doi:10.1017/aju.2023.18

SYMPOSIUM ON DIGITAL TRADE AND INTERNATIONAL LAW

DIGITAL ECONOMY AND NATIONAL SECURITY: CONTEXTUALIZING CYBERSECURITY-RELATED EXCEPTIONS

*Shin-yi Peng**

This essay addresses the challenges of the digital economy in the context of cybersecurity threats that have growing implications for national security. It analyzes cybersecurity-related exceptions to international trade rules to explore whether and how these exceptions protect the state's digital policy space. The essay argues that the pre-digital era exceptions to trade rules are too narrowly framed to address cybersecurity concerns. This is in contrast to trends in the new generation of international trade agreements that create expansive security exceptions that are designed to reset the balance between international trade and national security. These new approaches must, however, be carefully guarded against potential abuses.

Digital Economy and Cyber Risks

Digital technologies have significantly transformed the way we live our lives. The performance of both the public and private sectors is reliant on a resilient digital infrastructure that facilitates cross-border data flows. The rapid development of "smart cities," in conjunction with progress in the internet of things and artificial intelligence, has increasingly transformed social and economic activities into data, which has in turn produced new forms of vulnerabilities: the multiplication of cybersecurity risks. In our daily lives, digital technology suppliers—ranging from mobile phone manufacturers to social media platforms—have the ability to build "back doors" into hardware or software and thus gain access to computer systems that bypass standard security mechanisms.

At the national level, cybersecurity threats have become a major concern for policymakers.[1] Specifically, critical infrastructure is "increasingly if not exclusively controlled by computers."[2] Cyber-attacks can damage critical infrastructure in various ways, including, for example, through directly taking control of industrial processes to block the functioning of power plants or water distribution systems. Due to the relatively low cost and wide availability of digital technologies, cyber-attacks now represent a popular method of warfare.[3] High-profile, hostile incidents over the years[4] and the recent war in Ukraine provide powerful lessons to other countries about the importance of a cyber defense.[5] In particular, cyber risks in the supply chains of critical industries are perceived as threats to the

* *Distinguished Professor of Law, National Tsing Hua University, Taiwan.*

[1] OECD, *Good Governance for Critical Infrastructure Resilience* 18–24 (2019).

[2] Parliamentary Joint Commission of the Australian Crime Commission, *Recent Trends in Practices and Methods of Cybercrime*, ch. 5 (Mar. 24, 2004).

[3] Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J. L. & TECH 403, 404–07 (2007).

[4] *See e.g.*, *Cyberattack Disrupts UK's NHS 111 Emergency Line*, ECON. TIMES (Aug. 8, 2022).

[5] *See e.g.*, Linus Chiou, *Taiwan Has to Secure Satellite Internet*, TAIPEI TIMES (Oct. 30, 2022).

© The Author(s) 2023. Published by Cambridge University Press for The American Society of International Law. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/aju.2023.18 Published online by Cambridge University Press

integrity of a state's critical infrastructure. Due to their role as the infrastructural central nervous system for the digital economy, the 5th generation (5G) networks face acute challenges as a result of cyber espionage, surveillance, and other cybersecurity risks, creating an intertwined relationship between digital trade,[6] cybersecurity, and national security.

Escalating Trade-Restrictive Cybersecurity Measures

The cyber arms race and digital reprisal have intensified geopolitical frictions. Major geopolitical players in the digital economy have adopted increasingly comprehensive cybersecurity measures. 5G supply chain security has been at the center of national security strategy in the United States under both Presidents Trump and Biden. Stressing that the backbone of the digital economy must be trustworthy and reliable, the Biden administration has accelerated the implementation of a set of trade measures to diversify supply chains and secure the infrastructural resilience of 5G networks.[7] At the infrastructural level, following Trump's "Clean Network" and "Clean Path" initiatives,[8] the current Federal Communications Commission (FCC) has cited the same national security grounds to order U.S. telecommunications companies to remove Huawei equipment (e.g., cell towers) and services (e.g., cloud services) from their networks.[9] At the digital platform level, although the Biden administration has withdrawn Trump's executive orders that ban transactions with eight Chinese software applications, the FCC has continued to request that U.S. digital platforms remove TikTok from their app stores.[10]

Across the Atlantic, recognizing that digital technologies constitute a vulnerable target, the European Union (EU) has put the implementation of measures to protect against cybersecurity threats at the forefront of its cybersecurity policies. The EU's adoption of the 5G Toolbox of Risk-Mitigating Measures, which delineates potential risk areas and remedial measures connected with suppliers of 5G infrastructure, seeks to achieve diversity among suppliers and reduce Chinese companies' (especially Huawei's) participation in the 5G roll-out.[11] Along this policy path, the proposed EU Cyber Resilience Act is expected to "bolster cybersecurity rules to ensure more secure hardware and software products."[12]

