NOTES

DRAFTING CYBERSECURITY ARTICLES INTO TRADE AGREEMENTS FOR "DEVELOPING" NATIONS

An Analysis of How Different Trade Agreements Address Cybersecurity, How "Developing" Nations Are Disproportionately Affected by Cyber Threats, and How Trade Agreements Can Address Cyber Concerns

Nichole Chen*

Abstract

The rapid growth of the digital age has been met with greater reliance on digital trade in all sectors. While this increasing digital connectedness is proportional to the growth in cyber threats, digital trade has not yet caught up in dealing with these threats. Part I of this Note introduces what digital trade and cybersecurity are and how the lack of cybersecurity affects digital trade, especially for "developing" nations. Part II explores how the traditional exceptions of security and necessity in trade agreements, through the lens of the World Trade Organization (WTO), are inadequate to deal with cybersecurity. Part II also explores the competing theories of mutual cooperation and data localization by examining select regional trade agreements. Part III discusses the gap between "developed" and "developing" nations in combating cybercrime and enforcing legislation. Part IV proposes solutions on how trade agreements can remedy the cybersecurity challenges "developing" nations face. Finally, Part V concludes the paper with an urge for mutual cooperation in cybersecurity.

---

* Nichole Chen. Georgetown University Law Center, J.D. 2023; University of California, Los Angeles, B. A. 2019. The author would like to sincerely thank her advisor, Professor Katrin Kuhlmann, for her advice throughout the writing process, her patient and thorough feedback, and her constant encouragement to pursue a future in international trade. She would also like to thank the Institute of International Economic Law for supporting this Note through the John D. Greenwald Writing Competition. Finally, she would like to thank the editorial board at the *Georgetown Journal of International Law* for their thoughtful support. This piece is also published in *Nichole Chen, Drafting Cybersecurity Articles into Trade Agreements for Developing Nations, in* NEXT-GENERATION APPROACHES TO TRADE AND DEVELOPMENT: BALANCING ECONOMIC, SOCIAL, & ENVIRONMENTAL SUSTAINABILITY (Katrin Kuhlmann, 2023).

I. INTRODUCTION

International trade and cybersecurity have become increasingly intertwined because of the growth in internet use and dependence on data flows by businesses and consumers for communication, e-commerce, and information exchange.[1] As a result, businesses, supply chains, and governments have become reliant on the internet and artificial

1. Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment* 7 (Glob. Econ. & Dev., Brookings Inst., Working Paper No. 79, Oct. 2014), https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf.

intelligence in a world of growing global interconnectivity.[2] Most industries rely on data movement to some degree, especially with internet platforms, e-commerce firms, online payment and financial services, computer services, and logistics firms. This growth in the use of information and communication technologies (ICT) results in a proportional reliance on ICT goods and services, estimated to represent 6.5% of the world's gross domestic product (GDP) in 2017.[3] The past two decades welcomed exponential growth in digital trade.[4]

The rise in e-commerce experienced an unprecedented boost during the COVID-19 pandemic, with greater consumer demand for both essential and non-essential goods.[5] Not only did businesses shift from physical stores to e-commerce, but many businesses also shifted from domestic sales to cross-border e-commerce with the mandated closure of non-essential retail stores.[6] As a result, e-commerce became more heavily tied to data transmission, which resulted in greater business reliance on third-party online platforms, especially in "developing" countries.[7] For example, Paystack, a financial payment company in Africa, recorded a five-fold surge in transactions compared to pre-pandemic levels.[8] Similarly, India's Unified Payment Interface, a platform for

2. Michael J. Ferentina & Emine E. Koten, *Understanding Supply Chain 4.0 and its Potential Impact on Global Value Chains*, *in* GLOBAL VALUE CHAIN DEVELOPMENT REPORT 103, 105 (2019).

3. Anahiby Becerril, *Cybersecurity and E-commerce in Free Trade Agreements*, 13 MEX. L. REV. 3, 6 (2021), https://doi.org/10.22201/iij.24485306e.2020.1.14808.

4. *Id.* at 5.

5. KATRIN KUHLMAN, U.N. ECON & SOC. COMM'N FOR ASIA AND THE PACIFIC, HANDBOOK ON PROVISIONS AND OPTIONS FOR TRADE IN TIMES OF CRISIS AND PANDEMIC 134 n. 467 (2021) [hereinafter UNESCAP HANDBOOK] (citing Dylan Loh, *Coronavirus Pandemic Fuels Asia E-Commerce Boom*, NIKKEI ASIA (May 31, 2020), https://asia.nikkei.com/Business/Retail/Coronavirus-pandemic-fuels-Asia-e-commerce-boom; Kok Xinghui, *Coronavirus: E-Commerce in Southeast Asia Rides High on Pandemic Boom*, S. CHINA MORNING POST (Aug. 1, 2020), https://www.scmp.com/week-asia/economics/article/3095585/coronavirus-e-commerce-southeast-asia-rides-highpandemic-boom); Ananya Bhattacharya, *Indians Are Now Spending More on E-Commerce Than They Did in 2019*, QUARTZ INDIA (Aug. 19, 2020), https://qz.com/india/1892653/despite-covid-19-slump-indians-are-spending-more-on-e-commerce/; Sarah Perez, *COVID-19 Pandemic Accelerated Shift to E-Commerce by 5 Years, New Report Says*, TECH CRUNCH (Aug. 24, 2020), https://techcrunch.com/2020/08/24/covid-19-pandemic-accelerated-shift-to-e-commerce-by-5-years-new-report-says/).

6. UNESCAP HANDBOOK, *supra* note 5, at 102 (citing Evelyn Cheng, *Chinese Companies Look to Ride A New Cross-Border E-Commerce Wave Driven By The Coronavirus*, CONSUMER NEWS & BUS. CHANNEL (July 28, 2020), https://www.cnbc.com/2020/07/29/chinese-companies-look-to-ride-a-new-cross-border-e-commerce-wave.html).

