions in the public procurement of network equipment may breach a state's market access schedules of commitment under the Government Procurement Agreement (GPA), which lists the procurement activities open to international competition.

In cases in which the security standards constitute "technical regulations" under the Technical Barriers to Trade Agreement (TBT Agreement), unique security standards that accord less favorable treatment to imported products than that accorded to like products of national origin may also breach non-discrimination obligations.[46] Given the technical characteristics of cybersecurity measures, the TBT Agreement has become the legal battleground for trade-restrictive security measures. To be more straightforward, China and the EU have been accusing each other of using mandatory cybersecurity standards to protect their own 5G equipment suppliers, namely, Huawei/ZTE and Ericsson/Nokia. On the one hand, China's paradigmatic approach to the use of technical standards in the ICT sector, which in many instances appears designed to favor China-specific approaches, has caused substantial worldwide concern within the industry. In particular, the EU has consistently claimed that the requirement of the Chinese ICT security certification regime "appears to extend well beyond what the EU would consider justified for national security protection, which was cited by China as the legitimate objective to be achieved."[47] The EU also

[43] Non-discrimination provisions in the Electronic Commerce/Digital Trade Chapters of the FTAs, see for example, CPTPP, Article 14.4; USMCA, Article 19.4.

[44] The obligations to eliminate quantitative restrictions, for example, GATT, Article XI.

[45] GATS, Article XVI. Note that China claimed that the US violated its market access commitments under the GATS when the Trump administration imposed restrictions on TikTok and WeChat. See Section 3.1 for more discussions.

[46] TBT Agreement, Article 2.1.

[47] Communication from the European Commission, "China's Transitional Review Mechanism" G/TBT/W/326 (October 29, 2009), para. 12.

repeatedly requested that China clarify the rationale for its cybersecurity measures and their relationship to national security. On the other hand, the EU 5G policy – notably, trade-related cybersecurity measures designed to decrease (over)dependence on non-EU goods and services – has been criticized by China for being inconsistent with the EU's dedication to open market principles. In particular, China has raised concerns about the measures adopted by Sweden, which aims to remove Huawei and ZTE from its 5G infrastructure by 2025 based on the EU 5G Toolbox.[48] The delegate for China in the WTO meetings also claimed that the Swedish decision violates the WTO rules of transparency and non-discrimination, that the assessment criteria in the 5G Toolbox have led to *de facto* discrimination, and that the favorable treatment of Ericsson is inconsistent with the TBT Agreement.[49] Similarly, at the same WTO meeting, China reiterated its "regret" that Chinese companies cannot participate in Australia's 5G network construction, and that their equipment in the existing 4G network has also been removed in Australia.[50] Interestingly, China asserted that "the issue of telecommunication network security should be addressed based on scientific verifiable facts and data, rather than the origin of suppliers."[51] China urged Australia to amend its 5G policy to bring its measures in line with WTO rules. In response to China's assertion, the Australian government stressed that its 5G policy is "country-agnostic, transparent, risk-based, non-discriminatory, and fully WTO-consistent."[52]

2.3 Contextualizing Security-Related Exceptions: Possible Reconciliation

Nonetheless, general and security exceptions provide a normative framework by which to balance free trade obligations against national policy interests. Thus, the key issues here relate to whether and how those

[48] *Ibid.* The delegate for China pointed out that the Swedish government established its 5G licensing requirements in October 2020, under which the 5G spectrum auction must not be carried out with base station equipment from the Chinese companies. In addition, the existing equipment of Huawei and ZTE, no matter the 4G or 5G system within Sweden, should be removed in the coming years. See also European Commission, supra note 30.

[49] WTO, "Minutes of the Meeting of the Council for Trade in Goods" G/C/M/139 (June 16, 2021), paras. 13.2–13.7.

[50] *Ibid.*

[51] *Ibid.*, paras. 40.3–40.5.

[52] *Ibid.*, para. 40.5.

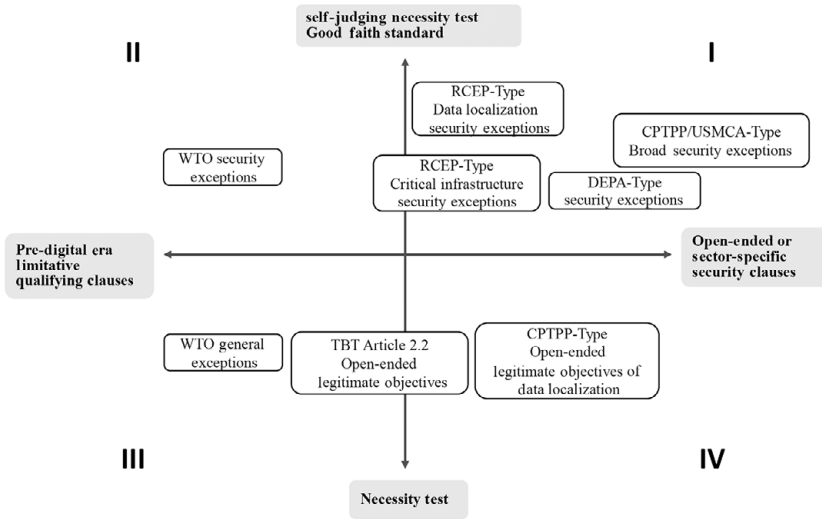

Figure 2.1 Contextualizing security-related exceptions

exceptions would protect a state's policy space through regulatory actions directed at national security matters. In this context, Figure 2.1 distinguishes between the types of exception clauses related to national security in international trade agreements. The vertical axis, with the "necessity test"[53] and "good faith standard" at each end,[54] represents the discretionary nature of the necessity element required by the exception. The horizontal axis, with "limitative qualifying clauses" and "expansive security clauses" at each end, represents the scope of situations allowed by the exception. This book argues that although on the face of it multiple exceptions may be available, complex technical and political-economic factors trigger their applicability. On the one hand, in the pre-digital age, "conventional" general exceptions (quadrant III)[55] and security

[53] Please refer to Section 1.4.3 for how the necessity test has been formulated by the Appellate Body in the context of WTO law.