At the same time, China's cybersecurity regime has become even more complex and strict since its cybersecurity law was implemented,[13] primarily due to its lack of tailored definitions. The broad scope and vague language of China's cybersecurity law gives the government even wider latitude to facilitate its political and economic agendas.[14] The Chinese government has issued implementation measures for its cybersecurity law, including the "cybersecurity review" which imposes restrictions on foreign information technology goods and services based on "potential national security risks" related to the reliability of supply chains. Moreover, the Chinese Cryptography Law also contains trade-restrictive rules for commercial encryption products that involve national

[6] Trade-restrictive cybersecurity measures involve both trade in goods (e.g., ban on equipment from Huawei) and trade in services (e.g., ban on TikTok). The latter largely falls into the concept of "digital trade," which in this essay is understood in a broad sense, encompassing international trade enabled by digital technologies.

[7] U.S. White House, *National Security Strategy* 33–35 (2022).

[8] U.S. Dep't of State, *The Clean Network*.

[9] David Shepardson, *U.S. FCC Set to Ban Approvals of New Huawei, ZTE Equipment*, Reuters (Oct. 13, 2022).

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

[11] Eur. Comm'n, *Cybersecurity of 5G Networks – EU Toolbox of Risk Mitigating Measures* (2020).

[12] Eur. Comm'n, *Cyber Resilience Act* (Sept. 15, 2022).

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

[14] U.S. Trade Rep., *Report to Congress on China's WTO Compliance* 34 (2021).

https://doi.org/10.1017/aju.2023.18 Published online by Cambridge University Press

security.[15] Under the Chinese regulatory framework, loosely defined "encryption products" encompassing a wide range of information technology (IT) goods and services, must mandatorily undergo a cybersecurity risk assessment.[16]

Contextualizing Cybersecurity-Related Exceptions

Cybersecurity-based trade restrictions have the potential to clash with international trade rules in many ways, at both the World Trade Organization (WTO) and free trade agreements (FTAs) levels. Country-specific bans on IT goods and services may violate the most-favoured-nation principle that generally prohibits discrimination between "like" products from different countries. Arguably, major competitors of Huawei from Europe (Nokia and Ericsson) and South Korea (Samsung) will be the beneficiaries of the Huawei ban in the United States.[17] Cybersecurity measures may also be inconsistent with national treatment obligations if the domestic IT good or service and the banned foreign good or service are "like" products or services.[18] In cases where the cybersecurity standards constitute "technical regulations," unique cybersecurity standards that accord imported products less favorable treatment than that accorded to "like" products of national origin may also breach non-discrimination obligations.[19] Moreover, non-discrimination provisions in the electronic commerce/digital trade chapters of FTAs also require parties to ensure the non-discriminatory treatment of "like" digital products.[20] Thus, if domestic and foreign digital platforms are treated as "like" digital services, the adverse treatment of foreign digital platforms may be considered discrimination.

Furthermore, in terms of market access, cybersecurity measures can simultaneously constitute quantitative restrictions on international trade in goods and violate obligations to eliminate quantitative restrictions.[21] Similarly, these measures may restrict cross-border data flows and violate market access obligations for trade in services.[22] Additionally, cybersecurity-based restrictions in the public procurement of network equipment may also breach a state's market access schedules of commitment under the Government Procurement Agreement, which list the procurement activities open to international competition.

Nonetheless, general and security exceptions to trade rules provide a normative framework to balance free trade obligations against national policy interests. Thus, the key issue here relates to whether and how these exceptions protect a state's policy space to adopt regulatory actions directed at cybersecurity matters. In this context, the discussion below distinguishes between the types of exception clauses related to cybersecurity in international trade agreements along two dimensions. The first dimension is the nature of the necessity element required by the exception, which asks whether the "necessity test" or the "good faith standard" applies. The second dimension is the scope of situations allowed by the exception, which addresses whether the exception contains open-ended language or is limited to enumerated grounds. This essay argues, on the one hand, that the "conventional" general

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

[16] *Id.* at 35.

[17] MFN, e.g., General Agreement on Tariffs and Trade (GATT), Art. I; General Agreement on Trade in Services (GATS), Art. II.

[18] NT, e.g., GATT, *supra* note 17, Art. III; GATS, *supra* note 17, Art. XVII.

[19] Agreement on Technical Barriers to Trade (TBT Agreement), Art. 2.1.

[20] *E.g.*, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Art. 14.4, ATS 23 (*entered into force* Dec. 30, 2018); United States-Mexico-Canada Agreement (USMCA), Art. 19.4 (Nov. 30, 2018).