7. UNESCAP HANDBOOK, *supra* note 5, at 102.

8. Pallavi Pengonda, *Flipkart IPO May Ride Piggyback on Post Covid-19 Boom in ECommerce*, LIVEMINT (Dec. 7, 2020), https://www.livemint.com/market/mark-to-market/flipkart-ipo-may-ridepiggyback-on-post-covid-boom-in-e-commerce-11607343275121.html.

digital payments, saw double the number of transactions from 2020-21.[9] COVID-19 has shown the importance of many data privacy and protection issues. First, increased digitalization necessitates protection for stakeholders and government parties. Second, increased data collection for state-wide initiatives, such as contact tracing, demonstrates how wholesale personal data is collected and therefore needs to be regulated. Third, COVID-19 has highlighted states' approaches to data sovereignty in efforts to protect from cyber threats. Although cybersecurity has long been a concern with the rise of digital trade, COVID-19 has highlighted the issue of cyber threats even more.

The growth of global interconnectivity also increases exposure to the risks and costs of cyberattacks. For example, the WannaCry ransomware attributed to North Korea infected over 200,000 computers across 153 countries, resulting in millions of dollars in damage.[10] In 2018, Facebook notified its users of the largest data breach ever, affecting over 50 million people.[11] Due to an increased reliance on digital trade across sectors globally, the risks of cyber threats have been even greater amid the COVID-19 pandemic. This is especially problematic for "developing" countries, whose digital capacities lag behind the rest of the world's. Accordingly, "developing" nations are more likely to be the targets of cyber criminals. For example, Uganda's telecommunications and banking sectors were hacked through SIM cards in October 2020, compromising the country's mobile money network and costing the country approximately USD $3.2 million.[12] At the height of COVID-19 in June 2020, the second-largest hospital operator in South Africa was hit by a cyberattack, forcing the hospital to switch back to manual backup systems.[13] The International Telecommunication Union's Global Cybersecurity Index reported that "developing" countries, especially in South America, Africa, the Middle East, and Southeast Asia are

9. Tarush Bhalla, *UPI Transactions More Than Doubled in A Year to 2.7 Bn.*, LIVEMINT (Apr. 1, 2021), https://www.livemint.com/news/india/upi-transaction-in-india-doubles-in-a-year-11617261866805.html.

10. Joshua P. Meltzer & Cameron F. Kerry, *Cybersecurity and Digital Trade: Getting it Right*, BROOKINGS INST. (Sept. 18, 2019), https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/.

11. Isaac Mike & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

12. Stephen Kafeero, *Uganda's Banks Have Been Plunged into Chaos by a Mobile Money Fraud Hack*, QUARTZ AFRICA (Oct. 10, 2020), https://qz.com/africa/1915884/uganda-banks-mtn-airtel-hacked-by-mobile-money-fraudsters/.

13. Samuel Mungadze, *Life Healthcare Group Hit by Cyber Attack Amid COVID-19*, ITWEB (June 9, 2020), https://www.itweb.co.za/content/JBwErvnBK4av6Db2.

among the countries that are least equipped to deal with cyber threats.[14]

The growth of ICT in every sector of the world's economy, political processes, and social systems presents security threats. As cyberspace is transnational, countries face ongoing difficulties in enforcing cybersecurity. This Note will discuss how trade policy can strengthen cybersecurity practices and how trade agreements can better incorporate cybersecurity.

A. *Defining Digital Trade and E-Commerce*

The WTO defines e-commerce as "the production, distribution, marketing, sale or delivery of goods and services by electronic means."[15] Digital trade is broader than e-commerce because it also involves data flow and the exchange of goods and services.[16] In its Work Programme on Electronic Commerce, the WTO adopts a comparatively broad definition, noting that "electronic commerce is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means."[17] This encompasses everything from electronic fund transfers, credit card payments, virtual markets, cloud computing, big data, artificial intelligence or blockchain, the Internet of Things (IoT), biotechnology, nanotechnology, and other related areas.[18] Cyberspace is the platform where e-commerce is carried out, as well as the foundation for digital trade.[19]

B. *Defining Cybersecurity*

Cybersecurity strives to deal with threats in cyberspace. The International Technology 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."[20] However, there is

14. INT'L TELECOMM. UNION [ITU], *Global Cybersecurity Index 2018*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

15. General Council, *Work Programme on Electronic Commerce*, WTO Doc. WT/L/274 (adopted Sept. 25, 1998).

16. *Id.*

17. *Id.*

18. *See* Becerril, *supra* note 3, at 10.

19. *Id.* at 16.

20. ITU, *Capabilities and Their Context Scenarios for Cybersecurity Information Sharing and Exchange*, Rec. ITU-T X.1209 (12/2019) (Dec. 17, 2010), https://www.itu.int/rec/T-REC-X.1209-201012-I.

currently a lack of consensus over the boundaries of what cybersecurity entails. For example, the U.S. National Institute of Standards and Technology (NIST) defines cybersecurity as:

> [T]he prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.[21]

This definition suggests that cyberattacks can be divided into two types: attacks on information and attacks on information systems. However, the NIST definition does not differentiate between actions taken by countries and actions taken by private individuals. Additionally, it does not differentiate between the impact of a cyberattack on public information or networks from the impact on private ones. The NIST definition of cybersecurity highlights the difficulty of a lack of consensus over cybersecurity policies. This Note takes the position that digital trade requires a clear definition of cybersecurity rooted in mutual cooperation in trade agreements.