[54] For discussions on good faith as a core principle of interpretation of the WTO Agreement, see, for example, Andrew D. Mitchell, *Legal Principles in WTO Disputes* (Cambridge University Press 2008), at 107–144; Isabelle Van Damme, *Treaty Interpretation by the WTO Appellate Body* (Oxford University Press, 2009), at 19–21; Marion Panizzon, *Good Faith in the Jurisprudence of the WTO: The Protection of Legitimate Expectations, Good Faith Interpretation and Fair Dispute Settlement* (Hart Publishing, 2006).

[55] The General Exceptions, for example, GATT, Article XX; GATS, Article XIV.

exceptions (quadrant II)[56] are too narrowly framed to address cybersecurity objectives. On the other hand, trends to create open-ended or digital sector-specific security exceptions (quadrant I) may also fall short for being excessively unrestrained if due process and good faith are not accorded. The four quadrants are respectively discussed below.

2.3.1 GATT-Type General Exceptions

2.3.1.1 GATT General Exceptions

The exception clauses in quadrants II & III were drafted in the brick-and-mortar age. Therefore, these "pre-digital era exceptions" are not properly formulated to address today's cyber threats. Taking GATS Article XIV General Exception (in quadrant III) as an example, although none of the grounds enumerated under the general exception explicitly refer to cyber risks, a WTO panel may find that the "public morals" exception affords an avenue through which to protect cybersecurity.[57] The parties in dispute, however, must present evidence – most likely involving classified documents – to demonstrate whether alternative measures, such as cybersecurity certifications or conformity assessment procedures, are less intrusive but equally effective. The Panel would have to assess whether such alternative measures should be regarded as WTO-consistent measures that are reasonably available to the responding party. Arguably, the necessity test can serve as a tool that guides states in taking targeted actions necessary to address cybersecurity concerns and refrain from creating unnecessary barriers to international trade.[58]

To be more concrete, the core issue here is the connection between the trade-related cybersecurity measures and the public morals objectives upon which such cybersecurity measures are based. The standard necessity test requires the consideration of alternatives to the measures taken in order to determine whether existing options are "less trade restrictive," while "providing an equivalent contribution to the achievement of the

[56] The Security Exceptions, for example, GATT, Article XXI; GATS Article XIV *bis*.

[57] WTO jurisprudence offers examples of public policies that have been found by panels or the Appellate Body to pertain to "public morals." See Section 1.4.3.

[58] Note that in quadrants III and IV, the TBT Agreement (TBT, Article 2.2) and the CPTPP-type data localization exceptions (CPTPP, Article 14.13) contain a "non-exhaustive" list of policy objectives, under which cybersecurity measures, subject to the necessity test, may be justified.

objective pursued."[59] In litigation, however, it would be unrealistic to expect two hostile states to present their intelligence information for or against the cybersecurity measures at issue. Because the complaining party must present scientific evidence to demonstrate that the proposed cybersecurity alternatives are at least "as good as" the trade measures taken by the responding party, the confidential and politically sensitive nature of security matters makes it particularly difficult for the parties to prove their case to a trade tribunal's satisfaction. It is equally impractical for the tribunal to engage in an evidence-based necessity test.

In any event, it will be a politically and technically challenging task for a trade tribunal to engage in an examination of whether the chapeau of the general exceptions can be satisfied. The two key concepts are "arbitrary or unjustifiable discrimination between countries where the same conditions prevail" and "disguised restriction on international trade," which "prohibit the abusive exercise of rights by states,"[60] and oblige a responding party to "articulate its defense promptly and clearly."[61] Again, such a procedural safeguard, however, poses a fundamental conflict with cybersecurity matters, where intelligence and other classified information are involved.[62] As Cohen argued, trade and security reflect different paradigms. The conflicts between the two competing interests occur not only at the legal technical level, but also at the systems level.[63] As a result, in most cases, the conventional GATT-type general exceptions operate awkwardly when balancing trade and security interests.

2.3.1.2 TBT Legitimate Objectives

In contrast to GATT Article XX and GATS Article XIV, the TBT exceptions, and in particular the "non-exhaustive" list provided in the

[59] See, for example, Panel Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products (EC – Seal)*, WT/DS400/R, June 18, 2014, paras. 5.260–5.264.

[60] Panel Report, *Peru – Additional Duty on Imports of Certain Agricultural Products (Peru – Agricultural Products)*, WT/DS457/R, November 27, 2014, para. 7.94.

[61] *Ibid.*

[62] Shin-yi Peng, "Cybersecurity and Trade Governance" in Julien Chaisse & Cristián Rodríguez-Chiffelle (eds), *The Elgar Companion to the WTO* (Edward Elgar 2023), chapter 3.

[63] Harlan Grant Cohen, "Nations and Markets" (2020) 23(4) Journal of International Economic Law 793, at 811.

