GLOBAL ECONOMY & DEVELOPMENT
WORKING PAPER 132 | November 2019

Global Economy and Development at BROOKINGS

# Cybersecurity and digital trade

## What role for international trade rules?

Joshua P. Meltzer

**Joshua P. Meltzer** is a senior fellow and lead of the Digital Economy and Trade Project in the Global Economy and Development program at the Brookings Institution

**Acknowledgements**

The author would like to thank Tania Voon for helpful comments.

# Cybersecurity and digital trade: What role for international trade rules?

Joshua P. Meltzer

Working Paper #132
Global Economy and Development
Brookings Institution

# Introduction

Trade and cybersecurity are increasingly intertwined. The global expansion of the internet and increased use of data flows by businesses and consumers—for communication, e-commerce, and as a source of information and innovation—are transforming international trade.[1] The spread of artificial intelligence, the "internet of things," (IoT) and cloud computing will accelerate the global connectivity of businesses, governments, and supply chains.[2]

As this connectivity grows, however, so does our exposure to the risks and costs of cyberattacks.[3] As the President's National Security Telecommunications Advisory Council observed, the U.S. is "faced with a progressively worsening cybersecurity threat environment and an ever-increasing dependence on internet technologies fundamental to public safety, economic prosperity, and overall way of life. Our national security is now inexorably linked to cybersecurity."[4]

Not only are traditional defense and other national security targets at risk of cyberattack, so too is the broader economy. This includes critical infrastructure—such as telecommunications, transport, and health care—which relies on software to network services. There is also cybertheft of intellectual property (IP) and manipulation of online information. More broadly, these risks undermine business and consumer trust in the internet as a basis for commerce and trade.[5]

Many countries are adopting policy measures to respond to the threat.[6] According to one estimate, at least 50 percent of countries have adopted cybersecurity policies and regulations.[7] Some of these policies recognize a need for international cooperation: the EU identified "a need for closer cooperation at a global level to improve security standards, improve information, and promote a common global approach to network and information security issues … "[8] and the most recent U.S. Cybersecurity Strategy reaffirms the need to "strengthen the capacity and interoperability of those allies and partners to improve our ability to optimize our combined skills, resources, capabilities, and perspectives against shared threats."[9]

Cybersecurity policy is also increasingly risk-based, requiring governments, organizations, and businesses to assess the risk of attack, determine potential harm, and develop appropriate measures to reduce the risk or impacts.[10] This includes addressing cybersecurity risk over

[1] Meltzer, Joshua P. "Governing Digital Trade." Vol. 18, Special Issue S1 World Trade Review (April 2019), 1-26.
[2] Michael Ferentina and Emine Elcin Koten 2019, "Understanding supply chain 4.0 and its potential impact on global value chains", in Global Value Chain Development Report 2019 (WTO, IDE-JETRO, OECD, UIBE, World Bank).
[3] Ben Ze Yuan, "An Abbreviated Technical Perspective on Cybersecurity", in Perspectives on Cybersecurity: A Collaborative Study, Eds. Nazli Choucri & Chrisma Jackson, MIT 2015.
[4] NSTAC, Report to the President on a Cybersecurity Moonshot, Draft.
[5] Symantec Internet Security Threat Report, April 2019.
[6] OECD 2012, "Cybersecurity Policy Making at a Turning Point" (OECD Paris 2012).
[7] ITU Global Cybersecurity Index 2017.
[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[9] White National Cybersecurity Strategy 2018.
[10] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, p. 6-8; OECD (2015), Digital Security Risk Management for Economic and Social Prosperity.

global supply chains. Some proposed measures are likely to constitute barriers to data flows and digital trade. These include data-flow restrictions, data-localization requirements, and import restrictions on information technology (IT) products, including software from countries or supply chains where cyber risk is high. Countries may also resort to import restrictions including higher tariffs as a means of punishing and deterring cyberattacks.

By treating goods, services, or data from high-risk countries less favorably than those from countries where cyber risk is lower, cybersecurity measures may violate various World Trade Organization (WTO) and free trade agreement (FTA) commitments. Where a government is in breach of such commitments, they can seek to justify the cybersecurity regulations under the security or general exception provision of the relevant treaty.