II. Cybersecurity in Trade Agreements: Challenges to Enforcement in International Law

Cybersecurity is often not a priority in trade agreements. Instead, aspects of cybersecurity, such as data privacy, are often mentioned as sections under various sector-specific parts of trade agreements.[22] Absent an international framework for cybersecurity, countries are left to negotiate their free trade agreements (FTAs) or rely on multilateral trade agreements. Global rulemaking efforts dealing with cyberspace

21. Nat'l Inst. of Standards & Tech., Glossary of Key Information Security Terms (last updated Mar. 28, 2023).

22. *See* Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization art. 2, June 16, 2009, http://eng.sectsco.org/load/207508/(This Agreement by the Shanghai Cooperation Organization (SCO) was created to fight terrorism, separatism, and extremism to counter the Western approach to cyberspace threats. Article 2 of the SCO Agreement defines the reach of these threats to encompass social, political, economic, spiritual, moral, and cultural spheres); African Union Convention on Cyber Security and Personal Data Protection art. 28, adopted June 27, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (This Agreement by the African Union focuses on e-commerce, secured transactions, and contracts in the African region with an additional provision on international cooperation for information exchange).

continue to be fragmented with varying views and without a centralized international institution or multilateral legal approach. Considering these extremes, this section examines how the existing WTO framework functions as a standard for most FTAs and discusses how major treaties deal with enforcement in cyberspace.

A. *Digital Trade and Cybersecurity in the WTO*

Trade agreements traditionally have exceptions for parties to take measures out of necessity. Because digital technology affects nearly every sector of trade, the necessity exception has sometimes been expanded to cybersecurity through a new "digital protectionism," where countries restrict cross-border data transfers and implement laws requiring data localization.[23] For example, even a good-faith measure taken to protect consumer personal information or a system to track exports can be vulnerable to malicious code or hacking, creating trade barriers. The WTO's "national security" exception under GATS Article XIV provides the most comprehensive explanation of how the necessity exception has been used and how it can be applied to cybersecurity. This section uses the example of the WTO to highlight how the security and general exception provisions common to most trade agreements are inherently inadequate to address cybersecurity.

1. WTO Security Exception and Why It Is an Inadequate Framework for Cybersecurity

The security exceptions in the General Agreement on Tariffs and Trade (GATT), the General Agreement on Trade in Services (GATS), and the Generic Access Profile (GAP) allow members to adopt measures for security purposes that would otherwise be inconsistent with their WTO obligations. This exception, though seemingly logical to apply to cybersecurity, was drafted during the Cold War in 1948, and defines "national security" as matters related to arms trafficking and fissionable material.[24] The security exception of the GATS Article XIV is as follows:

---

23. Ziyang Fan & Anil Gupta, *The Dangers of Digital Protectionism*, HARV. BUS. REV. (Aug. 30, 2018), https://hbr.org/2018/08/the-dangers-of-digital-protectionism; *Data Fortress: Digital Protectionism Embraced by Many in Asia*, NIKKEI ASIA (Feb. 11, 2023), https://asia.nikkei.com/Politics/Data-fortress-Digital-protectionism-embraced-by-many-in-Asia.

24. *See generally* Mona Pinchis-Paulsen, *Trade Multilateralism and U.S. National Security: The Making of the GATT Security Exception*, 41 MICH. J. INT'L L. 109 (2020).

> 1. Nothing in this Agreement shall be construed:
>
> (a) to require any Member to furnish any information, the disclosure of which it considers contrary to its essential security interests; or
>
> (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests:
>
> (i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment;
> (ii) relating to fissionable and fusionable materials or the materials from which they are derived;
> (iii) taken in time of war or other emergency in international relations; or
>
> (c) to prevent any Member from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.
>
> 2. The Council for Trade in Services shall be informed to the fullest extent possible of measures taken under paragraphs 1 (b) and (c) and of their termination.[25]

Until recently, this exception was not often used because parties were reluctant to cite "national security" as a factor for a dispute settlement test and because the exception could greatly affect trade.[26] However, because cybersecurity consists of a broad umbrella of risks from online hate speech to identity theft, many parties have cited "national security" as a cybersecurity justification to exert political control or protect domestic industries.[27] For example, China's cybersecurity law justifies limiting access to foreign firms due to a "national security" interest, and Vietnam's cybersecurity law prohibits "distorting history, denying revolutionary achievements, or destroying the fine

25. *See* General Agreement on Trade in Services art. XIV, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183.

26. Tania Voon, *Can International Trade Law Recover? The Security Exception in WTO Law: Entering a New Era*, 113 AM. J. INT'L L. 38, 45-50 (2019).

27. Meltzer & Kerry, *supra* note 10.

tradition and customs of the people, social ethics or health of the community."[28]

National security as a policy justification extends beyond the cybersecurity sphere. For example, in the United States, the Trump Administration used a national security rationale to justify tariffs on steel and aluminum imports.[29] However, the 2019 WTO panel in *Russia—Measures Concerning Traffic in Transit* clarified that the GATT national security exception is not subjective.[30] Rather, the WTO panel makes an objective assessment as to whether an event rises to the level of "an emergency in international relations."[31] Each WTO party member has the right to determine whether a cybersecurity measure is justified under the national security exception and the general exceptions.[32] However, the national security exception is ill-suited for dealing with cybersecurity problems in digital trade. This exception is not completely self-judging because it could be abused to disguise protectionism. As a result, any analysis is fact-specific and can vary widely.[33]

Cybersecurity, unlike traditional physical forms of security, presents the challenge of how to distinguish between legitimate security problems and disguised protectionism or trade restrictions. Given the WTO panel's definition of "national security" in the *Russia Transit* case, in addition to its definition of what constitutes an "emergency in international relations," and the temporal link required between them, the national security exception is not an available legal avenue for resolving cybersecurity issues in digital trade.[34] Cyber risks can originate from any country with an internet connection and throughout the entire global supply chain. Because cyber threats are continuous and require parties

28. *Id.*; Cybersecurity Review Measures (draft for comments, May 21, 2019), art. 10 (China); Law on Cybersecurity (June 12, 2018), art. 8(c), No: 24/2018/QH14 (Vietnam).

29. *Id.*

30. Panel Report, *Russia–Measures Concerning Traffic in Transit*, ¶¶ 7.64, 7.77, WTO Doc. WT/DS512/R (adopted Apr. 26, 2019).