TBT Agreement Article 2.2,[64] fall between quadrants III and IV due to their broader scope. As shown in Figure 2.1, unlike the conventional GATT general exceptions, which have a relatively narrow application in terms of the scope of the qualifying conditions, WTO jurisprudence makes it very clear that TBT Article 2.2 provides a "non-exhaustive list of legitimate objectives."[65] In other words, the open and illustrative list under TBT 2.2, which uses the word "inter alia," provides wider policy space for legitimate objectives advanced by the invoking party. Overall, it should be relatively easy to establish that the disputed cybersecurity standards fall within the scope of the exceptions provided under TBT 2.2.[66]

Nevertheless, the necessity requirement remains. TBT exceptions resemble those of the GATT general exceptions in the way that the standard necessity test applies. The key issue here involves whether certain cybersecurity measures, while serving "legitimate objectives," are "more trade restrictive than necessary" to fulfill the legitimate objective. The complaining party bears the burden of establishing that the cybersecurity measures are inconsistent with TBT Article 2.2 because the challenged standards created an "unnecessary" obstacle to international trade.[67] Further, the complaining party must explain why there are reasonably available, less trade-restrictive means of achieving the same

[64] TBT Agreement, Article 2.2: "Members shall ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade. For this purpose, technical regulations shall not be more trade restrictive than necessary to fulfill a legitimate objective, taking account of the risks nonfulfillment would create. Such legitimate objectives are, inter alia: national security requirements; the prevention of deceptive practices; protection of human health or safety, animal or plant life or health, or the environment. In assessing such risks, relevant elements of consideration are, inter alia: available scientific and technical information, related processing technology or intended end-uses of products."

[65] Appellate Body Reports, *United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products (U.S. – Tuna II)*, Recourse to Article 21.5 of the DSU by the US, Second Recourse to Article 21.5 of the DSU by Mexico, WT/DS381/AB/RW/USA, WT/DS381/AB/RW2, January 11, 2019, paras. 7.436–437.

[66] Particular attention should also be accorded to the TBT Preamble, which emphasizes a state's right to protect its "essential security interest." Arguably, the nature of certain cyberattacks, especially those involving critical infrastructure, disrupts "national security" and threatens a state's "essential security interests."

[67] Appellate Body Report, *Australia – Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging* (*Australia – Tobacco Plain Packaging*), WT/DS435/AB/R, WT/DS441/AB/R, June 29, 2020, para. 57–65.

level of protection.[68] The confidential, nontransparent nature of the cybersecurity matters once again renders the exercise of the necessity test relatively difficult.[69]

2.3.2 GATT-Type Security Exceptions

Conventional security exceptions (in quadrant II), which can be found in the WTO and many FTAs, represent another form of pre-digital era exceptions that are out of touch with cybersecurity policies. GATT Article XXI(b), as a representative clause, allows a state to take any action "it considers necessary" to protect its "essential security interests," stating the following:

> Nothing in this Agreement shall be construed:
>
> . . .
>
> (b) to prevent any contracting party from taking any action which *it considers necessary for the protection of its essential security interests*
>
> (i) relating to fissionable materials or the materials from which they are derived;
>
> (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;
>
> (iii) *taken in time of war or other emergency in international relations*; or
>
> . . . (emphasis added)

Historically speaking, national security exceptions had been utilized in a restrained and cautious manner. China, in both *China – Raw Materials* and *China – Rare Earths*, considered but eventually did not invoke the national security exceptions.[70] In those disputes, despite the fact that the

[68] *Ibid.*, para. 58.

[69] *Cf.*, Gregory Shaffer, "The WTO Tuna-Dolphin II Case (United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products)" (2013) 107 American Journal of International Law 192. Shaffer pointed out that, in 2012, the Appellate Body in all three TBT decisions found that the responding party failed to comply with TBT Article 2.1 nondiscrimination obligations. However, the Appellate Body concluded that the responding party did not violate TBT Article 2.2 obligations regarding "unnecessary obstacles to international trade." Although in different context, it can be argued that the trade tribunals are less comfortable about deciding whether a technical standard that pursues a state's legitimate objectives is "unnecessary."

[70] The disputes concerned China's use of export quotas and export duties on various forms of rare earths. Panel Report, *China – Measures Related to the Exportation of Various Raw*

Chinese government repeatedly stressed that China's restrictions were based on important national security concerns surrounding its reliance on foreign suppliers for its military supply chain since rare earth minerals are used in missile and aircraft systems,[71] China nevertheless did not invoke Article XXI(b) of the GATT.[72] In short, before the Panel Report of *Russia – Traffic in Transit* broke the ice, the GATT/WTO consistently avoided issuing findings on the merits of security exceptions for decades. The *Russia – Traffic in Transit* dispute somehow served as a catalyst for WTO members to bring legal challenges against security-based measures, and to invoke the security exception as a defense.

Since *Russia – Traffic in Transit*, WTO panels have clarified how the so-called self-judging clauses operate.[73] In theory, the term "it considers necessary" was drafted to reserve the right to opt out of certain treaty obligations otherwise imposed by the WTO agreements.[74] For decades, it was not clear how the concept of self-judging worked under Article XXI. How much discretion should there be in the determination of a measure's necessity? Should these national security exceptions be construed as entirely self-judging so as to sufficiently preserve the autonomy of a state's security matters? Does this mean that a state is entitled to unilaterally decide on what its essential security interests are, as well as what action is necessary to protect those interests?[75] In this regard, the Panel in *Russia – Traffic in Transit* conceded that Article XXI(b)(iii) "is not totally self-judging."[76] According to the panel, the discretion of a member to designate particular concerns as "essential security interests" is limited by

Materials (China – Raw Materials), WT/DS394/R, February 22, 2012; Panel Report, *China – Measures Related to the Exportation of Rare Earths, Tungsten, and Molybdenum (China – Rare Earths)*, WT/DS431/R, March 26, 2014.

