VOL. 13 JULY 2025 NO. 4

CHINA LEGAL SCIENCE

ARTICLES

TEXTUAL ANALYSIS OF CYBERSECURITY PROVISIONS IN DIGITAL TRADE AGREEMENTS AND CHINA'S RESPONSE

Huang Shixi

TABLE OF CONTENTS

TEXTUAL ANALYSIS OF CYBERSECURITY PROVISIONS IN DIGITAL TRADE AGREEMENTS AND CHINA'S RESPONSE

Huang Shixi[*]

With the development of Internet technology and artificial intelligence, the cybersecurity issue is not only a complex technical problem but also a regulatory issue of laws and policies. The governments and the international community have promulgated relevant laws and regulations to regulate cybersecurity. In recent times, the digital trade chapter of free trade agreements and certain digital trade agreements have also begun to stipulate specialized cybersecurity clauses, providing overall principles and obligations for digital trade, government capacity building, international operational cooperation, workforce cooperation, risk-based standards, and cybersecurity standards for the Internet of Things, etc. The cybersecurity provisions in existing digital trade agreements emphasize cooperation and consensus among contracting parties, and the rights of different types of enterprises. The cybersecurity provisions in China's digital trade agreements need to further keep up with the times. On the premise of emphasizing national security and digital sovereignty, a design draft that conforms to the concept of a community with a shared future in cyberspace and balances the interests of all stakeholders should be proposed to strengthen China's voice in the formulation of digital trade rules.

The nature of interconnectivity brought by digital technology in modern society has accelerated social development and is profoundly changing people's way of life and the mode of economic development. It is closely connecting governments, companies, and associations of all kinds, as well as individuals across the globe on an unprecedented scale. In particular, following the trade in goods and services, the development of high technology has promoted digital trade to become a new and emerging form of cross-border trade, using digital information network as an important carrier and a digital platform as strong support. Compared with traditional trade, digital trade has broken through the geographical boundaries of

* Professor at Law School of Shandong University. This article was funded by the National Social Science Fund in the later stage (Grant No. 20FFXA006) and the Innovation Team Project of 'Data Application and Governance in the Implementation of the Comprehensive Rule of Law Strategy' in Humanities and Social Sciences of Shandong University.

countries, as well as the temporal and spatial attributes of traditional trade. It has had a profound impact on global trade rules and regulatory models.

The global economy continues to adapt to an increasingly digital environment as international trade law regimes shift from multilateral agreements to bilateral or regional free trade agreements (FTAs). From mobile devices to social media and personal electronic devices, digital technologies are revolutionizing the way people collect and obtain information, live, shop, socialize, and work, generating more data than ever before. At the same time, high-tech developments such as robotics, artificial intelligence, and quantum computing are providing opportunities for businesses and governments in a wide range of industries to reap significant social and economic benefits. In an increasingly interconnected world, businesses, supply chains, and governments have become more dependent on the Internet and artificial intelligence. The proper utilization of such information or big data has enormous potential to improve human knowledge and understanding, increase productivity and efficiency, and deliver targeted goods and services to potential users. However, as the digital world expands, cybersecurity issues such as cybersecurity vulnerabilities, cyber malware intrusions, and data loss are also expanding. The intersection and potential tension between digital trade and cybersecurity continue to evolve. Cybersecurity issues pose a variety of risks (e.g., financial, strategic, and lethal risks) to governments, businesses, and people globally.[1] In addition to land, sea, air, and space, cyberspace has become the fifth new space for political, military, economic, social, and cultural interactions among countries.[2] The issue of cybersecurity has become an important part of national and international laws and policies. Governments and the international community are taking relevant measures to address cybersecurity issues.

As a new form of trade, digital trade, while bringing convenience and speed, has also brought about some new legal issues not anticipated by traditional trade rules. After all, the development of digital technology and its regulation vary among economies with different levels of development in the world. Different countries or regions have implemented different regulations on digital trade, including the establishment of rules for the application of digital technology, the formulation of digital trade rules, as well as cybersecurity and regulatory rules, etc. In particular, cybersecurity

1 Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 American Journal of International Law Unbound 207, 208 (2017).

2 Li Xiaoming, *The Criminal Law Legislative System and Its Construction in the Internet Era*, 5 China Legal Science 49 (2023).

governance and regulatory control, which are closely related to security, have become one of the hot debating topics in various countries and the international community. Cybersecurity is critical for all digital transactions, and it extends well beyond the technical aspects of network and data security to include national security, economic security, and even social order.[3] International trade and cybersecurity have become increasingly intertwined as a result of the increasing use of the Internet and the reliance of businesses and consumers on data flows for communications, e-commerce, and information exchange. In view of the different approaches taken by different countries in handling digital trade-related cybersecurity issues, the linguistic differences in the regulatory paradigms of cybersecurity provisions in different FTAs, and China's proposals to 'strengthen the cybersecurity system and institute oversight systems to ensure the safety of artificial intelligence', 'deepen international law enforcement cooperation in the realm of security', and 'enhance the mechanisms for China's participation in global security governance', etc., this paper analyzes the legal regulation of cybersecurity in the context of digital trade and textual differences, in the hope of identifying China's solution to deal with the provisions of digital trade. At the same time, given that the main content of this article is the cybersecurity provisions in trade agreements, the disputes on cybersecurity governance will not be discussed from the perspective of national security exception clauses.

I. INTRODUCTION

Cybersecurity is an issue that has gradually emerged with the development of the Internet. It is an approach to protecting Internet-connected devices from the threat of malicious attacks by actors around the world, preventing damage, and protecting and restoring communication services such as computers and electronic communication systems, as well as the information contained therein, in order to ensure, among other things, their availability, integrity, and confidentiality. In other words, cyberattacks are usually deliberate attempts by unauthorized persons to access information and communications technology (ICT) systems, typically for theft, sabotage, damage, or other illegal acts that disrupt business operations and may pose a wide range of risks to financial and communication systems, national

3 NEHA MISHRA, INTERNATIONAL TRADE LAW AND GLOBAL DATA GOVERNANCE: ALIGNING PERSPECTIVES AND PRACTICES, at 62 (Hart Publishing, 2024).

security, privacy, and digital trade and commerce.[4] From the perspective of cyber-physical infrastructure, cybersecurity encompasses defense mechanisms necessary to protect data infrastructure, network cables, and other physical components of the digital economy's underpinnings, such as smart devices.[5] Emerging cybersecurity threats and attack methods pose the greatest potential threat to cross-border data and privacy protection, leading to a continuous push by states and the international community to develop policies and regulations on cybersecurity regulation and governance, not only at the domestic level but also at the international level, especially when international and regional organizations have begun to regulate cybersecurity from different perspectives.

Cybersecurity is a security defense or safeguard issue that inevitably arises with the development of cybertechnology, especially cross-border data flows. It has become one of the fastest-growing policy areas in global data governance today, with the main purpose of addressing threats in cyberspace. However, there is still a lack of international consensus on the definition of cybersecurity. For example, the International Telecommunication Union (ITU) defines cybersecurity as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets ... Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.'[6] By characterizing the 'tools' and so on that protect the network environment and institutions as 'assets', the ITU recognizes that cybersecurity ensures that the security attributes of the organization's assets and users are achieved and maintained in response to the corresponding security risks in the network environment.[7] It has been proven that maintaining cybersecurity is difficult. However, it is also a process of constructing cyber norms, and 'understanding the actual processes by which cyber norms form, diffuse, and evolve is likely to influence the future shape of cybersecurity.'[8] Therefore, the technical and legal meanings

4 SHAYERAH I. AKHTAR & MICHAEL D. SUTHERLAND, DIGITAL TRADE AND U.S. TRADE POLICY, at https://crsreports.congress.gov/product/pdf/R/R44565 (Last visited on January 2, 2025).