[21] GATT, *supra* note 17, Art. XI.

[22] GATS, *supra* note 17, Art. XVI. China claimed that the U.S. ban on TikTok violates its GATS commitments on advertising, entertainment and audiovisual services. *China Accuses U.S. of Violating WTO Rules in TikTok, WeChat Moves*, Inside U.S. Trade (Oct. 2, 2020).

https://doi.org/10.1017/aju.2023.18 Published online by Cambridge University Press

exceptions[23] and security exceptions[24] that were drafted in the pre-digital era are too narrowly framed to address cybersecurity objectives. On the other hand, trends to create open-ended or digital sector-specific security exceptions may also be problematic for being excessively unrestrained if due process and good faith are not accorded. Both perspectives are respectively discussed below.

Pre-Digital Era Exceptions: Not Fit for the Purpose

Conventional exception clauses that were drafted in the brick-and-mortar age are not properly formulated to address today's cyber threats. Taking General Agreement on Trade in Services (GATS) Article XIV General Exception 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 to protect cybersecurity. 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 in protecting public morals. The panel would then 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 to take targeted actions necessary to address cybersecurity concerns and refrain from creating unnecessary barriers to international trade.[25] In litigation, however, it would be unrealistic to expect two hostile states to present intelligence information for or against the cybersecurity measures at issue. The confidential and politically sensitive nature of security matters makes it legally impractical to perform an evidence-based necessity test.

Conventional security exceptions, which can be found in the WTO and in most FTAs, represent another form of pre-digital era exceptions that are out of touch with cybersecurity policies. The determination of what constitutes "essential security interests" and thus qualifies as an exception to trade rules is a self-judging process by the invoking state, but "good faith" obligations apply. Namely, a "plausible link" must be established between the invoking state's "essential security interests" and the trade-restrictive measures in dispute.[26] More importantly, in both *Russia—Traffic in Transit* and *U.S.—Steel and Aluminum 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) to the General Agreement on Tariffs and Trade (GATT) exhaustively enumerate the circumstances in which a state may "take the action which it considers necessary for the protection of its essential security interests."[27] Additionally, an "emergency in international relations" within the meaning of GATT Article XXI(b)(iii) must be "at least comparable in its gravity or severity to a war" in terms of its impact on international relations.[28] In this regard, an emergency may be difficult to establish where the cybersecurity risks are routine and ubiquitous. Moreover, the temporal link that requires the measures to be "taken in time of" the "emergency in international relations" is also problematic when addressing a long-lasting cybersecurity matter,[29] which, as Heath

[23] GATT, *supra* note 17, Art. XX; GATS, *supra* note 17, Art. XIV.

[24] GATT, *supra* note 17, Art. XXI; GATS, *supra* note 17, Art. XIV*bis*.

[25] Note that TBT Agreement Article 2.2 and CPTPP-type data localization exceptions (CPTPP, *supra* note 20, Art. 14.13) contain a "non-exhaustive" list of policy objectives, under which cybersecurity measures, subject to the necessity test, may be justified.

[26] Panel Report, Russia-Measures Concerning Traffic in Transit (Russian-Traffic in Transit), WT/DS512/R, paras. 7.131–7.148 (Apr. 5, 2019).

[27] *See e.g.*, Panel Report, United States—Certain Measures on Steel and Aluminium Products (US—Steel and Aluminium Products), WT/DS544/R, paras. 6.14–6.16, 7.113–7.114 (Dec. 9, 2022).

[28] *Id.*, para. 7.139.

[29] *Id.*, paras. 7.112, 7.139–7.149.

https://doi.org/10.1017/aju.2023.18 Published online by Cambridge University Press

argues, is of a permanent nature and must be systematically addressed over time.[30] It is apparent that conventional security exceptions must be modernized to meet the policy needs of this digital era.

Expansive Security Exceptions: Balance (Re)set?

Trends in the new generation of international trade agreements suggest that "updated" exceptions—either via expansive, open-ended security exceptions or through a sector-specific exception—are designed to reset the balance between international trade and national security. Innovative clauses have been incorporated to reconcile conflicts between (digital) trade and (cyber) security, including the following:

First, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)-type broad security exceptions: Contrary to Article XXI(b) of the GATT, such security exceptions do not include a closed list of circumstances under which security exceptions could be triggered, but rather contains broad exceptions which states are allowed to implement according to their discretion. Similar provisions can be found in the United States-Mexico-Canada Agreement (USMCA).[31] This type of exception is similar to the self-judging element from the WTO security exceptions but does not contain the qualifications included in WTO law.[32]