[71] Panel Report, *China – Rare Earths*, *ibid.*, paras. 7.398, 7.404, 7.712.

[72] This discussion draws upon materials in Shin-yi Peng, "Cybersecurity Threats and the WTO National Security Exceptions" (2015) 18(2) Journal of International Economic Law 449, at 461–462.

[73] See *e.g.*, Panel Report, *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights (Saudi Arabia – IPRs)*, WT/DS567/R, not yet adopted, para. 7.238.

[74] Andrew Emmerson, "Conceptualizing Security Exceptions: Legal Doctrine or Political Excuse?" (2008) 11 Journal of International Economic Law 135, at 139–140; Ryan Goodman, "Norms and National Security: The WTO as a Catalyst for Inquiry" (2001) 2 Chicago Journal of International Law 101, at 119.

[75] Stephan Schill and Robyn Briese, "If the State Considers: The Self-Judging Clauses in International Dispute Settlement," in Armin von Bogdandy et al. (eds), *13 Max Planck Yearbook of United Nationals Law* (Martinus Nijhoff Publishers 2009), at 61, 67–69.

[76] Panel Report, *Russia – Measures Concerning Traffic in Transit* (*Russia – Traffic in Transit*), WT/DS512/R, April 5, 2019, paras 7.59, 7.78–7.82.

its obligation to apply GATT Article XXI(b)(iii) "in good faith."[77] The panel pointed out that the obligation of good faith requires members not to use the security exceptions as a means to circumvent their WTO obligations.[78] The panel must therefore review whether the security measures have been applied in good faith.[79] In this context, a "plausible link" must be established between the invoking state's "essential security interests" and the trade-restrictive measures in dispute.[80] If we follow the reasoning in *Russia – Traffic in Transit*, an invoking member must demonstrate that the disputed cybersecurity regulations "meet a minimum requirement of plausibility" in relation to the member's national security.[81] In this regard, "plausible link" might be questioned, and "bad faith" might be found, when network security regulations substantially favor domestic goods or services. However, the "good faith" standard will be particularly problematic when the measure at issue is motivated by both "protectionism" and "patriotism," namely, when commercial and security interests are inextricably linked.

More importantly, from *Russia – Traffic in Transit* to *U.S. – Steel and Aluminium Products*, WTO panels have adopted the view that the subparagraphs ("fissionable materials," "traffic in arms," and "war or other emergency in international relations") of Article XXI(b) are exhaustive in establishing the circumstances under which a state may "take the action which it considers necessary for the protection of its essential security interests."[82] In *U.S. – Steel and Aluminium Products*, the panel did not find that the measures at issue were "taken in time of war or other emergency in international relations" within the meaning of GATT Article XXI(b)(iii). In the panel's view, the subparagraphs "form alternative endings to a complete sentence under Article XXI(b)."[83] In other words, the opening terms in each subparagraph qualify the "action" referred to in Article XXI(b), and the three subparagraphs are exhaustive in establishing the circumstances under which a member may take the

[77] *Ibid*., para. 7.132.
[78] *Ibid*., para. 7.133.
[79] *Ibid.*
[80] *Ibid*., paras. 7.131–7.148.
[81] *Ibid*., para. 7.138.
[82] See, for example, Panel Report, *United States – Certain Measures on Steel and Aluminium Products (U.S. – Steel and Aluminium Products),* WT/DS544/R, not yet adopted, paras. 6.14–6.16, 7.113–7.114.
[83] *Ibid.*, para. 6.14.

"action" under Article XXI(b).[84] After emphasizing that there is no textual indication that the subparagraphs of Article XXI(b) are merely illustrative,[85] the panel also specifically pointed out – contrary to TBT Article 2.2, which explicitly indicates the illustrative nature of the provisions – that the subparagraphs of GATT Article XXI(b) are exhaustive in establishing the circumstances under which a member may take action to protect its essential security interests.[86]

Thus, trade-restrictive security measures can only be justified under Article XXI(b) if they meet one of the subparagraphs of Article XXI(b), specifically, the existence of an "emergency in international relations" within the meaning of Article XXI(b)(iii). An "emergency in international relations" within the meaning of Article XXI(b)(iii), however, must be "at least comparable in its gravity or severity to a war" in terms of its impact on international relations.[87] In this regard, where cybersecurity risks are routine and unexceptional in modern days, the gravity or severity of an "emergency in international relations," particularly with regard to its impact on international relations, may not be established. Moreover, the phrase "taken in time of" indicates a temporal relationship to the "war or other emergency in international relations."[88] The temporal link that requires cybersecurity measures to be "taken in time of" the "emergency in international relations" is also logically confusing when addressing a long-standing cybersecurity matter that,[89] as Heath observes, is of a permanent nature and must be systematically addressed over time.[90] Evidently, (conventional) security exceptions must be modernized to meet the policy needs of this digital era.