5 Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51(2) UC Davis Law Review 475 (2017).

6 INTERNATIONAL TELECOMMUNICATION UNION, CAPABILITIES AND THEIR CONTEXT SCENARIOS FOR CYBERSECURITY INFORMATION SHARING AND EXCHANGE (ITU-T X.1209, 12/2010), at https://www.itu.int/rec/T-REC-X.1209-201012-I (Last visited on February 2, 2025).

7 Anahiby Becerril, *Cybersecurity and E-Commerce in Free Trade Agreements*, 13(1) Mexican Law Review 3, 18 (2020).

8 Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 American Journal of International Law 425, 479-480 (2016).

of cybersecurity may differ.

Cybersecurity does not seem to have much to do with trade on its surface, but digital trade is critical for any company that wants to trade across borders, thus bringing new complexities and security concerns. Cybersecurity risks arise when products or services contain computers or can be connected to the Internet across national borders. Moreover, in digital trade practices, there are no global rules for cybersecurity governance. Governments choose different models of cybersecurity governance and digital trade policies, resulting in major challenges such as differences in data privacy protection, restrictions on cross-border data flow, and uncontrolled expansion of data jurisdiction. People are increasingly concerned that digital products may be misused by foreign countries or multinational companies to collect private data, implant vulnerabilities, or pose threats to national security, etc., which means that digital products sold across borders should be subject to stricter scrutiny and control, and may become the target of bans by host governments. Given that cybersecurity has gone far beyond the technical and physical dimensions of cyber and data security, it is no longer a question of right or wrong, but rather a matter of when and how to deal with it. In any case, 'cybersecurity and trade are increasingly intertwined ... New trade rules that can both support risk-based effective cybersecurity regulation, build bridges between the cybersecurity policy in different countries to maximize synergies, and minimize barriers to trade are needed.'[9] However, if cybersecurity needs to be explored in the context of digital trade, there needs to be a clear definition of cybersecurity that is rooted in mutual cooperation in trade agreements.

In terms of domestic legal regulation of cybersecurity in digital trade, governments can adopt a variety of strategies to address cybersecurity risks, such as imposing import restrictions and establishing market access conditions and after-sales service requirements, etc. As a result, every time a multinational enterprise enters a country, it should be aware of the country's cybersecurity governance rules and requirements. Such policies not only differ between countries but also are changing constantly. After all, technological advancements are evolving all the time, which poses a significant risk to corporate governance seeking to manage cybersecurity. In practice, the measures implemented by governments to address cybersecurity vary widely, including strict controls of foreign investment in data-driven industries, stringent requirements on data storage and encryption methods, control of investment in foreign data industries on the ground of security, and

9 JOSHUA P. MELTZER & CAMERON F. KERRY, CYBERSECURITY AND DIGITAL TRADE: GETTING IT RIGHT, at https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/ (Last visited on February 2, 2025).

even the imposition of cyber sanctions in the face of threats.

As for the international legal regulation of cybersecurity, the importance of the regulation and principles of cybersecurity have been recognized in various international instruments. It has become a generally accepted notion in the international community that the order in cyberspace cannot be established without the application of international law.[10] Globally, the *Charter of the United Nations* and existing international law relating to national and international security apply to information and communication technology relations between states, serving as the cornerstone for achieving stability and security in cyberspace through international cooperation.[11] Security aspects are also covered by the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, which includes software and technology designed or used to conduct military offensive cyber operations.[12] Within the United Nations system, the *United Nations Convention Against Cybercrime*,[13] adopted in August 2024 to address cybersecurity and in particular to combat the use of ICTs for criminal purposes, demonstrates the efforts of sovereign states to secure cyberspace. Its provisions relating to electronic data, service providers, and regional economic integration mean that it can also be applied to the area of digital trade.

Given the rapid growth of digital trade, the expanding scope and depth of cybersecurity, and the involvement of both the state and the private sector, the connection between digital trade and cybersecurity involves many complex legal and policy issues. A number of FTAs, including digital trade agreements, have begun to incorporate the issue of cybersecurity into digital trade or e-commerce chapters. However, there may be some differences in terms of language and paradigms.

II. PARADIGM FOR CYBERSECURITY PROVISIONS IN FTAS

The current global economy is based on digital systems, which are essential for delivering digital products and services across borders and

10 Huang Zhixiong, *Application of International Law in Cyberspace: Establishing Rules of the Game*, 3 Global Law Review 5 (2016).

11 UN GENERAL ASSEMBLY, GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY: REPORT OF THE SECRETARY-GENERAL, A/70/174, 2015, at https://digitallibrary.un.org/record/555369?v=pdf&ln=fr (Last visited on May 26, 2025).

12 TAKU NEMOTO & JAVIER LÓPEZ GONZÁLEZ, DIGITAL TRADE INVENTORY: RULES, STANDARDS AND PRINCIPLES, OECD TRADE POLICY PAPERS NO. 251, at 20 (OECD Publishing, 2021).

13 The *United Nations Convention Against Cybercrime* was adopted by the General Assembly of the United Nations on December 24, 2024 in New York by resolution 79/243.

for conducting business with customers around the world. Trust in digital systems enhances each country's ability to promote consumer confidence and participate in the digital economy. Cybersecurity threats can transcend national borders and undermine the foundation of digital trade. In order to effectively respond to cybersecurity, governments and organizations must have the capability to address security threats technologically, implement risk management best practices in operations, and take consistent legal actions, including through the development of digital trade rules.

The problem is that cybersecurity is usually not a priority in trade agreements.[14] Instead, other issues of cybersecurity, such as data privacy, are often incorporated into specific parts of trade agreements.[15] In the absence of an international cybersecurity framework, countries are left to negotiate FTAs to regulate cybersecurity in digital trade. As a result, global rulemaking or regulatory efforts for cyberspace remain fragmented, with divergent perspectives and no centralized international institution or multilateral legal approach, undermining the growth potential of cybersecurity and digital trade. At present, FTAs serve as a crucial pathway to address this fragmentation by enabling governments to align with best practices, strengthen cybersecurity, and avoid the creation of non-tariff trade barriers. Some recently signed FTAs contain specific cybersecurity norms, such as the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP), the *Regional Comprehensive Economic Partnership* (RCEP), and the *United States-Mexico-Canada Agreement* (USMCA), as well as some specialized digital protection agreements, such as the *Digital Economy Partnership Agreement* (DEPA), which also have similar provisions on cybersecurity. Such trade agreements contain more comprehensive cybersecurity provisions, which are becoming increasingly rich, marking a paradigm of regulatory cooperation different from the national security exceptions in traditional FTAs, and more in line with the needs of global trade development in the digital era and the special rules of Internet governance. Therefore, serious attention needs to be paid to cybersecurity rules. Importantly, the new generation of FTAs recognizes the various linkages between digital trade and cybersecurity, takes into account the roles of different stakeholders, and reflects a wider view of cybersecurity cooperation and policymaking. This

14 According to OECD statistics, by June 2021, only 66 countries or territories have signed regional trade agreements containing cybersecurity provisions. However, the report does not specify which trade agreements incorporate cybersecurity provisions. *See* TAKU NEMOTO & JAVIER LÓPEZ GONZÁLEZ , *supra* note 12, 22.