31. *Id.*

32. General Agreement on Tariffs and Trade 1994 arts. XX, XXI, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187.

33. Panel Report, *Brazil–Measures Affecting Imports of Retreaded Tyres*, ¶ 7.341, WTO Doc. WT/DS332/R (adopted Dec. 17, 2007) (finding law banning imports of retreaded tires from WTO members not party to MERCOSUR were indeed about reducing environmental and health risks, rather than protecting domestic tire industry; however, the appellate body later reversed this ruling); Appellate Body Report, *European Communities–Measures Prohibiting the Importation and Marketing of Seal Products*, ¶ 5.338, WTO Doc. WT/DS400/AB/R, WT/DS401/AB/R (adopted June 18, 2014) (finding EU measure banning most imports and exports of seal products was a trade restriction rather than protecting animal welfare).

34. Meltzer & Kerry, *supra* note 10.

to adopt long-term measures to minimize risks, preventative measures are not considered to be actions "taken in time" of an "emergency in international relations." Therefore, the security exceptions found in the GATT, GATS, and GAP are insufficient to apply to the cybersecurity context.

2. General Exceptions in the WTO and Why They Are Inadequate Frameworks for Cybersecurity

The WTO's GATT Article XX and GATS Article XIV general exception provisions can be used to justify trade restrictions for cybersecurity under the supply chain exception or protection of human life or health exception. However, the WTO Appellate Body has found that to qualify for these general exception provisions, governments must ensure that their cybersecurity measures are necessary—that is, they are defined as the least restrictive measure—and that a less trade-restrictive alternative does not exist to provide the same level of protection from cyber threats.[35] Additionally, to qualify, governments must prove that their cybersecurity measures are not unjustifiable or a disguised trade restriction.[36]

The GATT and GATS general exception provisions, if invoked, would also be difficult to apply to the cybersecurity context. To invoke these exceptions, governments would have to prove that the cybersecurity action is the least trade-restrictive measure and that there are no less trade-restrictive alternatives available for the same level of protection. Additionally, a WTO panel would need to assess the impact of the measure on private sector incentives and determine whether alternative measures apply.[37] If the cybersecurity measure is taken under a broader set of actions to reduce cyber risk, the WTO Appellate Body would need to consider the overall system and its impact over time, which further complicates this analysis. The balance test also presents evidentiary requirements directing the burden of proof to fall on the complaining party to identify a less trade-restrictive alternative, which would be difficult if an action consisted of classified information.

3. WTO Exceptions in Free Trade Agreements (FTAs)

The security and general exception provisions in the WTO, as well as the many FTAs that follow WTO provisions, do not distinguish between

35. Appellate Body Report, *Brazil–Measures Affecting Imports of Retreaded Tyres*, ¶ 156, WTO Doc. WT/DS332/AB/R (adopted Dec. 17, 2007).

36. Meltzer & Kerry, *supra* note 10.

37. *Id.*

cyber risks arising from state and non-state actors and do not account for government measures meant to address economy-wide cyber risks.[38] Therefore, setting boundaries for government reach under the "national security" exception would first require a common global definition of the cybersecurity domain. As previously discussed, cybersecurity is a broad term that encompasses threats from both state and non-state actors, attacks on information and information systems, and impacts on public and private networks. Coupled with the narrow objective definition of necessity, the security exceptions in the GATT or similar "national security" exceptions in trade agreements are ill-suited to govern cybersecurity. These exceptions do not provide enough flexibility or a clear definition for parties to form cybersecurity policies and are not specific to digital trade. Additionally, given the proliferation of cyber threats, cybersecurity policies should be a priority in trade agreements, not governed by an exception to trade. Therefore, current multilateral trade agreements do not adequately address cybersecurity.

B. *Competing Theoretical Frameworks in Regional Trade Agreements*

There are multiple approaches to enhancing cybersecurity and protecting digital trade. Cybersecurity experts generally agree that "although states are not obliged to cooperate in the investigation and prosecution of cybercrime, such cooperation may be required by the terms of an applicable treaty or other international law obligation."[39] Even outside of the sphere of cybersecurity, international law includes a broad network of bilateral conventions for mutual cooperation in criminal matters.[40] Additionally, international agreements can also include mutual cooperation provisions that do not explicitly mention information security and data sharing, but may implicitly apply and attach when the specific activities are triggered. For example, the International Convention for the Suppression of Terrorist Bombings and the International Convention for the Suppression of Acts of Nuclear Terrorism both require parties to cooperate.[41] Statutes arising from international criminal tribunals and binding United Nations

38. *Id.*

39. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 75 (Michael N. Schmitt ed., 2d ed. 2017).

40. ANDREW K. WOODS, GLOB. NETWORK INITIATIVE, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET ERA 3–5 (2015).

41. International Convention for the Suppression of Terrorist Bombings art. 7(1–2), Dec. 15, 1997, U.N.T.S. 284; International Convention for the Suppression of Acts of Nuclear Terrorism art. 7(1)(b), Sept. 15, 2005, 1987 U.N.T.S. 125.

Security Council resolutions may also require cooperation.[42] Therefore, the notion of requiring mutual cooperation is neither new nor exclusive to cybersecurity.

However, jurisdiction in cyberspace consists of two extremes between mutual cooperation and data localization. On one end, as already adopted by multiple countries, is an integrated view of cyberspace, using existing international legal frameworks to allow disclosure of information held overseas. Western nations' mainstream approach involves framing the narrative around "cybersecurity," which can be defined as "the ability to protect or defend the use of cyberspace from cyberattacks" by the NIST[43] or "the protection of cyberspace itself [and] electronic information [from] either tangible or intangible . . . attacks originating in cyberspace."[44] In other words, cybersecurity is focused on control and compliance within the cybersphere with open information flow on a global scale. The other extreme is to reassert territorial control through data localization, which includes policies that play both facilitative and preventive roles.[45] This protectionist approach allows governments to use domestic procedures to both access data located within other countries and prevent definite access by other governments. The discourse on data localization, as taken by China, Russia, and some Arab countries, also focuses on protecting a nation's "digital sovereignty," the society, and the government from negative information flow.[46] In particular, China and Russia have been enacting horizontal data localization policies under domestic law to restrict data flow.[47] The disjointed approaches taken by countries, if they take any approach at all, could culminate in an arms race for internet jurisdiction. With these competing theories in mind, this Note argues that digital localization is ultimately unsustainable and disproportionately harms "developing" nations.