Until recently, governments have largely avoided relying on the security exception to justify trade restrictions. There had been no WTO case dealing with the security exception provision prior to 2018. This was largely because of the potential for abuse of this provision to justify trade restrictions. However, changes in the global security environment, in particular the end of the notion that major powers would converge and stop treating each other as rivals,[11] has revealed once again that economic integration can be a source e of vulnerability,[12] Digital connectivity over the internet and through cross-border data flows has expanded opportunities for trade and integration more broadly. In parallel, this has created vulnerability to cyberattacks. This includes use of cyber methods to attack another government's defense and industrial base, or steal its IP or trade secrets or manipulate online information to sow discord.

These developments are underpinning a broader turn by governments to economic instruments to promote or defend what are seen as national security, leading to greater reliance on the WTO security exception to justify these measures.[13] The Trump administration's reliance on national security to justify tariffs on steel and aluminum, and potentially on imports of automobiles, points to this trend. U.S. tariffs on Chinese imports is also in part an effort to deter Chinese cyber theft of U.S. IP and trade secrets.[14] This administration is not alone in resorting to security to justify trade barriers. Russia relied on a WTO security exception to justify restrictions on the transit of Ukrainian goods and services, leading to the first WTO case on the security exception. The UAE is also using the WTO security exception to justify trade restrictions with Qatar as part of its broader dispute.

The rising need for cybersecurity creates two distinct challenges for the rules-based trading system. The first is the role of the security or general exceptions provision in the WTO and in FTAs in distinguishing between genuine cybersecurity measures taken by governments and those that are merely disguised protectionism. The second is that as economies become more digital and connected, there is likely to be significant growth in trade restrictions for legitimate cybersecurity purposes.

---

[11] Tom Wright, "All Measures Short of War." Yale University Press, 2017.
[12] White House. "United States National Security Strategy." December 2017. www.whitehouse.gov/wp-content/uploads/2017/12/NSSFinal-12-18-2017-0905.pdf.
[13] Robert D. Blackwill and Jennifer M. Harris, War by Other Means, Geoeconomics and Statecraft", Harvard University Press 2016, p. 20
[14] S.301 Report

As discussed in this paper, the WTO security exception was designed to address a more traditional set of security measures: it is not well designed to deal with measures that restrict trade to address cybersecurity risk. In particular, the approach in the WTO to determining what is a security issue, and the requirement that security measures be taken in response to a security issue, is at odds with how governments are responding to the diffuse, longer-term nature of cyber risk. FTA security exceptions provide more flexibility. Yet here, the risk is that growth in cybersecurity regulation will blow a hole in FTA digital trade commitments.

The alternative to relying on the security exception is to justify cybersecurity regulation under the WTO and FTA general exceptions. Yet, governments are unlikely to tolerate the higher levels of third-party scrutiny that goes with seeking to justify what they see as increasingly important security measures. Moreover, the complexity of the issues, and the mix of economic and security concerns that leads government to rely on classified information, will present significant hurdles to using the general exceptions provision as a way to discipline disguised protectionism.

Addressing these issues requires a new way of thinking about the trade rules for cybersecurity. What is needed is a more fine-grained understanding of the types of cybersecurity risk. Consideration should be given to developing a new set of cybersecurity-specific trade rules.

It is also necessary to build cooperation on cybersecurity: this paper outlines areas where this can happen, including around sharing and access to data and the development of cybersecurity standards. Indeed, where the ethics of cybersecurity are about reducing harm and building trust, cybersecurity can be a vital part of the digital economy and trade. Yet, in the absence of cooperation, cybersecurity risks becoming a core organizing principle for the digital economy, leading to increasing trade with trusted partners and less exposure to countries presenting cyber risk.

This paper proceeds as follows:

- Part 1 outlines the importance of data and the internet for economic growth and international trade, including with respect to the fifth generation of cellular network technology (5G).
- Part 2 discusses what cybersecurity is, its components, and various risks to national security and the economy.
- Part 3 provides an overview of the cybersecurity polices of the U.S. and China.
- Part 4 discusses how international developments have affected the interaction between security and trade and how cybersecurity creates new risks from integration.
- Part 5 outlines how the WTO and FTA security exception and general exception apply to cybersecurity and where the current internal trade law framework falls short in relation to cybersecurity.
- Part 6 makes the case for new trade rules on cybersecurity and provides some initial thoughts on what these might comprise, such as commitments to basing cybersecurity measures on a risk assessment.
- Part 7 concludes the paper.