15 Mira Burri, *Cross-Border Data Flows and Privacy in Global Trade Law: Has Trade Trumped Data Protection?*, 39(1) Oxford Review of Economic Policy 85 (2022).

section will analyze the language used in a selection of 17 typical FTAs that have included cybersecurity provisions to date,[16] outlining the characteristics and the paradigms of the language used in these FTAs.

A. The Importance of Government in the Cybersecurity Governance

Given that cybersecurity is one of the most typical technical and legal issues arising from the rapid development of global networks and digital trade, most parties to digital trade agreements recognize the link between cybersecurity and digital trade, including admitting that 'threats to cybersecurity undermine confidence in digital trade',[17] having 'a shared vision to promote secure digital trade to achieve global prosperity and recognize that threats to cyber security undermine confidence in digital trade',[18] recognizing 'the importance of cooperation on cybersecurity issues related to digital trade',[19] and so on. Such different languages have not materially changed the purpose of cybersecurity provisions, which is to facilitate the development of digital trade.

It is important to note that almost all digital trade agreements include the language for government capacity building in the context of cybersecurity services, requiring contracting parties to strive to build the capacity of their respective national entities responsible for cybersecurity incident response, emphasizing the importance of such government agencies to promote governmental capabilities in cybersecurity incident response. The CPTPP, for example, while not establishing an explicit link between cybersecurity and trade, does have one of the strongest cybersecurity capacity-building provisions, namely, 'building the capabilities of their national entities responsible for computer security incident response'.[20] Moreover, over time, trade agreements have not necessarily included stronger cybersecurity provisions, and the more recent *European Union (EU)-New Zealand FTA* does not contain any language on capacity building.

16 Digital trade agreements specifically examined include the USMCA of 2018, the CPTPP of 2018, the *US-Japan DTA of 2019*, the RCEP of 2020, the DEPA of 2020, the *Singapore-Australia DTA of 2020*, the *EU-UK TCA of 2020*, the *Singapore-New Zealand Protocol to Amend CEP of 2020*, the *UK-Australia FTA of 2021*, the *Korea-Singapore DPA of 2022*, the *UK-Singapore DEA of 2022*, the *UK-New Zealand FTA of 2022*, the *EU-Singapore DPA of 2023*, the *EU-New Zealand FTA of 2023*, the *UK-Ukraine DTA of 2023*, and the *ACFTA Digital Trade Protocol (Draft) of 2024*.

17 USMCA of 2018, article 19.15.1; *US-Japan DTA of 2019*, article 19.1; *UK-Australia FTA of 2021*, article 14.20.1; *UK-Ukraine DTA of 2023*, article 132-Q.1.

18 *Singapore-Australia DTA of 2020*, article 34.1; *UK-Singapore DEA of 2022*, article 8.61-L.1; *UK-New Zealand FTA of 2022*, article 15.18.1.

19 *EU-New Zealand FTA of 2023*, article 12.14.4.

20 CPTPP of 2018, article 14.16(a).

B. The Cybersecurity Operational Cooperation with Workforce Development as an Example

In the context of international cooperation on cybersecurity, FTAs require the use of new, enhanced, or existing intergovernmental cooperation mechanisms to identify and mitigate malicious cyber activities, for example, emphasizing the importance of collaboration mechanisms among parties to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks.[21] Alternatively, efforts can be made to enhance existing cooperation mechanisms to identify and mitigate malicious intrusions or malicious code propagation that affect electronic networks, respond quickly to cybersecurity incidents, maintain a dialogue on cybersecurity-related matters, share information to raise awareness and best practices,[22] and so on. However, the *UK-Singapore DEA* articulates ideals around cybersecurity but does not detail the areas of work or mechanisms needed to support cybersecurity as in other trade agreements, which are left to be negotiated in the future.[23]

The inclusion of international operational cooperation provisions for cybersecurity purposes is a widely adopted approach in FTAs, with the vast majority of agreements including some forms of international cooperation commitment. Although initial cooperation may set reasonable parameters for identifying and mitigating malicious cyber intrusions, the paradigm espoused by the United States and the United Kingdom,[24] respectively, goes a step further and includes language for sharing information and best practices among international partners. Moreover, the parties to FTAs continue to have difficulty in reaching consensus on cybersecurity issues. The differences remain in their commitment to the principles and how to implement them.

Some recent FTAs recognize the importance of workforce development in the area of cybersecurity and highlight opportunities for cooperation among parties, including possible initiatives related to mutual recognition of qualifications, diversity, and equality; or, alternatively, to cybersecurity

21 CPTPP of 2018, article 14.16(b); DEPA of 2020, article 5.2.2; *Singapore-Australia DTA of 2020*, article 34.2(b); *Singapore-New Zealand Protocol to Amend CEP of 2020*, article 9.17(b); *Korea-Singapore DPA of 2022*, article 14.22.2.1; RCEP of 2020, article 13.1.

22 USMCA of 2018, article 19.15.1(b); *US-Japan DTA of 2019*, article 19.1(b); *UK-Australia FTA of 2021*, article 14.20.2(c); *UK-New Zealand FTA of 2022*, article 15.18(b); *ACFTA Digital Trade Protocol (Draft) of 2024*, article 20.2.b-e.

23 *UK-Singapore DEA of 2022*, article 8-61.L.1(c).

24 *See UK-Australia FTA of 2021*, article 14.21.1(b)(iv); *UK-New Zealand FTA of 2022*, article 15.18.2(d); USMCA of 2020, article 19.15.1(b); *US-Japan DTA of 2019*, article 19.1.b, etc.

research, training, and development, among others.[25] Changes in the workforce development component of cybersecurity provisions in FTAs illustrate the difficulty of adopting the same language in the agreements. When FTAs adopt the same language regarding cybersecurity, it enhances the international community's ability to seamlessly interact with other partners who adhere to the same principles. Even minor changes in language can affect the interoperability of cybersecurity actions and initiatives across countries.

C. The Use of Risk-Based Criteria to Address Cybersecurity Threats

In addressing cybersecurity threats, several FTAs recognize that 'risk-based' approaches are more effective, encouraging parties to rely on consensus-based standards and risk management best practices to identify and prevent cybersecurity risks, detect, respond to, and recover from cybersecurity events,[26] or improve the cybersecurity resilience of the businesses and their customers,[27] etc. Alternatively, as stated in the draft African FTA digital trade protocol, 'each state party shall require enterprises within its jurisdiction to use best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity incidents.'[28] This provision does not explicitly provide the term 'risk-based', but it is clear from the entire provision that it appears to adopt a 'risk-based' standard. In applying risk-based standards, the relevant FTAs encourage companies to use 'consensus-based standards' or 'open and transparent industry standards', which, although interchangeable, refer to voluntary cybersecurity standards with the primary goal of reducing risks. Although 'consensus-based standards' are more abstract, 'open and transparent industry standards' mean that these standards can be implemented by the industry. Importantly, cybersecurity standards are practical and supported by the specific industry, which will rely on them to guide the cybersecurity risk management process.

Already widely adopted in domestic digital legislation in countries or organizations,[29] a risk-based approach allows for the establishment of

25 DEPA of 2020, article 5.2.3; *Singapore-Australia DEA of 2020*; *Australia-UK FTA of 2021*; *UK-New Zealand FTA of 2022*, article 15.18.2(c); *Korea-Singapore DPA of 2022*, article 14.22; *UK-Singapore DEA of 2022*, article 8-61.L.1(e); *UK-Ukraine DTA of 2023*, article 132-Q.2.