---

42. Rome Statute of the International Criminal Court arts. 86–87, 89, 91–93, July 17, 1998, 2187 U.N.T.S. 90; S.C. Res. 1593, ¶ 2 (Mar. 31, 2005); S.C. Res. 1970, ¶ 5 (Feb. 26, 2011).

43. U.S. DEP'T OF COMMERCE, NISTIR 8170, APPROACHES FOR FEDERAL AGENCIES TO USE THE CYBERSECURITY FRAMEWORK, app. B at 20 (2020).

44. Rossouw Von Solms & Johan Van Niekerk, *From information security to cyber security*, 38 COMPUT. & SEC. 97, 101 (2013).

45. Paul Greaves, *How African Countries Can Benefit From the Emerging Reform Initiatives of Cross-Border Access to Electronic Evidence*, CROSS BORDER DATA FORUM (July 6, 2020), https://www.crossborderdataforum.org/how-african-countries-can-benefit-from-the-emerging-reform-initiatives-of-cross-border-access-to-electronic-evidence/.

46. Julia Pohle & Thorsten Thiel, *Digital Sovereignty*, 9 INTERNET POL'Y. REV. 1, 8 (2020), https://policyreview.info/concepts/digital-sovereignty.

47. Stanislav Budnitsky & Lianrui Jia, *Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance*, 21 EUR. J. CULTURAL STUD. 594, 595 (2018).

1. Mutual Cooperation: The United States-Mexico-Canada Agreement (USMCA) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

Both the USMCA and the CPTPP, which created the framework for the Digital Economy Partnership Agreement (DEPA), create a comprehensive framework for digital trade. The USMCA adopts a "risk-based" approach to cybersecurity by "relying on census-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events."[48] The USMCA requires parties to adopt or maintain the legal framework for areas such as non-discriminatory treatment of digital products, electronic authentication and signatures, online consumer protection, and personal information protection.[49] The CPTPP contains an entire chapter devoted to electronic commerce. Article 14.16 on Cooperation of Cybersecurity Measures affirms the importance of cooperation on cybersecurity matters but does not create any obligations for the parties.[50] The remainder of the CPTPP chapter on cybersecurity discusses digital trade issues and creates minimum obligations for parties such as the non-discriminatory treatment of digital products, electronic authentication and electronic signatures, and personal information protection.[51]

Examples of mutual cooperation in the USMCA and CPTPP are best seen through code sharing. Specifically, both Agreements preclude parties from requiring code-sharing proposals related to "mass-market

48. *See* United States-Mexico-Canada Agreement art. 19.15(2), Nov. 30, 2018, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement ("Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.") [hereinafter USMCA].

49. *See* Chimene Keitner & Harry Clark, *Cybersecurity Provisions and Trade Agreements*, 10 HARV. BUS. L. REV. ONLINE 1, 2 (2019), https://repository.uchastings.edu/cgi/viewcontent.cgi?article=2764&context=faculty_scholarship.

50. Comprehensive and Progressive Agreement for Trans-Pacific Partnership art. 14.16, Mar. 8, 2018, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng ("The Parties recognise the importance of: (a) building the capabilities of their national entities responsible for computer security incident response; and (b) using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties.") [hereinafter CPTPP].

51. *Id.* art. 14.

software or products containing such software."[52] The USMCA explicitly prohibits parties from requiring disclosure of source code and goes further to bar governments from requiring the disclosure of "algorithms expressed in that source code" unless that disclosure was required by a regulatory body for a "specific investigation, inspection, examination enforcement action or proceeding."[53] This is important because parties and nations are interested in ensuring that the code running on their systems is free from malicious components.[54] For example, many cybersecurity experts have urged the U.S. Federal Communications Commission (FCC) to require all manufacturers of WiFi devices to ensure that their source code is "publicly available and regularly maintained" in response to the Volkswagen emission scandal, where computer code was left uninspected and allowed the company to cheat in its emissions testing.[55] In short, the USMCA and CPTPP are examples of trade agreements that are more in favor of mutual cooperation.

2. Data Localization: The Regional Comprehensive Economic Partnership (RCEP)

The RCEP promotes data localization rather than mutual cooperation. The RCEP permits parties to impose data localization requirements to achieve a public policy objective provided that the restriction is non-discriminatory.[56] The RECP specifically states, "The Parties recognise that each Party may have its own measures regarding the use or location of computing facilities, including requirements that seek to ensure the security and confidentiality of communications."[57] Furthermore, it states that the provisions do not prevent a party from adopting or maintaining any measures it subjectively judges to be a protection of essential security interests.[58] Other parties may only allege

52. *Id.* art. 14.17(1) ("No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory.").

53. USMCA art. 19.16.

54. Keitner & Clark, *supra* note 49, at 5.

55. Darlene Storm, *Vint Cerf and 260 Experts Give FCC a Plan to Secure Wi-Fi Routers*, COMPUTERWORLD (Oct. 14, 2015, 7:49 AM), https://www.computerworld.com/article/2993112/vint-cerf-and-260-experts-give-fcc-a-plan-to-secure-wi-firouters.

56. Regional Comprehensive Economic Partnership, art 12.14, Nov. 15, 2020, https://www.dfat.gov.au/trade/agreements/notyet-in-force/rcep/rcep-text-and-associated-documents [hereinafter RCEP].

57. *Id.* art. 12.14(1).

58. *Id.* art. 12.14(3).

that a measure is arbitrary, unjustifiably discriminatory, or a disguised restriction on trade, but they cannot claim that it does not pursue a legitimate public policy objective or that it is not necessary.[59] Finally, the RCEP encourages good-faith consultations between the parties and within the RCEP's Joint Committee, rather than creating a dispute mechanism.