# 1. Development of the digital economy and digital trade

Growth in the production and use of data is at the core of the digital economy. This includes the digitalization of broad areas of industry and services. Understanding the scope of the of the digital economy and how data and emerging technologies such as AI are transforming international trade, highlights the economic, social and political stakes, as well as the potential cybersecurity risks.

According to the U.S. Bureau of Economic Analysis (BEA), the United States digital economy in 2017 was valued at almost $1.5 billion, accounting for 6.9 percent of total GDP and representing the 7th largest sector.[15] The BEA included in its measure the enabling infrastructure such as computer hardware, software, telecommunications equipment, (2) e-commerce which includes business to business (B2B) and business to consumer (B2C) and (3) digital content such as digital media and big data. Globally, UNCTAD estimates that e-commerce was worth $25 trillion in 2015 and McKinsey estimates that in 2014, cross border flows of data were worth more than global trade in goods.[16]

The digital economy and emerging technologies rely on the global flow of data for innovation and access to hardware and software for production and delivery. Take artificial intelligence (AI)—a data-driven technology which could add trillions of dollars to global output over the next 10 years and accelerate the transition towards a services-driven global economy.[17] The McKinsey Global Institute estimates that AI could add around 16 percent, or $13 trillion, to global output by 2030.[18] AI requires access to large data sets as machine learning needs to incorporate as many past outcomes as possible into future predictions.[19] Data also increasingly resides in the cloud—which comprises globally distributed data centers that move data to users and to other data centers for backup and security. In 2014, cross-border data flows were valued at around $2.8 trillion—more than the global trade in goods.[20]

Global data flows are also enabling the delivery of goods and services online, both direct-to-consumer and business-to-business within global value chains. Already, around 12 percent of global goods trade is via international e-commerce.[21] According to a 2019 U.N. Conference on Trade and Development (UNCTAD) report, e-commerce globally was worth $29 trillion in 2017, with around 1.3 billion people shopping online—up 12 percent from the previous year.[22]

---

[15] Kevin Barefoot et al, "Measuring the Digital Economy", Survey of Current Business, The Journal of the U.S. Bureau of Economic Analysis, Vol 99, No. 5, May 2019.
[16] McKinsey & Company (2016), Digital Globalization: The New Era of Global Flows, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.
[17] Jacques Bughin et al. "Notes from the AI Frontier, Modeling the Impact of AI on the World Economy," *McKinsey Global Institute Discussion Paper*, September 2018. Paul Daugherty and Mark Purdy. "Why AI is the Future of Growth?" 2016. https://www.accenture.com/t20170524T055435__w__/ca-en/_acnmedia/PDF-52/Accenture-WhyAI-is-the-Future-of-Growth.pdf.
[18] Jacques Bughin et al. "Notes from the AI Frontier, Modeling the Impact of AI on the World Economy." *McKinsey Global Institute Discussion Paper*, September 2018.
[19] Generative adversarial networks or use of digital twins can minimize need for large data sets to train AI.
[20] McKinsey & Company. 2016. *Digital globalization: The New Era of Global Flows*. 2016. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-ofglobal-flows.
[21] McKinsey & Company. *Digital globalization: The New Era of Global Flows*. 2016. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-ofglobal-flows.
[22] UNCTAD. "Global e-commerce sales surged to $29 trillion." 2019. https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2034.

E-commerce also provides a potentially significant opportunity to increase small business participation in international trade.[23] For instance, having a website gives small businesses an instant international presence without having to establish a physical presence overseas. In addition, the internet provides access to advertising and communication services, as well as information on foreign markets—all of which help small businesses participate in international trade.[24] In the U.S., for instance, 97 percent of small businesses on eBay export, compared to 4 percent of offline peers.[15] Similar results play out across developed and developing countries. The emerging technologies that rely on global data flows are themselves also supporting digital trade applications. For example, eBay's machine translation service has increased eBay-based exports to Spanish-speaking Latin America by 17.5 percent.[25] According to the WTO, using digital technologies to reduce trade costs could increase world trade by up to 34 percent by 2030.[26] This includes using digital technologies to reduce transport by increasing the efficiency of logistics, using robots to optimize storage and inventory, and using blockchain to facilitate customs processing. For example, by using AI, businesses are improving the management of supply chain risk, developing smart manufacturing, and using AI language translation services to increase exports to countries where language was a barrier to commerce.[27]