26 USMCA of 2018, article 19.15.2; *US-Japan DTA of 2019*, article 19.1; *UK-Australia FTA of 2021*, article 14.20.3; *UK-Ukraine DTA of 2023*, article 132-Q.3.

27 *UK-Singapore DEA of 2022*, article 8-61.L.2; *UK-New Zealand FTA of 2022*, article 15.18.3.

28 *ACFTA Digital Trade Protocol (Draft) of 2024*, article 25.3

29 Zhao Haile, *Research on Risk-Oriented Governance of Cross-Border Data Flows in the Negotiation of Trade Rules*, 6 Northern Legal Science 34 (2024).

appropriate controls for the most serious vulnerabilities and is more likely to achieve the level of security required for cybersecurity than prescriptive and compliance-based approaches to addressing cybersecurity threats. While a risk-based approach provides flexibility for national regulators to encourage innovation, it also carries the danger of abuse of decision-making powers. 'After all, the approach relies on policy judgments to provide tailored protection, depending upon the level of risk at stake for each specific situation.'[30] As a result, the adoption of risk-based cybersecurity provisions in FTAs has not met with much success and has only been adopted sporadically in the agreements selected for analysis.

D. The Mutual Recognition of Benchmark Security Standards for Consumer IoT

In practice, the Internet of Things (IoT) is the intersection of the physical and digital worlds and represents a transformative concept in the digital age. It fundamentally changes the way we interact with technology and the physical world.[31] Devices of all kinds are harnessing the power of interconnectivity to provide seamless experiences for consumers and businesses. The interconnectedness of IoT devices means that disrupting one device can lead to broader network vulnerabilities that threaten the security of the entire ecosystem, especially as the public policy issues that the innovation and growth of IoT pose on privacy, security, and reliability threaten the protection of the global digital economy.[32]

To realize the potential of IoT as a fully connected ecosystem, the answer may lie in the convergence of cybersecurity solutions and IoT.[33] However, by the end of August 2024, the only mutually recognizable provision in one digital trade agreement that encourages the establishment of baseline security standards for consumer IoT is the *Digital Trade Agreement* signed between

30 Shin-Yi Peng, *Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions*, 117 American Journal of International Law Unbound 122, 127 (2023).

31 Essentially, IoT refers to the interconnected network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, enabling these objects to connect, collect, and exchange data. This groundbreaking idea extends Internet connectivity beyond traditional devices like desktop and laptop computers, smartphones, and tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment via the Internet. *See* JASON EDWARDS, MASTERING CYBERSECURITY: STRATEGIES, TECHNOLOGIES, AND BEST PRACTICES, at 281 (Apress, 2024).

32 *See* Laura DeNardis & Mark Raymond, *supra* note 5.

33 JEFFREY CASO, ZINA COLE & MARK PATEL ET AL., CYBERSECURITY FOR THE IOT: HOW TRUST CAN UNLOCK VALUE, at https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value (Last visited on February 2, 2025).

the United Kingdom and Singapore. Under the terms of this agreement, the parties recognize the importance of 'establishing mutual recognition of a baseline security standard for consumer IoT devices to raise overall cyber hygiene levels and better protect cyberspace domestically'.[34] This provision addresses the use of a common security baseline for regulatory approvals by providing the language of mutual recognition of IoT security baselines. At the same time, the agreement recognizes that emerging technologies such as artificial intelligence and the IoT 'play important roles in promoting economic competitiveness and facilitating international trade and investment flows, and may require coordinated action across multiple trade policy areas to maximize their economic and social benefits',[35] and 'can benefit trade by creating the conditions required for consumers and businesses to maintain confidence when participating in digital trade'.[36]

With the development of IoT technology, the range of Internet products that make up the IoT is expanding, and they are vulnerable to relatively common security vulnerabilities. Many consumers are unaware of their security and do not have clear and simple access to trustworthy security information. Therefore, a standardized labeling system will help meet this need. Both the United States and the EU are developing cybersecurity labeling programs for IoT devices, but different or conflicting requirements would create another technical barrier to transatlantic cooperation and trade. Cooperation via common technical standards, testing bodies, and a mutual recognition agreement would provide a common baseline for IoT cybersecurity and allow firms to test only once in order to sell in both markets.[37]

Mutual recognition, such as a security baseline for IoT devices, could therefore be an important part of cybersecurity provisions in future digital trade agreements, which can promote the sale of IoT products that meet the security standards of contracting parties. In particular, the establishment of a common security baseline could help to improve the visibility of the cybersecurity ecosystem, enhance the overall resilience of the digital

34 *UK-Singapore DEA of 2022*, article 8.61-L.1(d).

35 *Id*., article 8.61-R.1.

36 *See* GOVERNMENT OF UK, EXPLANATORY MEMORANDUM ON THE DIGITAL ECONOMY AGREEMENT BETWEEN THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE REPUBLIC OF SINGAPORE, at https://assets.publishing.service.gov.uk/media/62287534d3bf7f1580c4ce4e/EM_CS_Singapore_1.2002_UK_Singapore_Digital_Economy_Agreement.odt (Last visited on February 2, 2025).

37 NIGEL CORY, WHY THE UNITED STATES AND EU SHOULD SEIZE THE MOMENT TO COOPERATE ON CYBERSECURITY LABELING FOR IOT DEVICES, at https://www2.itif.org/2024-us-eu-iot-cybersecurity.pdf (Last visited on February 2, 2025).

economy, and ensure that all necessary data is protected, such as the privacy and security concerns of IoT consumers or data users. Sharing a common cybersecurity baseline across the international community will improve the interoperability between nation-states, enhance the security posture of the economy, and prevent malicious threat actors.

In principle, advances in technology are the driving force behind the future landscape of digital agreements. As technology continues to evolve, the landscape of digital agreements will undoubtedly undergo further changes. Emerging technologies, including the IoT, may play a key role in making digital agreements more efficient and intelligent, and IoT devices can provide real-time data for digital contract execution. At the same time, future FTAs should promote, replicate, or expand the influential cybersecurity language not included in the previous agreements, such as key tools to promote the adoption of consensus-based standards and risk management best practices, but with relevant modifications based on national practices. The adoption of common principles will make the global cybersecurity ecosystem stronger as a whole, enhance consumer trust in digital systems, increase digital trade, and contribute to international economic development.

III. TEXTUAL ANALYSIS OF CYBERSECURITY PROVISIONS IN FTAS

In an increasingly digitalized world, international trade agreements need to incorporate and address cybersecurity provisions. That is a key issue in the technological realm. Incorporating cybersecurity principles into such agreements and emphasizing the importance of combining national policies with best practices and consensus standards have brought many benefits to the digital trade industry, as well as governments and consumers. However, there still remain a number of cybersecurity-related issues that need to be addressed.

A. The Cooperation and Consensus Among Parties

The development of cross-border digital trade is of critical importance to governments and consumers, as well as other stakeholders. Ensuring cybersecurity to protect consumers and maintain network availability will play a key role in enhancing digital cooperation and trust between countries. The norms of international cooperation in the field of cybersecurity are becoming increasingly important, with cooperative activities ranging from building the capacity of national entities responsible for responding to

cybersecurity incidents to making use of existing collaborative mechanisms to cooperate in identifying and mitigating malicious intrusions or code affecting electronic networks of both parties. One of the most important forms of cooperation is the risk-based approach to security prevention provided in trade agreements. Normative policies that deviate from established cybersecurity practices further exacerbate these limitations and may leave digital systems vulnerable to threats.