Second, Digital Economy Partnership Agreement (DEPA)-type broad security exceptions: In a similar vein, the security exceptions under the DEPA—a sector-specific framework that represents a new form of engagement for digital economy—accommodate open-ended exceptions, which are not followed by a closed list of situations.[33]

Third, Regional Comprehensive Economic Partnership (RCEP)-type data localization exceptions: Another digital sector-specific security clause that merits attention are data localization security exceptions to the digital trade rules in the RCEP, which allow the parties to take any data localization measure they consider necessary for the protection of essential security interests.[34] The self-judging element has been strengthened with a subparagraph stating that such measures shall not be disputed by other parties,[35] effectively opening the doors for parties to restrict data flows to achieve a range of regulatory objectives including privacy protection.

Finally, RCEP-type critical infrastructure security exceptions: given that the risk of compromised critical infrastructure can cause massive disruptions to the well-being of citizens, the protection of critical infrastructure—whether publicly or privately owned—has been added to several FTAs as one of the enumerated situations under which security exceptions may be invoked.[36] Recent initiatives, including the EU-U.S. Trade and Technology Council and the Indo-Pacific Economic Framework, further represent policy reforms to strengthen cyber supply chain security.

Concluding Remarks

Taken together, the trends that create open-ended or digital sector-specific security exceptions represent directions to ensure that the exceptions to international trade rules are aligned with the policy needs of the digital

[30] J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1046 (2020).

[31] USMCA, *supra* note 20, Art. 32.2.

[32] *See e.g.*, CPTPP, *supra* note 20, Art. 29.2.

[33] *See e.g.*, Digital Economy Partnership Agreement Between Chile, New Zealand, Singapore (DEPA), Art. 15.2 (June 11, 2020).

[34] *See e.g.*, Regional Comprehensive Economic Partnership (RCEP), Art. 12.14. Similar provision can be found in Article 13.12 of the Indonesia-Australia Comprehensive Economic Partnership Agreement (IA-CEPA).

[35] Note that, unlike the RCEP-type self-judging data localization exceptions, the CPTPP-type data localization exceptions (CPTPP, *supra* note 20, Art. 14.13) are subject to the necessity test.

[36] RCEP, *supra* note 34, Art. 17.13(b)(iii). Similar provisions can be found in other recently concluded FTAs, such as the EU—Singapore FTA (Article 16.11) and IA-CEPA (Article 17.3).

https://doi.org/10.1017/aju.2023.18 Published online by Cambridge University Press

economy. This essay contends, however, that these new approaches may risk being overly broad in application. In particular, should CPTPP/USMCA-type broad security exceptions become a template for future international trade negotiations, they may prove to be a fractious way forward in defining the boundary of national security, and particularly cybersecurity. In this age of digital capitalism, commercial and cybersecurity interests are intertwined. That said, fundamentally difficult questions, both legally and technologically, follow: to what extent are cybersecurity concerns legitimate? Further, how can we distinguish these concerns from illegitimate protectionist measures that primarily stem from considerations surrounding economic competition? This is particularly important because governments are moving toward risk-based approaches to protect cybersecurity.[37] Instead of adopting prescriptive rules, a risk-based approach provides national regulators with flexibility to encourage innovation that may otherwise be constrained under catch-all provisions. A risk-based approach to cybersecurity, however, carries the danger of abuse of decision-making powers. After all, the approach relies on policy judgements to provide tailored protection, depending upon the level of risk at stake for each specific situation.

How, then, can we curb the potentially expansive interpretations of "modernized" security exceptions? One possible future direction for trade and cybersecurity governance is to scrutinize the distinction between critical and non-critical infrastructure. Should social media platforms be considered "critical infrastructure?" Questions as to what constitutes "critical infrastructure" and how it should be designated require due process mechanisms to constrain discretionary abuse. Arguably, creating a commonly accepted definition of "critical infrastructure" would serve as a touchstone for determining the boundaries of "essential security interests." Namely, the protection of critical infrastructure presents a much stronger case than non-critical infrastructure to meet a minimum requirement of plausibility in relation to a state's "essential security interests." In this way, the concept of critical infrastructure may be a useful tool to filter out over-generalization of national security claims. Ultimately, a more proper balance may be sustained between free trade and national security, and particularly, cybersecurity.

[37] See, e.g., USMCA Article 19.15, which promotes risk-based approaches rather than prescriptive regulation in addressing cyber threats. Similar text can be found in the consolidated negotiating text of the ongoing WTO JSI on E-Commerce, WTO Doc. INF/ECOM/62/Rev, 58 (Dec. 2020).

https://doi.org/10.1017/aju.2023.18 Published online by Cambridge University Press