2.3.3 *CPTPP-Type Data Localization Exceptions*

CPTPP-type exceptions to data localization, which are contextualized in quadrant IV of Figure 2.1, contain a "non-exhaustive" list of policy objectives, under which security measures that are subject to the necessity

[84] *Ibid.*, paras. 7.111, 7.116.
[85] *Ibid.*, para. 7.113.
[86] *Ibid.*, footnote 443.
[87] *Ibid.*, para. 7.139.
[88] *Ibid.*, para. 7.112.
[89] *Ibid.*, paras. 7.112, 7.139–7.149.
[90] J. Benton Heath, "The New National Security Challenge to the Economic Order" (2020) 129 Yale Law Journal 1020, at 1046.

test may be justified.[91] To illustrate, Article 14.13 of the CPTPP (Location of Computing Facilities), while recognizing the parties' regulatory autonomy regarding requirements that seek to ensure the security and confidentiality of communications, prohibits parties from adopting data localization measures as a condition for conducting business. The Article also states the following:

> Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
>
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
> (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.[92]

Article 14.13 should be understood to mean that parties are allowed to maintain data localization measures to pursue their national security objectives as long as the measure satisfies the anti-protectionism requirements set out in the Article, namely, the procedural safeguard and the necessity test. Although locating computing facilities and storing data in multiple data centers within diverse jurisdictions seem to make more technological sense in managing cybersecurity risks, data localization measures that restrict the ability of companies to transfer data or, more narrowly, require local storage within a particular national border, have been a feature of national security policies. For example, China's Cybersecurity Law, citing national security, requires "critical information infrastructure" operators to store personal information or important data within the territory of China.[93] The Cybersecurity Law of Vietnam, as another example, requires Vietnamese data to be stored locally so as to protect national sovereignty.[94] Similar regulatory initiatives, with different degrees of emphasis on cybersecurity, can be found in various developed and developing countries, including Australia, Brazil, Canada, the EU, India, Peru, Malaysia, New Zealand, Russia, South Korea, and Taiwan, to name just a few.[95]

[91] CPTPP, Article 14.13. For more discussion on data localization, see Section 6.2 of this book.
[92] CPTPP, Article 14.13(3).
[93] China's Cybersecurity Law, supra note 37, Article 37.
[94] The Cybersecurity Law of Vietnam, Decree No. 53/2022/ND-CP, effective August 15, 2022, Article 26.
[95] This discussion draws upon materials in Shin-yi Peng and Han-Wei Liu, "The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?" (2017) 51:2 Journal of World Trade 183, at 185.

Note that, much like TBT Article 2.2, the CPTPP-type data localization exceptions contain an open-ended list of legitimate objectives and require an initial determination regarding whether, as an objective, the cybersecurity policy is legitimate. Such an approach leaves much ambiguity about how far the exceptions can go in curbing protectionist practices.[96] A CPTPP panel may consider relevant WTO jurisprudence with respect to the general exceptions of the WTO Agreement.[97] Additionally, as previously illustrated, precedent holds that the weighing and balancing exercise under the necessity analysis contemplates a determination as to whether a cybersecurity measure that is less inconsistent with the CPTPP rules is reasonably available.[98] Such alternative measures must provide an equivalent contribution to the achievement of the cybersecurity objectives pursued through the challenged measure. This "trade v. security" balancing exercise is likely to be impractical when confidential national security matters are involved. That being said, a trade tribunal is expected to be cautious when balancing trade and security interests if the localization measures overwhelmingly boost the domestic data industry.[99]

2.3.4 *New Generation Trade Agreements' Security Exceptions*

Trends in the new generation of international trade agreements suggest that "updated" security exceptions, either via expansive, open-ended formats or through a sectoral approach, are designed to reset the balance between international trade and national security. As shown in quadrant I in Figure 2.1, innovative clauses have been incorporated to reconcile the conflicts between (digital) trade and (cyber) security. The four types of security exceptions in quadrant I represent a dramatically expansive scope and excessively unfettered discretion in security exceptions under the international trade agreements.

2.3.4.1 CPTPP/USMCA-Type Broad Security Exceptions

Contrary to conventional security exceptions, under the CPTPP and USMCA, for example, security exceptions omit the subparagraphs that

[96] *Cf.*, note that several FTAs, such as the USMCA, contain a straightforward ban on data localization. See, for example, USMCA, Article 19.12.

[97] CPTPP, Article 28.12.

[98] See, for example, Panel Report, *EC – Seal*, WT/DS400/R, June 18, 2014, paras. 7.636–639. Appellate Body Report, *EC – Seal*, WT/DS400, paras. 5.260–264.

[99] See generally Neha Mishra, "The Trade – (Cyber)security Dilemma and its Impact on Global Cybersecurity Governance" (2020) 54(4) Journal of World Trade 567.

list the circumstances under which such exceptions could be triggered. By way of illustration, the security exceptions to the CPTPP state that "Nothing in this Agreement shall be construed to . . . preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests." This type of exception borrows the self-judging element from the WTO security exceptions but contains no limitative qualifying clauses that condition the application of security exceptions,[100] representing an open-ended, broad security clause.

2.3.4.2 DEPA-Type Security Exceptions

Similarly, the security exceptions under the DEPA – a digital sector-specific comprehensive framework – accommodate open-ended exceptions, which are not followed by a closed list of situations.[101] Given the fact that CPTPP is the primary textual source of the DEPA, it is not unusual that the three founding parties of the DEPA – Chile, New Zealand, and Singapore – incorporate the CPTPP-type broad security clauses into the DEPA text. Considering that DEPA is an international trade agreement tailored to the digital economy, and that cybersecurity threats take place across the entire digital ecosystem, such broad and loose security exceptions to the DEPA may mean that there is "no certainty of digital market access."[102] In other words, security interests will easily prevail over economic interests.