Although domestic policies are critical to address digital trade barriers and cybersecurity threats, international cooperation can generate benefits by maximizing positive cross-border spillovers through the exchange of expertise and resources. At the same time, states should adhere to and formulate globally interoperable digital rules on the basis of unity, cooperation, inclusiveness, mutual respect, and broad consensus, so as to prevent the division and fragmentation of digital governance rules.[38] Given the cross-cutting nature of cybersecurity, enhanced international cooperation can further create synergies to promote digital trade and address the security challenges faced by the least developed countries (LDCs) and other developing economies in digital trade.

As for consensus, it is mainly reflected in the fact that a growing number of consensus standards in digital trade and cybersecurity regulatory policymaking by state parties will facilitate market access and competition for stakeholders in different jurisdictions on an equal footing, as policy divergences in different countries can pose a significant threat to cybersecurity, thereby undermining market access and competition. For example, under the provisions of certain FTAs, contracting parties have the opportunity to address common regulatory objectives in a manner that is not trade-restrictive by adopting a risk-based approach and implementing consensus-based standards. However, when state parties implement policies that deviate from this approach, they risk creating a network of inconsistent or even conflicting legal requirements, which may have far-reaching implications and costs for companies. These conflicting legal requirements act as non-tariff barriers, forcing companies to assess whether such requirements are redundant or frequently have material differences. At the same time, the use of consensus standards can reduce regulatory complexity and promote multinational supply chain cooperation. By applying these consensus-based standards consistently on an international level, a level

38 CHINA'S POSITIONS ON GLOBAL DIGITAL GOVERNANCE (CONTRIBUTION FOR THE GLOBAL DIGITAL COMPACT), at https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-submission_China.pdf (Last visited on February 2, 2025).

playing field can be established to ensure that companies have equal access to opportunities regardless of the country of origin.

B. The Interests Balance Between High-Tech Enterprises and Small and Medium Enterprises

FTAs that incorporate the private sector, including both high technology enterprises and small and medium enterprises (SMEs), in cybersecurity provisions are still very rare. However, the collaborative role of large technology firms should be considered during the drafting and negotiation of FTAs. The complexity and uniqueness of cybersecurity make high-tech enterprises more powerful in cyberspace. They play a critical role in the development of cybersecurity norms in different ways, such as drafting and developing cybersecurity standards, enforcing security design requirements, collaborating with governments to develop cybersecurity best practices, and regulating cyber threats, etc.[39] In particular, large technology companies such as Google, Amazon, and Meta, which rely on advanced technology to firmly control the global cyber-physical infrastructure, code, algorithms, or data, etc., have the actual power to formulate cybersecurity rules.[40] Such non-state actors can also build their influence through consortiums to advance global cybersecurity governance principles by participating in regional and thematic Internet governance forums and other multi-stakeholder initiatives, such as the *Digital Geneva Convention*[41] and the *Paris Call for Trust and Security in Cyberspace*[42] in the domestic and international marketplace.

Unlike the dominant status of technology companies in terms of cybersecurity capabilities, governments may lack sufficient cybersecurity capabilities but have the power to set the rules, and are therefore more willing to accept the expertise of global consortia in cybersecurity. Indeed, while some governments are more willing to engage the high-techs in developing

39 Ben Haklai, *Cybersecurity Private-Public Partnerships: A Bridge to Advance Global Cybersecurity*, 56(3) Texas Tech Law Review 627, 687 (2024).

40 Huang Ying, *Cyberspace Fragmentation from the Perspective of Technology Trends*, 4 The Journal of International Studies 95 (2022).

41 *See* JOSEPH GUAY & LISA RUDNICK, WHAT THE DIGITAL GENEVA CONVENTION MEANS FOR THE FUTURE OF HUMANITARIAN ACTION, at https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/ (Last visited on March 2, 2025).

42 The *Paris Call for Trust and Security in Cyberspace*, launched on November 12, 2018, is the first major international initiative which is a resolute part of a multi-stakeholder approach including states, private companies (706 companies and private sector entities), and civil society organizations (309 organizations and members of civil society). *See* FRANCE DIPLOMACY, PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE, at https://www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace (Last visited on March 2, 2025).

cybersecurity norms and standards, others have adopted a more defensive role in accommodating them. For example, Vietnam has emphasized the critical importance of cybersecurity and non-traditional security issues, including ensuring national sovereignty in cyberspace, in the cause of nation building and national defense.[43]

In contrast to the collaborative role of large technology companies, FTAs should provide more commitments to SMEs in the area of cybersecurity operations. The formulation of digital trade policy and the drafting and negotiation of FTA provisions, including cybersecurity provisions, in many cases, have been developed in the context of prompting by large technology companies, with very limited participation from SMEs. However, the provisions of FTAs have greatly reduced the complexity of SMEs to participate in digital trade, enabling them to seamlessly integrate into the global supply chain while adhering to consensus standards, including 'enhancing the cybersecurity capability of businesses … and enabling greater cyber security resilience within industry'.[44] For example, by simplifying supply chain integration, promoting information sharing, and improving security effects, the commitments to cybersecurity trade provide substantial support for SMEs. Moreover, the consensus standards approach in FTAs enhances the ability of SMEs to participate in the market, integrating capable suppliers into their supply chains while complying with established security standards, thereby promoting healthy competition and welcoming new market entrants. Thus, the inclusion of cybersecurity provisions in trade agreements and the adoption of consensus standards can reduce the costs of compliance for SMEs, help to demonstrate best practices to SMEs, reduce their operational complexity, and incentivize SMEs to invest in key areas such as workforce development, education, and training, which are key factors in addressing cyber threats.

In the case of cybersecurity vulnerabilities, for example, in the context of preventing cybersecurity threats, almost all cybersecurity provisions in digital trade agreements remain silent on the issue of security vulnerability disclosure, which is detrimental to technologically disadvantaged SMEs. In principle, this should be a voluntary process for communicating the disclosure and receipt of identified cybersecurity vulnerabilities to

43 *See* ANH KIET, VIETNAM TIGHTENS NATIONAL SOVEREIGNTY PROTECTION IN CYBERSPACE, at https://hanoitimes.vn/vietnam-tightens-national-sovereignty-protection-in-cyberspace-319495.html (Last visited on March 2, 2025).

44 *See UK-Ukraine DTA of 2023*, article 132-Q, 1(b). There are few provisions that explicitly state that the parties are aware of the need to strengthen the cybersecurity capabilities of SMEs and increase cybersecurity resilience within their industries in digital trade agreements.

stakeholders. Trade agreements encourage the private sector, especially large technology enterprises, to implement a coordinated vulnerability disclosure program and incorporate it within the finalized cybersecurity provisions. Implementing a cybersecurity vulnerability disclosure program enhances product resilience and trust, thereby increasing trust in the digital ecosystem. While no trade agreement has included this element to date, the policies of some countries seem to encourage the adoption of such provisions in future trade agreements. Thus, the provision of unified vulnerability disclosure norms in trade agreements could also help to address trade barriers and promote better cybersecurity management by the international community.