Internet access and cross-border data flows are also increasing services trade.[28] Services can increasingly be purchased and consumed online. This is particularly true for IT, professional, financial, retail, and education services.[29] Many of the emerging technologies delivered online are themselves services. Cloud computing, for instance, offers software, applications, and IT infrastructure as a service.[30]

Data collection and analysis are adding value to goods exports through so-called "servicification." Data flows enable digitization of the entire manufacturing enterprise, shorter production cycles and collaborative and connected supply chains.[31] For example, data collected from sensors attached to mining and farming equipment allow businesses to improve their operations, thereby adding value. This also applies to commercial services such as research and development (R&D), design, marketing, and sales. A 2016 PricewaterhouseCoopers survey of more than 2,000 companies identified data and data analytics as the key to a successful transformation toward smart manufacturing.[32] This reflects the importance of digital services for increasing productivity, which affects the capacity of firms

---

[23] Meltzer, Joshua P. "Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-Sized Enterprises and Developing Countries." *Brookings Working Paper,* 69, February 2014.
[24] OECD. "Top Barriers and Drivers to SME Internationalization." *Report by the OECD Working Party on SME and Entrepreneurship.* Paris: OECD Publishing, 2009.; Schoonjans, Bilitis, Van Cauwenberge, Philippe and Heidi Vander Bauwhede et al. Formal Business Networking and SME Growth. *Small Business Economics.* 41, 2013. [15] Ebay. "Empowering People and Creating Opportunity in the Digital Single Market" An eBay report on Europe's potential, October 2015.
[25] Brynjolfsson, E, X Hui and Meng Liu. "Does Machine Translation Affect International Trade? Evidence from a Large Digital Platform." 2018.
[26] WTO Trade Report 2018.
[27] Brynjolfsson, E, X Hui and Meng Liu. "Does Machine Translation Affect International Trade? Evidence from a Large Digital Platform." *National Bureau of Economic Research Paper*, 2018.
http://ide.mit.edu/sites/default/files/publications/Machine_Translation_NBER.pdf.
[28] Aaditya Mattoo and Sacha Wunsch-Vincent, "Pre-empting Protectionism in Services: The GATS and Outsourcing", Journal of International Economic Law 7(4), 2004.
[29] United States International Trade Commission. *Digital Trade in the U.S. and Global Economies, Part 2*. Investigation 332-540, Pub. No.4485, August 2014, p. 42.
[30] United States International Trade Commission. *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*. Pub. No 4716, August 2017, pp. 58-66.
[31] L. Yu, et al. "Current Standards Landscape for Smart Manufacturing Systems." *NIST*, NISTIR 8107, February 2016.
[32] PricewaterhouseCoopers 2016. Industry 4.0: Building the digital enterprise. 2016 Global Industry 4.0 Survey.

to compete domestically and overseas.[33] In fact, taking account of the value of services embedded in goods exports, such as the design, professional service, and IT contributions to manufactured goods, services make up over 55 percent of total EU exports.

Global data flows underpin global value chains (GVCs), creating new opportunities for participation in international trade.[34] For many economies, participation in GVCs is the deciding factor for trading internationally. More than 50 percent of trade in goods and over 70 percent of trade in services is in intermediate inputs.[35] Data and digital technologies are affecting GVC participation in several ways. The development of these value chains has been enabled by global connectivity and cross-border data flows that facilitate communications and can be used to coordinate logistics.[36] Global data flows are also enabling so-called "supply chain 4.0"—where information flows are integrated and omnidirectional instead of linear.[37] Integrated information flows enabled by supply chain 4.0 are creating new opportunities to enhance productivity and expand employment opportunities. There is also a trend towards increasing the use of imported service inputs in manufactured goods exports, suggesting that digital services are being traded within GVCs as well.[38] This includes allowing small- and medium-size enterprises to offer their own specific service within global value chains or to strengthen more traditional e-commerce offerings. Global data flows have also allowed digital platforms to source key digital services across borders, creating entirely digital value chains. The digital supply chain of Gojek, an Indonesian ride-sharing platform, includes a cloud-based company from Singapore, a payment service based in Singapore and New York, and mapping service and software interfaces from Silicon Valley.