2.3.4.3 RCEP-Type Data Localization Exceptions

Another digital sector-specific security clause worth particular attention can be found in the security exceptions to data localization in the Regional Comprehensive Economic Partnership (RCEP). Article 12.14 (Location of Computing Facilities) allows the parties to undertake any data localization measures they consider necessary for the protection of essential security interests.[103] Unlike the CPTPP-type data localization

[100] See, for example, USMCA, Article 32.2; CPTPP, Article 29.2.

[101] See, for example, DEPA, Article 15.2 (Security Exceptions) <www.sice.oas.org/trade/DEPA/DEPA_Module15_e.pdf>.

[102] Dan Ciuriak and Robert Fay, "The Digital Economy Partnership Agreement: Should Canada Join?" (2022) 171 Centre for International Governance Innovation Policy Brief, at 6.

[103] See, for example, RCEP, Article 12.14 (Location of Computing Facilities) <http://fta.mofcom.gov.cn/rcep/rceppdf/d12z_en.pdf>. A similar provision can be found in the

exceptions, which are subject to the standard necessity test, RCEP data localization exceptions, by allowing a party to adopt any measure that "it considers necessary" for the protection of its "essential security interests," impose a lower and softer threshold. This threshold requires the invoking party to substantiate its good faith belief – albeit subjectively – that there is a threat to its "essential security interest," and that data localization measures are necessary for the protection of that essential security interest. It should also be noted that in the RCEP data localization exceptions, the self-judging element has been strengthened with a sub-paragraph stating that such measures shall not be disputed by other parties.[104]

2.3.4.4 RCEP-Type Critical Infrastructure Security Exceptions

As previously explained, critical infrastructure, such as 5G networks, constitutes the backbone of the functioning of a state. Given that the risk of compromised critical infrastructure can cause massive disruptions to the well-being of citizens, the protection of "critical public infrastructure" – whether publicly or privately owned – has been added to several new generation FTAs as one of the enumerated situations under which security exceptions can be invoked.[105] The textual structure of RCEP Article 17.13, which lists "national/international relations emergency" (Article 17.13(b)(iv)) and "critical infrastructures protection" (Article 17.13(b)(iii)) as parallel circumstances under which the security exceptions could be triggered, indicates that the negotiators of the RCEP intended to distinguish between "national/international emergency" and "critical infrastructures protection." Simply put, the structural separation signals that, when interpreting RCEP Article 17.13 (b) (iii) in

Indonesia-Australia Comprehensive Economic Partnership Agreement (IA-CEPA), Article 13.12 (Location of Computing Facilities) <www.dfat.gov.au/trade/agreements/in-force/iacepa/iacepa-text/Pages/iacepa-chapter-13-electronic-commerce>.

[104] *Cf.*, supra note 92. Note that the CPTPP-type data localization exceptions (CPTPP, Article 14.13) are contextualized in quadrant IV.

[105] RCEP, Article 17.13 (b) (iii) (Security Exceptions) <http://fta.mofcom.gov.cn/rcep/rceppdf/d17z_en.pdf>. Similar provisions can be found in other recently concluded FTAs, such as EU-Singapore Free Trade Agreement and Investment Protection Agreement (EU-Singapore FTA), Article 16.11(Security Exceptions) <https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore/eu-singapore-agreement/texts-agreements_en>; IA-CEPA, Article 17.3 (Security Exceptions) <www.dfat.gov.au/trade/agreements/in-force/iacepa/iacepa-text/Pages/iacepa-chapter-17-general-provisions-and-exceptions>.

context, the "emergency" element, which strictly limits the application of the GATT-type security exceptions, does not extend to critical infrastructure security exceptions. The textual structure thus effectively creates a broad and relatively easily satisfied enumerated exception to trade rules – the protection of critical infrastructure.

2.4 National Security and Trade Governance in a Datafied World

2.4.1 Scoping "Essential Security Interests": "Critical Infrastructure" as Touchstone

Taken together, the pre-digital era general and security exceptions are ill-tailored to address today's national security concerns. On the contrary, the new trends, which create open-ended or digital sector-specific security exceptions, are encouraging directions to ensure that the exceptions to international trade rules are aligned with the policy needs of the digital economy. However, the approaches taken in quadrant I may risk the potential for abuse and excessively broad overuse. In particular, the CPTPP/USMCA-Type Broad Security Exceptions – should they become a template for future international trade negotiations – may prove to be a fractious way forward in assessing the concepts of cybersecurity and national security. How can the good faith that requires minimum plausibility curb the potentially expansive interpretations of these types of security exceptions? In this age of digital capitalism, commercial and cybersecurity interests are entangled and often overlap. Most national regulations sit at the intersection of economic and security interests and can serve as both economic and national defense tools. Therefore, two fundamentally difficult issues, legally and technologically speaking, are to what extent cybersecurity concerns are legitimate, and how to distinguish the boundaries of these concerns from illegitimate protectionist measures that primarily stem from considerations surrounding economic competition. Moreover, in terms of sector-specific security exceptions, the questions of what constitutes "critical infrastructure" and how to designate it require due process mechanisms to constrain discretionary abuse.[106] Should social media platforms be considered "critical infrastructure"? How can we ensure non-discrimination in the process of

[106] Gregory Shaffer, "Governing the Interface of U.S. – China Trade Relations" (2022) 115 (4) American Journal of International Law 650, at 655–657.

identification and designation of critical infrastructure? These are the key issues the new generation trade agreements' security exceptions will confront.