C. The Role of Principle-Based Provisions in Cybersecurity Issues

The majority of the terms used in the cybersecurity provisions of the aforementioned FTAs do not provide the legal obligations or responsibilities of the parties from the perspective of substantive law but instead use some vague or even somewhat ambiguous terms to require the parties to undertake 'diligence' obligations in dealing with the issue of cybersecurity in principle. For example, in the chapeau of some articles, the expression 'recognize the importance of', or words such as 'shall encourage', or something like 'shall endeavor to', etc., are commonly used. While such 'aspirational' rules do not explicitly create binding and enforceable obligations, such guidance is not unusual in international trade agreements and remains valuable to ground the contracting parties' general expectations of each other and set the stage for future development in this area.[45] At the same time, similar provisions imply that the main content of such clauses is not the provisions of absolute substantive obligations, but rather principle-based obligations with the nature of soft law. Compliance with these obligations rests with the parties themselves, which raises the question of the implementation of cybersecurity provisions. That is, whether, in case of non-compliance by a party with the relevant provisions of such a clause, the other parties can bring a complaint or arbitration claim under the relevant provisions of the trade agreement. Of course, such principle-based prescriptive provisions allow treaty partners to use various FTA committees to review the implementation of these best endeavor provisions and emerging best practices, develop common principles that can be easily ratified, and attempt to identify potentially binding new

45 ELIZABETH WHITSITT, INTERNATIONAL TRADE LAW AND CYBERSECURITY: BALANCING FREE MARKETS AND REGULATION, *in* PUBLIC AND PRIVATE GOVERNANCE OF CYBERSECURITY: CHALLENGES AND POTENTIAL, at 180 (Tomoko Ishikawa & Yarik Kryvoi eds., Cambridge University Press, 2023).

provisions.

One question that arises from this is the issue of compliance mechanisms in FTAs. Trade agreements may encourage parties to periodically self-assess the progress in addressing cybersecurity threats or require their governments to allow other parties to conduct conformity assessments to minimize the burdens on trade. However, from the perspective of liability, they do not provide for the liability of non-compliance with relevant obligations. At the same time, countries with an average level of cyber technological development often lack the bargaining power to ensure that Internet service providers and digital trade exporters comply with local standards, and often face greater cyber threats because of a lack of domestic experts with specialized knowledge of cybersecurity and foreign legal systems.

IV. CHINA'S RESPONSE TO CYBERSECURITY REGULATION IN FTAS

The purpose of studying the textual paradigm of cybersecurity provisions in digital trade agreements and their main contents is to provide a basis to make suggestions on the design of cybersecurity clauses when negotiating and signing digital trade agreements, so as to better promote the development of Sino-foreign digital trade relations.

A. China's Policy and Legislation on Cybersecurity Regulation

The development of the Internet in China has gone through three stages: the Internet access stage from 1994 to 1999, the PC Internet stage from 2000 to 2011, and the mobile Internet stage from 2012 to the present.[46] Up to this point, China's network regulation has tended to gradually cover the process of comprehensive network governance, including network information services, information technology development, and network security protection.[47] There are more than 150 pieces of legislation in the cyber field,[48] including the *Regulations on the Security Protection of Computer*

46 JACK LINCHUAN QIU, THREE PHASES IN THE DEVELOPMENT OF CHINA'S NETWORK SOCIETY, *in* SOCIETY AND THE INTERNET: HOW NETWORKS OF INFORMATION AND COMMUNICATION ARE CHANGING OUR LIVES, at 341 (Mark Graham et al. eds., Oxford University Press, 2019).

47 CHINA'S LAW-BASED CYBERSPACE GOVERNANCE IN THE NEW ERA, at http://english.scio.gov.cn/node_9001076.html (Last visited on March 2, 2025).

48 Xu Qiang & Liu Xin, *China's Internet Rule of Law Has Made Steady Progress over the Past 30 Years*, Legal Daily, June 21, 2024, at 6-7.

Information Systems,[49] the *Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security*,[50] the *Measures for Cybersecurity Review*,[51] the *Provisions on the Management of Network Product Security Vulnerabilities*,[52] the *Cybersecurity Law*,[53] the *Data Security Law*,[54] the *Personal Information Protection Law*,[55] the *Regulation to Strengthen Protection over Critical Information Infrastructure*,[56] and so on. China's digital economy regulations place particular emphasis on cybersecurity.[57] For example, the *Cybersecurity Law of 2016*, with the main objectives of maintaining cybersecurity, safeguarding cyberspace sovereignty and national security, and promoting economic and social information, clarifies the governance objectives of cyberspace and increases the transparency of China's cybersecurity policies.

On top of consolidating the foundation of the cyberspace legal system, for the issue of cybersecurity, it is necessary to insist on synchronizing development and security, protect development with security, and promote the Internet to become the largest increment of social and economic development. Given that cybersecurity is a new topic of non-traditional national security that concerns the overall situation, it is necessary to build China's cybersecurity legal system through the enactment of national security laws, cybersecurity laws, data security laws, and other laws and regulations, in order to respond effectively to cybersecurity risks.

In terms of international cooperation, China actively participates in the construction of the rules of cyberspace and maintains the international order within the framework of the United Nations and international law, supports the role of the United Nations as the main channel for international cyber governance, puts forward the concept of a community with a shared future in cyberspace[58] and documents such as the *Global Initiative on Data Security*[59] to provide a blueprint for formulating the rule on global data security,

49 *Regulations on the Security Protection of Computer Information Systems of China of 2011*.

50 *Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security of 2000* (revised in 2011).

51 *Measures for Cybersecurity Review of 2021*.

52 *Provisions on the Management of Network Product Security Vulnerabilities of 2021*.

53 *Cybersecurity Law of the People's Republic of China of 2016*.

54 *Data Security Law of the People's Republic of China of 2021*.

55 *Personal Information Protection Law of the People's Republic of China of 2021*.

56 *Regulation to Strengthen Protection over Critical Information Infrastructure of 2021*.

57 Peng Yue, *Studies on the Issue of Trade Regulation in Data Localization Measures*, 2 Global Law Review 178 (2018).

58 XINHUA, FULL TEXT: JOINTLY BUILD A COMMUNITY WITH A SHARED FUTURE IN CYBERSPACE, at https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html (Last visited on March 8, 2025).

59 XINHUA, FULL TEXT: GLOBAL INITIATIVE ON DATA SECURITY, at https://english.www.gov.cn/news/topnews/202009/08/content_WS5f573805c6d0f7257693bb01.html (Last visited on March 8, 2025).

participates in the formation of regional rules on cyber governance,[60] and promotes the accession to the CPTPP and the DEPA and other high-level digital economic rules. At the same time, China has worked with certain countries to strengthen international law enforcement and judicial cooperation on cyber security, protect the online rights and interests of minors, and strive to set up a platform for exchanges on the rule of the network through the World Internet Conference.[61]

The rule of law in cyberspace has been gradually developed in China, and cybersecurity protection and governance have been strengthened. However, the problem of uneven distribution of network resources in the international community poses a potential threat. For that, during the negotiation of the *United Nations Convention Against Cybercrime*, China adhered to the concept of a community with a shared future in cyberspace, supported the development of a widely acceptable code of conduct for cyberspace under the framework of the United Nations, and made an important contribution to the consensus building.[62]

Furthermore, cybersecurity rules have been implemented under certain trade agreements in some domestic free trade zones in China. For example, on December 7, 2023, the State Council issued the *Overall Program for Comprehensively Keeping Pace with the High-Standard International Trade Rules and Implementing a High-Level Institutionalized Opening-Up Policy in the China (Shanghai) Pilot Free Trade Zone*, which focuses on digital trade and related cybersecurity issues. The relevant measures involve data, digital trade, and cybersecurity, including implementing high-standard digital trade rules as a priority, complying with the national security requirements for cross-border data transmission, allowing financial institutions to transfer data necessary for daily operations overseas, encouraging the establishment of a mechanism for cooperation with overseas cybersecurity organizations, fully implementing the responsibilities for the protection of critical information infrastructure, and carrying out data security management certification system to guide businesses to enhance data security management, etc.[63]

60 For example, China signed the RCEP in October 2020 and ratified it in March 2021. Chapter 12 of the RCEP deals with digital trade or electronic commerce.