C. *Why Trade Agreements Should Be Hesitant to Adopt Data Localization Articles*

Data localization is essentially the opposite of a trade agreement. The purpose of trade agreements is to reduce barriers in cross-border trade. While trade agreements can act as an incentive in foreign relations, punitive measures, such as sanctions and tariffs, can also motivate parties to negotiate trade agreements. However, cybersecurity and perceived cyber threats create incentives for nations to engage in trade-restrictive actions, absent a well-defined trade agreement, which counters general trade theory and cooperation.

Proponents of data localization often argue for the benefits of greater protection of privacy, protection of sensitive health information, and a higher standard for intellectual property protection.[60] However, data localization essentially permits foreign companies to work in a country only if they build out or lease costly separate data infrastructure in that country.[61] As a result, although data localization creates greater control for the country in which the business is operating, it limits access to global services for companies that are unable to create separate infrastructure or are unwilling to allow government access to data.

Both the USMCA and CPTPP recognize and call for strengthening the existing mechanism to cooperate and identify cyber threats among parties.[62] These present some of the clearest forms of digital data facilitation and intelligence cooperation. However, these U.S.-backed trade agreements' calls for intelligence sharing may be stunted if parties use equipment or platforms from China, a country that has often advocated

59. *Id.* art. 12.14.

60. *See* Michael Giest, *How the USMCA Falls Short on Digital Trade, Data Protection, and Privacy*, WASH. POST (Oct. 3, 2018. 3:02 PM), https://www.washingtonpost.com/news/global-opinions/wp/2018/10/03/how-the-usmca-falls-short-on-digital-trade-data-protection-and-privacy/.

61. *The Coming North American Digital Trade Zone*, COUNCIL ON FOREIGN RELS. (Oct. 9, 2018, 9:45 AM), https://www.cfr.org/blog/coming-north-american-digital-trade-zone.

62. USMCA art. 19; CPTPP art. 14.

for greater state sovereignty over data flow.[63] This contrast highlights a critical issue in multilateral trade agreements related to digital technology—a lack of consensus over state involvement and data localization.

III. Development: The Gap Between International Law and the Needs of "Developing" Countries

Cybercrimes have a disproportionate effect on "developing" countries, not only because of rampant cyberattacks but also because they rely on quickly evolving technologies. The rapid population and GDP growth in "developing" countries over the past two decades is linked to the liberalization of telecommunications, the widespread availability of mobile technologies, and the increasing availability of broadband systems.[64] However, this increasing reliance on technology raises cybersecurity concerns. "Developing" nations struggle with a lagging capacity to deal with cyberattacks, despite an increasingly digitalized infrastructure. Cyberattacks have often impacted financial services and private infrastructures.[65] Although some governments have alerted businesses and citizens of cyber threats, attacks remain rampant.[66] For example, Africa lost approximately USD $3.5 billion to cybercrimes in 2017.[67] Additionally, "developing" nations, especially those in the Arab region, are often targets of cybercrime because of the "significant gains, low risks, remote access, and the relative difficulty of assigning liability."[68] These issues are compounded by political instability, states prioritizing other problems, and a lack of digital culture among officials, all of which can create difficulty in ensuring that legislation passes.

Besides the prevalence of cybercrimes and the reliance on emerging technology in "developing" countries, these nations also struggle with enforcement because of (a) a lack of access to data, (b) a lack of

63. Intel Brief, *Could Huawei Signal the End of the "Five Eyes"?*, The Cipher Brief (Mar. 28, 2019), https://www.thecipherbriefcom/columnarticle/could-huawei-signal-the-end-of-the-five-eyes.

64. GSMA & A.T. Kearney, The Mobile Economy Report 2013, at 16 (2013), https://www.gsma.com/newsroom/wp-content/uploads/2013/12/GSMA-Mobile-Economy-2013.pdf.

65. UNESCAP Handbook, *supra* note 5.

66. *See* Landry Signé & Kevin Signé, *How African States Can Improve Their Cybersecurity*, Tech Stream (Mar. 16, 2021), https://www.brookings.edu/techstream/how-african-states-can-improve-their-cybersecurity/.

67. Serianu, Kenya Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line 11 (2017), http://www.serianu.com/downloads/KenyaCyberSecurityReport2017.pdf.

68. U.N. Econ. & Soc. Comm'n. for Western Asia (ESCWA), Policy Recommendations on Cybersecurity and Combating Cybercrime in the Arab Region 5 (Apr. 14, 2015), https://archive.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf [hereinafter UNESCWA Recommendations].

consensus over digital trade, (c) difficulties accessing enforcement tools, and (d) difficulties incorporating treaty provisions into domestic law. As a result, "developing" countries experience an overall disparity in combating cybercrimes.

A. *Issues with Access to Data*

"Developing" nations often cannot access data when investigating cybercrimes because evidence is often held by a foreign service provider, which usually requires that data requests be made through a bilateral mutual legal assistance treaty (MLAT). "Developing" nations are often unable to exercise extraterritorial production orders because they lack personal jurisdiction over service providers, as most are located in larger countries.[69] For example, U.S. law allows service providers to disclose data on a voluntary basis if requested by foreign law enforcement.[70] From the transparency reports of Facebook, Google, and Microsoft, African governments only made sixty-three requests in 2019, most of which were rejected.[71] In comparison, Facebook, Microsoft, and Google received 128,617, 45,956, and 75,650 data requests, respectively, from foreign law enforcement authorities in total in the same year.[72]

There are three reasons for this disparity. First, many "developing" nations lack MLATs in the first place. When prioritizing bilateral agreements, countries often prioritize agreements with countries holding the most electronic evidence, such as the United States, EU countries, and India, which creates a gap in mutual assistance for mid-sized to smaller countries.[73] As a result, criminal investigations in these countries often lack crucial evidence. Second, an enforcement agency might lack awareness of these request channels, assuming that the request would be ignored or take too long, or that there is a lack of substantive or procedural laws.[74] Third, this disparity is compounded because the more experience an internet service provider has with information requests from a particular country, the more the country's due process is authenticated.[75] Since smaller countries often do not make requests,

69. Greaves, *supra* note 45.

70. Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, U.S. DEP'T OF JUSTICE (Apr. 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

71. Greaves, *supra* note 45, at 6 nn.19-20.

72. *Id.*

73. *See id.*

74. *See id.*

75. *See id.*

the service provider has no similar basis for determining if due process standards are satisfied and is therefore more likely to reject the request. These factors contribute to access to data issues when investigating a crime.