It appears that the irreversible regulatory trends are designed to provide greater discretion for states in defining their own national security agenda. The excessively broad definition of "national security," as a result, is challenging the boundary between economic and security concerns. In its 2017 National Security Plan, the US explicitly declared that "economic security is national security."[107] As Claussen stated, the term "economic security" is now the central point, combining various concepts including economic dominance, independence, and hegemony.[108] Converged with the domain of economic security, the term "national security" is now being used in more and more expansive ways, literally including nearly everything – ranging from national broadband, industrial supply chain, and digital trade to steel tariffs, semiconductor export control, etc. This expansion will continue and will lead to an endless list in this digitally connected world. In the context of international economic law, the flexibilities provided under the new generation trade agreements' security exceptions could prove to be an inefficient approach in addressing legitimate security concerns. The overexpansion of the conceptual scope of national security may either mask legitimate objectives or fail to appropriately constrain illegitimate objectives.

What are the possible solutions to the dilemmas surrounding the overly limited quadrants II and III and the overly broad quadrant I approaches to national security? To be sure, there is no such thing as "zero risk" in cybersecurity.[109] In this hyper-connected datafied age,[110] the ever-increasing digital connectivity between computers and devices may mean that vulnerabilities can be introduced at any phase, and in any place.[111] Technical experts agree that a perfectly secure digital

[107] The US Joint Chiefs of Staff, "Trump Announces New Whole-of-Government National Security Strategy" (2017) <www.jcs.mil/Media/News/News-Display/Article/1400686/trump-announces-new-whole-of-government-national-security-strategy/>.

[108] Kathleen Claussen, "Trade's Security Exceptionalism" (2020) 72 Stanford Law Review 1097, at 1116.

[109] Robert O'Harrow, *Zero Day: The Threat in Cyberspace* (Washington Post E-book 2014).

[110] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014), at 34; Thomas Mowbray, *Cybersecurity: Managing Systems, Conducting Testing, and Investigating* (Wiley 2013), at 3–14.

[111] Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins Publishers 2012), at 69–102.

environment, free of vulnerabilities, is a dream, and "the notion of perfectly secure software almost certainly is a white whale."[112] The core issue turns out to be determining how much "risk" in cyberspace would amount to a danger to a state's "essential security interests."[113] Along a continuum of low to high national security risks, it is all about the relativities. In the context of "trade v. security," however, a borderline must be drawn somewhere, and trade-offs must be made.

That being the case, one possible future direction for trade and cybersecurity governance is to scrutinize the distinction between critical and noncritical infrastructure. Bearing in mind that more and more jurisdictions are now classifying critical infrastructure as a special category that is essential to national security in their domestic legal frameworks,[114] the creation of a commonly accepted definition of "critical infrastructure" would serve as a touchstone in determining the boundaries of "essential security interests." In other words, the protection of critical infrastructure presents a much stronger case than noncritical infrastructure in meeting the minimum requirement of plausibility in relation to a state's "essential security interests." In this regard, Shaffer observes that "the national security risks in the TikTok case are much lower than regarding Huawei's construction of critical infrastructure."[115] All in all, not every infrastructure is judged to be critical,[116] not every good or service from China is of national security concern,[117] and not all issues relating to innovative technology are equated with essential national security.[118] To conclude, "minimum plausibility" within the meaning of international economic law should be relatively easier to establish when it comes to critical infrastructure protection, because such risks, when severe, can disrupt the operations of a state's vital services, resulting in significant

[112] *Ibid*. See also Jane Chong, "Why Is Our Cybersecurity So Insecure?" (*The New Republic,* October 11, 2013).
[113] Peng, supra note 72, at 470.
[114] The UK National Protective Security Authority, supra note 15.
[115] Shaffer, supra note 106, at 650–654, 670.
[116] The UK National Protective Security Authority, supra note 15.
[117] In this regard, Kho pointed out that "taking the view that everything that China does is of national security concern ignores how best to address some of the key concerns that are in fact economic and competitiveness based." Stephen Kho and Yujin K. McNamara, "Focus on China: The Expansive Use of National Security Measures to Address Economic Competitiveness Concerns" (2022) 17 University of Pennsylvania Asian Law Review 368, at 375.
[118] Similar assertions have been made by the Chinese delegation in WTO meetings. See WTO, "Minutes of the Committee on Market Access" G/MA/M/70 (May 28, 2019).

loss of life and detrimental economic and social impacts. In this way, the concept of critical infrastructure may serve as a useful tool in filtering out the overgeneralization of national security claims. Ultimately, a more proper balance may be sustained between free trade and national security, and, in particular, cybersecurity.

2.4.2 Risk Assessment and Technical Standards

Another important direction for trade and cybersecurity governance is to prevent unfettered administrative discretion in security matters. This is particularly important in view of the fact that governments are moving toward risk-based approaches to protect national security and cybersecurity.[119] Instead of adopting prescriptive, one-size-fits-all rules, states assess cyber risks and exercise discretion to reduce them in a timely and proactive manner. It can be said that the most significant difference between ancient and modern security infrastructure is the rapid pace of change in security threats. The Great Wall of China was built across the northern border to protect imperial China against security threats. It took hundreds of years for ancient China's security situation to change. On the other hand, the modern security landscape has been measured in mere months, or even days. Literally, the perception of risks is in real time. In light of the dynamic nature of national security in modern days, it makes more sense for national regulators to take a risk-based approach rather than laying down prescriptive rules.