61 Xu Qiang & Liu Xin, *supra* note 48.

62 MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE'S REPUBLIC OF CHINA, CHINA AND THE UNITED NATIONS: POSITION PAPER OF THE PEOPLE'S REPUBLIC OF CHINA FOR THE 74TH SESSION OF THE UNITED NATIONS GENERAL ASSEMBLY, at https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367393.html (Last visited on March 2, 2025).

63 *Notice of the State Council on Issuing the Overall Plan for Fully Aligning with International High-Standard Economic and Trade Rules and Promoting High-Level Institutional Opening-Up of the China (Shanghai) Pilot Free Trade Zone*, State Council Gazette Issue No.35 Serial No.1826 (December 20, 2023).

Nevertheless, the domestic legal policies on cybersecurity legislation still need further improvement, and supporting regulations and rules related to the *Cybersecurity Law* should be formulated to strengthen implementation effects. In particular, in the area of digital trade, although there are relevant provisions such as the *Data Security Law* that apply to security issues regarding cross-border data flows, their role in dealing with digital trade is relatively limited. The pilot approach implemented applies to one particular free trade zone for now, and it will take time to generalize and expand its application in China.

B. The Cybersecurity Provisions in China's FTAs

By the beginning of 2025, China had signed 23 FTAs with 30 countries or regions.[64] In addition to some early trade agreements, 9 trade agreements or FTAs have upgraded protocols with e-commerce chapters.[65] Among them, 3 trade agreements have cybersecurity clauses, namely article 13 of chapter 12 of the RCEP, article 13 of chapter 19 of the *China-New Zealand FTA Upgrade Protocol of 2021*, and article 12 of chapter 10 of the *China-Ecuador FTA of 2023*. The main contents of the cybersecurity clauses under these three FTAs include: (1) the parties recognizing the importance of building the capabilities of their respective competent authorities responding to or responsible for computer security incidents; and (2) the use of existing cooperation mechanisms to collaborate and prevent matters related to cybersecurity. The latest *China-Ecuador FTA* also stipulates that parties 'shall endeavor to promote actions for the prevention and protection against various types of cybersecurity incidents'.[66]

Compared to the aforementioned digital trade agreements signed by developed countries, such cybersecurity provisions in China's FTAs emphasize the ability of the competent authorities of the parties to deal with cybersecurity and the importance of strengthening international cooperation, while lacking provisions for other elements such as labor cooperation, IoT security, the use of risk-based standards, and so on. Moreover, China's Internet technology has been recognized by many countries or academics as

64 GLOBAL TIMES, CHINA HAS SIGNED 23 FTAS WITH PARTNERS ON FIVE CONTINENTS: MOFCOM, at https://www.globaltimes.cn/page/202501/1326585.shtml (Last visited on March 2, 2025).

65 The FTAs that include digital trade or e-commerce are the *China-Australia FTA of 2015*, chapter 12; the *China-Korea FTA of 2015*, chapter 12; the *China-Singapore FTA of 2018*, new chapter 15; the *China-Mauritius FTA of 2019*, chapter 11; the RCEP of 2020, chapter 12; the *China-Cambodia FTA of 2020*, chapter 10; the *China-New Zealand FTA of 2021*, chapter 19; the *China-Ecuador FTA of 2023*, chapter 10; and the *China-Nicaragua FTA of 2023*, chapter 12. Among them, the latest FTA with Nicaragua provides for a chapter on 'digital economy', while the others include chapters titled 'e-commerce'. The *China-Singapore FTA* and the *China-New Zealand FTA* have been upgraded to include e-commerce chapters.

66 *China-Ecuador FTA of 2023*, article 10.12.

a digital power, but efforts shall still be made to go from a digital power to a digital superpower.[67]

C. The Construction of Cybersecurity Provisions in China's Digital Trade

In recent years, China has repeatedly emphasized the need to fully and deeply participate in the WTO e-commerce negotiations, promote the acceleration of the construction of global digital trade rules, accelerate the establishment of a cross-border data flow cooperation mechanism with major economic and trade partners, and promote the construction of a multi-level global digital cooperation partnership network. Meanwhile, China will continue to advance its accession into the CPTPP and the DEPA, promote domestic reforms in related fields, negotiate and sign FTAs with more countries and regions, and expand the global high-standard free trade zone network, etc.[68] Therefore, drafting and designing cybersecurity clauses that are consistent with major digital trade rules is the key to China's participation in digital trade rule-making. The question is whether China can accept the paradigm of cybersecurity provisions stipulated in such agreements. After all, China's accession is unlikely to trigger the modification of the established provisions, but can only accept them, including meeting the requirements stipulated in relevant FTAs through the construction of legislation and legal system domestically.

In any case, regarding the issue of joining relevant treaties or designing cybersecurity provisions, there are several principles that need to be adhered to. Firstly, it is important to safeguard cyber sovereignty, i.e., a country's internal supremacy and external independence over the cyber facilities, cyber entities, cyber behaviors, and related cyber data and information within the territory of its own country.[69] That is, the exercise of national jurisdiction over the Internet is the core of China's digital governance system.[70] Secondly, it should be noted that cybersecurity is a form of non-traditional national security in a broad sense, the primary purpose of which is to maintain national security, followed by safeguarding the rights and interests of the

67 Liu Xiaoxin, *The Key to Moving from a Digital Power to a Digital Superpower*, 17 People's Tribune 48 (2023).

68 *Notice of the General Office of the State Council on the Issuance of the Action Plan for Solidly Promoting High-Level Opening-Up to the World with Greater Efforts to Attract and Utilize Foreign Investments*, the General Office of State Council Issue No. 9 [2024].

69 UNODA, CHINA'S POSITION ON CYBER SOVEREIGNTY, at https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-CHN.pdf (Last visited on March 2, 2025).

70 Peng Yue, *The Construction and Improvement of the Transnational Legal Order of the Digital Silk Road*, 3 China Legal Science 124 (2024).

interested parties. Thirdly, it is particularly important to adhere to the concept of a community with a shared future in cyberspace, improve and promote the construction of a digital trade rule system, and strengthen China's discursive power in the construction and development of global digital trade rules.[71] Last but not least, it is necessary to strike a reasonable balance between national sovereignty, cybersecurity, economic growth, and various stakeholders involved in cross-border digital trade transactions. Above all, China supports the establishment of an inclusive and continuous cybersecurity process with universal participation under the framework of the United Nations.

With regard to the language to be used in the design of cybersecurity provisions, taking into account the relevant provisions of the CPTPP and the DEPA, and the situation that China is currently applying for accession, the following language may be recommended.

Firstly, the close relationship between digital trade and cybersecurity should be recognized, and the fact that cybersecurity threats undermine the information of digital trade should be admitted. These are essential for the promotion and achievement of shared global prosperity. Contracting parties should understand that the relationship between digital trade and cybersecurity is akin to a symbiotic relationship, with cybersecurity underpinning digital trade, and digital trade, in turn, contributing to the development of cybersecurity. Such provisions may require amendments to China's internal legal systems. The design of cybersecurity provisions should take into account the amendment and consistency of domestic laws.