B. *A Lack of Consensus Over Digital Trade*

The issue of state sovereignty over source code review for malicious content has been a source of ideological disagreement. On one hand, Western nations led by the United States, as seen in both the USMCA and CPTPP, have included provisions in trade agreements to preclude party access to source code.[76] As a result, businesses are left to negotiate their own source code verification provisions on a contract-by-contract basis, without government involvement in forming agreements to mandate access to source code.[77] On the other hand, China- and Russia-led initiatives for greater government sovereignty and extraterritorial jurisdiction have resulted in policies such as mandatory source code inspection.[78] IBM and Microsoft agreed to let the Chinese government inspect its code in a secure setting in 2015, resulting in Western criticism.[79] Similarly, IBM, Hewlett-Packard, McAfee, Cisco, and the German company SAP allowed Russia's Federal Security Service to inspect its source code through intermediary companies.[80] Without a coordinated approach to digital trade and cybersecurity, private businesses are left to negotiate their own terms. While digital trade provisions of the USMCA and CPTPP provide some feasible cooperation, trade wars and the fight for government sovereignty suggest that attempts at coordination in trade agreements are unlikely to create solutions with a global reach.

Although cooperation in mutual legal assistance in combating cybercrimes or incorporating digital trade in agreements exists between larger countries, the trickle-down effect on "developing" nations is even greater. While larger countries are in a position to either demand

76. CPTPP arts. 14.11-13; USMCA art. 19.16.

77. Keitner & Clark, *supra* note 49, at 6.

78. Samm Sacks & Manyi Kathy Li, *How Chinese Cybersecurity Standards Impact Doing Business in China*, CTR. FOR STRATEGIC & INT'L STUD. (Aug. 2, 2018), https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

79. *See* Bogdan Popa, *Microsoft, Intel, Others Oppose China's Plans to Get Access to Source Code*, SOFTPEDIA NEWS (Dec. 5, 2016), https:/news.softpedia.com/news/microsoft-intel-others-oppose-china-plans-to-get-access-to-sourcecode-510723.shtml.

80. *See* Greg Price, *U.S. Tech Companies Give Russia Secretive Source Codes to Stay in Multibillion-Dollar Market*, NEWSWEEK (June 23, 2017), https://www.newsweek.com/russia-us-tech-source-code-628589.

or circumvent source code inspection, "developing" nations do not hold the same power. In using platforms and services from "developed" nations, "developing" nations do not have the same bargaining power as China or Russia to demand source code inspection. Smaller countries highly rely on the technology platforms' services, lack alternative platforms, and only amount to a small percentage of a service provider's total income.[81] As a result, "developing" countries are subject to the service providers' promise of security and protection from the threat of malicious code. "Developing" countries do not hold the same power to preclude source code exchange when trading with larger nations for the same reason—a lack of bargaining power.

C. *Inadequate Access to Cybercrime Enforcement Tools*

Most training modules and legislation, if any at all, in "developing" countries are directly "copied and pasted" from Western legislation.[82] These models do not adequately capture the unique needs of "developing" countries. Additionally, "developing" nations often lack personnel and training programs to combat cybercrimes.[83] "Developing" nations often deal with a lack of cybercrime enforcement tools. These tools should describe immediate, nationwide actions with digital fallback alternatives should the government or private organizations experience a sudden loss of digital tools.[84] A country's enforcement plan must be context-dependent to account for "developing" nations' low income and lack of cybersecurity specialists to carry out a response plan.[85]

"Developing" nations often lack the infrastructure to deal with cyber threats. Compared to "developed" nations, "developing" nations notably lack data protection legislation, breach notification measures, legislation on the theft of personal information, legislation on illegal access, and legislation on online harassment.[86] Additionally, "developing" nations lag in having national Computer Incident Response Teams (CIRTs) or Computer Emergency Response Teams (CERTs) and sector-specific CERTs, as well as total spending in its CIRT if it has one.[87]

---

81. Paul Mozur et al., *A Global Tipping Point for Reigning in Tech has Arrived*, N.Y. TIMES (Apr. 20, 2021) https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html.

82. Catherine Chapman, *How Africa is Tackling its Cybersecurity Skills Gap*, DAILY SWIG (Aug. 22, 2018), https://portswigger.net/daily-swig/how-africa-is-tackling-its-cybersecurity-skills-gap.

83. *Id.*

84. *See* Signé & Signé, *supra* note 66.

85. *Id.*

86. ITU, GLOBAL CYBERSECURITY INDEX 2020, at 4-8 (2021), https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/.

87. *Id.*

D. *Issues with Local Legislation on Cybercrime*

Trends show that legal texts on cybercrime, if a country even has legislation at all, are not codified under one law but are instead spread out among penal codes, information technology laws, and criminal procedure laws.[88] Additionally, existing legislation often focuses more on criminalizing cybercrime than on procedural aspects such as evidence collection and international cooperation.[89] Because "developing" countries often prioritize legislation connected with economic growth, as seen in the Malabo Convention,[90] these countries have been slow to update both substantive and procedural laws relating to cybercrime.

E. *The Gap in Cybersecurity for "Developing" Nations*

As discussed in the introduction, "developing" nations are especially vulnerable to cyberattacks because they have less developed cybersecurity laws, major service providers are often located in "developed" nations, and the countries tend to focus on certain areas of economic growth instead of combating cyber threats. Compounded by rampant cyberattacks, "developing" countries are at a disadvantage in protecting their cybersphere.