In this regard, several FTAs such as the Digital Trade Chapter of the USMCA include recognition of "the evolving nature of cybersecurity threats"[120] and the importance of taking risk-based approaches instead of adopting prescriptive regulations in addressing those threats.[121] On the one hand, a risk-based approach provides national regulators with some extent of flexibility to encourage innovation that may otherwise be constrained under a catch-all approach. Rather than a uniform set of

[119] In the author's view, US export controls that block access by China to advanced semiconductors used in artificial intelligence and quantum computing can be seen as an example of a "risk-based approach" to security management. Arguably, the so-called "small yard, high fence" strategic policy that precisely defines what technologies are key to US national security interests represents a tailored and targeted risk-based approach.

[120] See, for example, USMCA, Article 19.15, which promotes risk-based approaches rather than prescriptive regulation in addressing cyber threats.

[121] Similar text can be found in the consolidated negotiating text of the WTO JSI on E-Commerce, INF/ECOM/62/Rev (December 2020), at 58.

blanket prohibitions that apply to all in the same manner, the risk-based approach recognizes variances across or within critical sectors, allows for individual assessments, more efficiently targets implementation efforts in those sectors that pose the highest risk, and, at the same time, minimizes the regulatory impact on the critical industry and avoids unintended side effects of regulation.[122] In short, because digital technologies are rapidly evolving, any overly specific or rigidly prescriptive rules governing cybersecurity will either become quickly outdated or hinder innovation in the digital market.

On the other hand, the risk-based approach to cybersecurity comes with the danger of abuse of decision-making powers. Instead of applying the same rules in an equal way, irrespective of the level of risk or harm, the risk-based approach provides tailored protection, depending upon the level of risk at stake under each specific situation. Rather than imposing any kind of inflexible rules, national regulators exercise a degree of discretion when weighing cybersecurity risks, cyberattack harms, and regulatory benefits.[123] Because the approach relies on policy judgements rather than detailed prescriptions, the cybersecurity regulatory scheme leaves national regulators with broad discretion when conducting risk assessments. After all, at the core of the risk-based approach is a regulatory strategy through which regulators target resources toward sectors or activities that present the highest risk and, at the same time, reduce resources in those sectors or activities with relatively low risk. These decision-making processes designed to achieve the "right" balance between lower and higher risks "are all matters of judgement that regulators have to confront along the way," according to Black and Baldwin.[124] In many jurisdictions, cybersecurity measures will only be proposed where a need has been identified, namely, the regulatory targets. The danger of a risk-based approach, therefore, is discretionary abuse.

In this regard, there are rules that provide due process and other procedural safeguards at both the national and international levels to constrain discretionary power when assessing cybersecurity risks.

[122] Australian Government, Attorney-General's Department, "Submission to the Parliamentary Joint Committee on Intelligence and Security" (2017).

[123] See generally Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020), at 1–25.

[124] Julia Black and Robert Baldwin, "When Risk-Based Regulation Aims Low: A Strategic Framework" (2012) 6(2) Regulation & Governance 131, at 144.

In particular, international economic law is increasingly designed to constrain domestic regulation where the application of these regulations has external effects on other states. At the multilateral level, the obligations of GATT X:3(a) and GATS Article VI:1,[125] which allow challenges to the administration of domestic regulations that are otherwise consistent with the GATT or GATS, were designed to be an important tool in tackling situations in which a general scheme does not make any distinction between foreign and domestic service suppliers, but the administration of this scheme is not "reasonable, objective, or impartial."[126] Admittedly, GATT X:3(a) and GATS Article VI:1 may not be sufficiently forceful in a manner that safeguards due process and counters the potential abuse of administrative power in the process of risk assessment.[127] That said, as Chapters 3 and 5 will continue to address, the "good regulatory practices" agenda in the new generation FTAs, which seeks to enhance due process, transparency, legal clarity, and judicial review of administrative decisions, may shed light on how international trade agreements might prove helpful in preventing irrational, biased, or arbitrary cybersecurity risk assessments. Moreover, the adoption of international cybersecurity standards can mitigate concerns surrounding discretionary abuses in risk assessment. In this regard, the TBT Agreement can assume a substantial role in promoting international standards on cybersecurity, which can in turn facilitate the global development of common security approaches. At the end of the day, a nonregulatory approach and international soft law play important roles in governing cybersecurity and reshaping international economic order in the age of datafication. Chapter 6 will dive deeper into this aspect.

[125] See, for example, GATS, Article VI:1, which states "[i]n sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner."

[126] Padideh Ala'i, "From the Periphery to the Center? The Evolving WTO Jurisprudence on Transparency and Good Governance" (2008) 11(4) Journal of International Economic Law 779, at 795.

[127] Shin-yi Peng, "The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?" (2019) 22(1) Journal of International Economic Law 1, at 23. In this regard, van Aaken proposed that one possible procedural solution is establishing a special council on cybersecurity. Anne van Aaken, "Introduction to the Symposium on Digital Trade" (2023) 117 AJIL Unbound 94, 98.

2.5 Conclusion

This chapter addresses the data network in the context of the cybersecurity threat landscape, which is increasingly perceived as a national security issue, especially when critical infrastructure is directly involved. Before we shift the focus to digital applications that drive datafication, it is worth reiterating that data networks have become strategic political and economic assets of a state. As the backbone infrastructure, 5G networks literally resemble interactive central nervous systems in the data-driven economy. The weaponization of 5G networks has brought about further challenges to international economic legal order. In Chapters 1 and 2, we explored two important dimensions of the broadband infrastructure – "trade and development" and "trade and security" – both of which are the foundations for a platform-driven, data-fueled world. The chapters in Part II will zoom in on digital applications, analyze the phenomenon of platformization, and explore considerations pertaining to the regulation of digital platforms.