Secondly, it is important to strengthen the capacity of national entities responsible for responding to computer security incidents, utilize existing international cooperation mechanisms to cooperate in identifying and mitigating malicious intrusions or malicious code propagation affecting the electronic networks of the parties, and share information to raise awareness and best practices. There is a selection of different language terms to include in international cooperation depending on the contracting partners. Also, the importance of workforce development in the field of cybersecurity should be fully recognized. The last item involves possible measures related to mutual recognition of workforce qualifications, diversity, and equality. In terms of labor development and certification, the domestic labor development policies in the field of cybersecurity shall be improved, and laws and regulations shall be formulated in consistency with international rules based on China's national conditions and the needs of digital trade.

71 Wei Hao, Ma Maoqing & Yuan Ran, *Regional Trade Agreements, Digital Trade Rules, and the Rising of the Digital Export Trade*, 4 Journal of Beijing Normal University (Social Science) 134 (2024).

Thirdly, in the area of cybersecurity, China may recognize the importance of multi-stakeholder solutions and promote cooperation to address global problems. In this regard, China's concept of a community with a shared future in cyberspace could serve as a guide to promote cooperation with multiple stakeholders, including contracting parties, large high-tech enterprises, SMEs, and developing economies, to jointly identify global, inclusive, and cooperative solutions.

Fourthly, the use of a risk-based approach to cybersecurity can be discussed on a case-by-case basis depending on the contracting parties. In the era of network information, the 'risk-based approach' is more often applied in the field of cross-border data flows, and the legal regulations related to data are showing the characteristics of risk governance. The entry and exit of certain sensitive or critical data may pose high risks to different jurisdictions, although the identification of 'risk' may vary from country to country. In contrast, the 'risk-based approach' to identifying cybersecurity in digital trade agreements has a broader scope of application that goes beyond the mere movements of data across borders. In practice, the *Regulations on Promoting and Regulating Cross-Border Data Flow of 2024* provide that data collected and generated in activities such as international trade, cross-border transportation, academic cooperation, transnational production manufacturing, and cross-border marketing, excluding personal information or important data, are exempt from declaring for a cross-border security assessment.[72]

Finally, the emerging issue of IoT security standards in some trade agreements need to be determined in light of the process of the relevant domestic legislative progress and individual negotiating partners. For example, the United States, the EU, the United Kingdom, and Singapore have all enacted laws and regulations on IoT security and have made certain progress in the standard baselines, regulatory measures, and mutual recognition of IoT security.[73] However, it will take some time to determine

72 REGULATIONS ON PROMOTING AND REGULATING CROSS-BORDER DATA FLOW OF 2024 (ORDER OF CYBERSPACE ADMINISTRATION OF CHINA, NO.16), at https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm (Last visited on March 2, 2025).

73 For example, the EU has published the *General Data Protection Regulation* (GDPR), the *Network and Information Security Directive* (NIS Directive), the *EU Cybersecurity Act*, and the *Cyber Resilience Act*. In particular, the *2024 Cyber Resilience Act* imposes mandatory cybersecurity requirements for manufacturers and providers of products with digital elements to ensure compliance with cybersecurity standards from the outset, including IoT devices, representing a significant step toward standardizing IoT device security across the EU. The U.S. has announced the *IoT Cybersecurity Improvement Act of 2020* and the laws regulating the collection and use of personal information such as healthcare, finance, and children's online privacy. The *UK's Product Security and Telecommunications Infrastructure (PSTI) Act*, which came into effect at the end of April 2024, is a mandatory cybersecurity statute for internet-enabled devices, affecting businesses involved in consumer IoT products. *See* THALES, IOT CYBERSECURITY: REGULATING THE INTERNET OF THINGS, at https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations (Last visited on March 2, 2025).

whether they can be incorporated into the digital trade agreements signed by China. *China's Cybersecurity Law* provides for issues related to IoT security in general. The China-led international standard of IoT, i.e., the *Cybersecurity – IoT Security and Privacy – Guidelines for IoT-Domotics* (ISO/IEC 27403:2024), was officially released at the end of July 2024. This standard analyzes the security and privacy risks of IoT systems in the home and addresses cybersecurity, artificial intelligence security, data security, and other aspects of security control measures.[74] Nevertheless, more domestic laws and regulations on the IoT shall be established with binding force. Therefore, regarding the regulation of IoT security in digital trade agreements, it is advisable to negotiate with other countries on the basis of domestic laws and international guidelines initiated by China.

V. CONCLUSION

The expansion of the global digital economy has exacerbated cybersecurity threats. Governments are adopting and implementing trade-restrictive cybersecurity measures to regulate these ubiquitous and evolving threats, including national security-related measures. If the measures in question restrict trade in goods or services, they may be challenged under relevant WTO provisions, but such provisions are less appropriate for cybersecurity governance. Security exceptions in FTAs may have greater applicability in the cybersecurity environment. However, it will depend more on the language of these provisions and their interpretation by adjudicating bodies. As a result, traditional dispute resolution methods in trade agreements may not be appropriate for resolving these emerging and rapidly changing cybersecurity disputes.

While negotiations on digital trade issues have been a source of contention among the parties in recent FTAs, and international consensus on these issues remains elusive, there has been a steady and tangible progress on digital trade, at least in the key area of cybersecurity.[75] Such agreements, which contain provisions to respond to cybersecurity incidents and threats, have begun to address cybersecurity issues more openly, indicating that a new paradigm for cybersecurity regulation, which differs from the traditional

74 THE INTERNATIONAL STANDARD OF THE CYBERSECURITY–LOT SECURITY AND PRIVACY–GUIDELINES FOR IOT-DOMOTICS PROPOSED BY CHINA HAS BEEN OFFICIALLY ADOPTED, at https://www.tc260.org.cn/front/postDetail.html?id=20240701093303 (Last visited on March 2, 2025).

75 ALEX BOTTING, CAN CYBERSECURITY BE A UNIFYING FACTOR IN DIGITAL TRADE NEGOTIATIONS?, at https://www.darkreading.com/cybersecurity-operations/can-cybersecurity-be-unifying-factor-in-digital-trade-negotiations- (Last visited on March 2, 2025).

exception-based governance model, has begun to emerge. In addition, as international standards for regional trade agreements are harmonized globally, one can expect greater consistency in cybersecurity governance. At the same time, cybersecurity risks are becoming more serious as businesses, governments, and people become increasingly connected and reliant on digital technologies. New trade rules are therefore needed that both support effective risk-based cybersecurity regulation and build bridges among cybersecurity policies in different countries to maximize synergies and minimize trade barriers. The cybersecurity provisions in China's digital trade agreements also need to keep up with the times, on the one side, emphasizing national security and digital sovereignty, and on the other side, conforming to the concept of a community with a shared future in cyberspace and balancing the interests of all stakeholders, in order to strengthen China's voice in the formulation of digital trade rules.

(Edited by Li Jiesi)

数字贸易协定中的网络安全条款评述与中国因应

内容提要 随着互联网科技的发展而出现的网络安全问题不仅是一个复杂的技术问题，也涉及法律政策的规制。各国政府以及国际社会已经颁布了相关规制网络安全的法律法规。区域贸易协定的贸易章节以及某些数字贸易协定也开始规定专门的网络安全条款，对网络安全方面的数字贸易、政府能力建设、国际运营合作、劳动力合作、使用基于风险的标准以及物联网基准等方面作了总体原则性的义务规定。现有数字贸易协定中的网络安全条款在强调缔约国之间合作共识的同时，也要考虑到不同类型企业的权益。我国数字贸易协定中的网络安全条款也需要与时俱进，在强调国家安全和数字主权的前提下，提出符合网络空间命运共同体理念以及平衡各利益悠关方权益的设计草案，强化中国在数字贸易规则制定方面的话语权。