IV. Trade: What Multilateral Treaties Should Incorporate as Their Focus

The challenges created by existing trade agreements and the cybersecurity issues among "developing" nations highlight reasons why new trade rules are needed. In an ideal world, parties would negotiate a multilateral trade agreement under the WTO or a similar agreement. However, government respect for sovereignty in the form of data localization and national security has shown that such an agreement would be unlikely. While trade agreements like the USMCA, CPTPP, and DEPA offer a starting point for mutual cooperation in digital trade, these Agreements are limited by region. Because of the gaps for "developing" nations created by the current frameworks, this section offers three recommendations for trade agreements: (a) to develop global

88. UNESCWA Recommendations, *supra* note 68.

89. *Id.*

90. Yohannes Eneyew Ayalew, *The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly After a Decade. What Does it Mean for Data Privacy in Africa or Beyond?*, EJIL Talk (June 15, 2023), https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/.

cybersecurity standards through best practices, (b) to develop compliance mechanisms, and (c) to call for access to data and information sharing.

A. *Global Cybersecurity Standards*

First, parties need to create common cybersecurity standards based on best practices. This could include common security features and a task force tasked with developing relevant standards. As previously discussed, some countries prioritize sovereignty, while others prioritize access. A framework for identifying which policies are effective for managing risks would be particularly helpful for "developing" nations. Because "developing" countries typically have a greater focus on sectors such as financial banking or trade, their government agencies often lack the specialization to understand cybercrime, contributing to an ineffective system.[91] A task force to implement best practices could help "developing" countries establish an agency with a cyber specialization. Trade agreements could then be used to reinforce the role of consensus-based standards by developing commitments for domestic regulation.[92] In short, creating international standards could support developing globally consistent, least trade-restrictive approaches to cybersecurity, as well as provide legislative guidance and local research data for parties with less developed cybersecurity regulations.

B. *Compliance Mechanisms*

Although regional conventions on cybersecurity can be useful and offer a more in-depth framework to combat cyber threats, conventions like the Budapest Convention lack compliance mechanisms.[93] Trade agreements can encourage parties to regularly self-assess their progress while minimizing the burdens they impose on trade by requiring governments to allow other parties to undertake conformity assessments in the country of export. "Developing" countries often lack the bargaining power to ensure internet service providers and exporters of digital trade comply with local standards, therefore exposing "developing" countries to greater cyber threats.

---

91. Meltzer & Kerry, *supra* note 10.

92. *Id.*

93. Cybercrime Programme Office (C-PROC) of the Council of Europe, CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region (PMM 2088) 2 (2021), https://rm.coe.int/2088-cybereast-summary-and-workplan-v9/1680a4db77.

Compliance mechanisms could also help countries deal with issues of judicial specialization. This is important for two reasons. First, because of a greater focus on sectors such as financial banking or trade, government agencies often lack specialization in understanding cybercrime, which creates an ineffective system. Second, because cybercrimes are often cross-border, prosecuting a crime often requires working with Western-centric legal systems.[94] The judicial systems in "developing" nations often lack expertise in foreign legal systems, most of which are more specialized in combating cybercrime because they have more cases and personal jurisdiction over internet service providers. As a result, reliance on global standards may help countries have more bargaining power in disputes over where judicial proceedings should take place and will place enforcement agencies in a better position when negotiating.

C. *Access to Data and Information Sharing*

Finally, mutual cooperation in cybersecurity requires real-time sharing of information on threats to promote awareness, plan responses, and adapt. Some trade agreements, such as the CPTPP and USMCA, and conventions, such as the Budapest Convention and Malabo Convention, have listed commitments to information flow to avoid data localization requirements.[95] Additionally, trade agreements need to include commitments to improve information sharing with international partners and within supply chains by committing to public and private sector information-sharing mechanisms. The following sections provide two examples of how such tools can benefit "developing" nations.

For example, trade agreements expedite information sharing by encouraging governing systems to act as authenticating organizations between countries, similar to correspondent banking transactions.[96] The correspondent banking transaction model[97] would use regional organizations or Cyber Emergency Response Teams (CERTs) to authenticate a country. In correspondent banking transactions, a smaller Bank A in Country X would not have a direct relationship with smaller Bank D in Country Y. To make a payment, Bank A would utilize its relationship with large Bank B in Country X, which has an existing relationship with large Bank C in Country Y.[98] In applying this model to

94. UNESCWA RECOMMENDATIONS, *supra* note 68.
95. CPTPP arts. 14.11-13; USMCA, arts. 19.11-12.
96. Greaves, *supra* note 45.
97. *Id.*
98. *Id.*

cross-border data sharing, a regional organization or CERT can act as a large bank on behalf of "developing" countries in the region.[99] The regional organization can enter into bilateral agreements with small, individual countries and act as a point of contact to authenticate the requests from these small countries.[100] This approach bypasses the costs for individual nations to create legislation, local procedures, and bilateral agreements.

D. *Mutual Cooperation in Cybersecurity*

All the above-mentioned areas of improvement for trade agreements—creating global compliance standards, compliance mechanisms, and access to data—focus on mutual cooperation. Due to an increasing gap in cybersecurity between "developed" and "developing" countries, and due to the pervasiveness of cyber threats, there is an even greater need for mutual cooperation. A data localization model would merely further drive "developing" countries to combat threats alone.

V. Conclusion

Increasing digital connectedness and interdependence in trade makes it necessary that regulatory barriers to cooperation be impermeable. In recent years, countries have increasingly relied upon digital trade. However, with this reliance comes a greater number of cyber threats. These issues have been exacerbated by the COVID-19 pandemic, and trade agreements are not well-equipped to deal with cybersecurity. Although the WTO and many traditional FTAs carve out exceptions for necessity and security, cyber threats should be dealt with on their own, rather than as an exception for governments to act. Additionally, regional trade agreements have highlighted the ideological differences between mutual cooperation and data localization in trade. The myriad issues "developing" nations deal with, in particular—access to data, lack of consensus over how digital trade should be framed, lack of enforcement tools, and underdeveloped local legislation—have proven the need for greater mutual cooperation. In a world of "developing" countries rapidly turning to digital trade for all their transactions, cybersecurity must be a primary, if not a paramount, consideration in trade agreements.

99. *Id.*
100. *Id.*