Looking ahead, the deployment of 5G networks and technologies will lead to a step change in the growth of the digital economy and digital trade. 5G will improve data speed and volume, enabling the expansion of new technologies, including autonomous vehicles, virtual reality, and health applications.[39] It will also enable a massive expansion of IoT—the connection of billions of devices, from homes to factories to the network. Cisco estimates that 500 billion devices will be connected to the internet by 2030.[40]

The development of 5G will require investment in cell towers and new equipment, but its most transformative impact will be in bringing faster processing speeds and increased network functionality. The Internet Protocol will be used in network architecture as well as by the applications that run on it. 5G will effectively turn everything into data as everything becomes an IP app.[41] This will make 5G software-focused, allowing the network to be updated using software patches. It will also enable "network slicing,"—separating different service layers on

---

[33] Hoekman, B. and Aaditya Mattoo. "Services Trade and Growth." *Policy Research Working Paper* No. 4461, Washington DC: World Bank 2008.; Liu, Xuepeng, Aaditya Mattoo, Zhi Wang, and Shang-Jin Wei. 2017. "Services Development and Comparative Advantage in Manufacturing." Unpublished manuscript.
[34] Baldwin, R. "The Great Convergence: Information Technology and the New Globalization." Boston: Harvard University Press. 2016.
[35] OECD. "Mapping Global Value Chains", TAD/TC/WP/RD(2012)9. 2012.
[36] Helpman E. "Understanding Global Trade." Cambridge, Mass: Harvard University Press. 2011.
[37] Michael Ferentina and Emine Elcin Koten 2019, "Understanding supply chain 4.0 and its potential impact on global value chains", in Global Value Chain Development Report 2019 (WTO, IDE-JETRO, OECD, UIBE, World Bank)
[38] Miroudot S., Charles Cadestin. Services in Global Value Chains: From Inputs to Value-Creating Activities." *OECD Trade Policy Paper 197*, p. 16. 2017.
[39] Milo Medin and Gilman Louie, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD", Defense Innovation Board, April 2019.
[40] Cisco, Internet of Things, At-a-Glance, https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf.
[41] Tom Wheeler, 5G in five (not so) easy pieces, Brookings Report, July 9, 2019.

the same network—making it possible to offer differentiated services over the network. As 5G becomes software in the cloud, this will also move functionality from the core to the edge of the network.

# 2. Cybersecurity and the digital economy

The growth in data and the digital economy creates new and potentially costly risks of cyberattack. The following outlines what cybersecurity is, the risks it presents, and government responses.

### What is cybersecurity?

There is no common agreed definition of cybersecurity. However, the International Telecommunication Union broadly defines it as,[42]

> *"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. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. 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."*

The U.S. National Institute of Standards and Technology (NIST) provides a more focused definition. It defines cybersecurity as "the 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."[43] In turn, the White House National Cyber Strategy focuses on increasing the security and resilience of the nation's information and information systems.[44]

This definition reflects two key targets of cyberattacks: information and information systems. It does not differentiate between action by states or criminals, or between cyberattacks' impact on public vs. private information, networks, and infrastructure. Thus, for example, it includes Russian use of false accounts to seed false information, as well as the NotPetya cyberattack that used malware to disable Ukraine's energy infrastructure systems.[45] Critically, this focus on the integrity of information and information systems does not encompass broader purposes such as the development of national industries, preserving access to information on citizens

[42] ITU definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity.
[43] NISTIR 7298, Revision 3, "Glossary of Key Information Security Terms", July 2019.
[44] White House National Cybersecurity Strategy, September 2018.
[45] Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, August 2018.

for law enforcement agencies, regulation of information content, or social controls that are not directly related to these core elements.

## What are the cybersecurity risks for the digital economy and global data flows?

There are four key areas of cyber risk with implications for global data flows in a digital economy. The first is the national defense space, including all branches of the military and intelligence services. These vulnerabilities include the defense infrastructure, networks, and related software, as well as classified information stored on the networks. The second is critical infrastructure. The third area includes trade secrets and IP with commercial value. The fourth area of vulnerability includes other online information.

The aim of this classification is to distinguish the types of cyber risks and the kind of rules that may be applicable to each area seeking to enhance cybersecurity while maximizing the economic and social benefits of the internet and global data flows. For instance, there are likely higher risks of cybersecurity for national defense, but some critical infrastructure such as energy or communications may have similar risk profiles. The harms from economic cyber-espionage accrue over time and have longer term security implications. Governments may also use trade restrictions to punish or deter cyber-espionage: this is cited as one of the reasons for the U.S. raising tariffs on imports from China.[46] However, not all such spying will have a national security edge and risks will change over time.

*National defense*

One area of risk is the use of cyberattack to hack into the defense industry.[47] This comprises defense capabilities which, in the U.S., would include the Department of Defense (DoD) and all national security agencies and contractors providing military equipment. For instance, the U.S. has experienced cyber theft of data related to the development of various fighter aircraft, including the F-35 Joint Strike Fighter, the F-22 Raptor, and the MV-22 Osprey.[48] A range of actions are taken in the defense sector to secure such information. There are also measures aimed at reducing risk from acquiring goods and services from third parties. In this respect, the DoD has developed rules aimed at reducing cyber risk in the procurement process stemming from the insertion of bad software or other products along the supply chain which end up in national security systems.[49]

*Critical infrastructure*

As infrastructure in various sectors—from water to energy to transport—becomes digitally networked, the potential for cyberattacks that cause large-scale shutdowns and other harm has also increased. For example, the NotPetya cyberattack on the Ukrainian power network caused power outages. Ransomware that blocks access to data led hospitals in the U.K. to cancel medical procedures and divert patients to other hospitals. [50] The USA PATRIOT Act

---

[46] Office of the United States Trade Representative. Findings of the investigation into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under Section 301 of the Trade Act of 1974. Washington, DC: Office of the United States Trade Representative, 2018. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.
[47] The Honorable James Clapper, The Honorable Marcel Lettre & Admiral Michael S. Rodgers, Joint Statement for the Record to the Senate Armed Services Committee, "Foreign Cyber Threats to the United States", 5 January 2017
[48] Id.
[49] Enhanced Procedures for Enterprise-Wide Use of Section 806 Supply Chain Risk Management Authorities for DOD National Security Systems.
[50] EU Coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, October 9, 2019

defines critical infrastructure as "(t)hose systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters."[51] This definition was referenced in Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and the NIST Framework for Improving Critical Infrastructure Cybersecurity.[52]

Vectors of attack on critical infrastructure include IT, industrial control systems, cyber-physical systems, and connected devices.[53] Critical infrastructure will include the 5G network as it supports key services such as health, energy, and transport. This means that a disruption to the 5G network could cut off access to essential services.[54] In the network supply chains, this includes radio frequency (RF) components, integrated chipsets, as well as the devices and services using the network. Reliance on global suppliers—many are from China—creates supply chain risk.[55] Accessing 5G through software allows governments to include back doors that can be used to control a system or steal information.[56] Even if it is possible to confirm initial software is safe, future releases and patches can compromise security. IoT devices are also vulnerable, including to botnet denial-of-service attacks. The vast amount of data that will traverse the 5G network presents opportunities to access and undermine the integrity, confidentiality, and privacy of information. Moreover, it will increase the challenge of detecting malicious traffic.

*Economic cyber-espionage*

Malicious actors can also use the internet to hack into commercial enterprises,[57] stealing trade secrets and IP. Cyber-espionage will erode America's longer term economic advantage.[58] The U.S. has identified cyber-espionage taking place across all the country's major economic sectors, including energy, biotechnology, environmental protection, high end manufacturing, and telecommunications.[59] Such espionage is often focused on theft using malicious software and access to cloud-based data. There are also supply chain opportunities to insert malware into software. For example, CCleaner software, used to optimize computers, was corrupted with a backdoor that infected computers with access to trade secrets from Intel, Samsung, Sony, and Fujitsu.[60]

*Digital information*

Online information can be falsified and manipulated to create confusion and distrust.[61] This would include, for example, in the lead-up to the 2016 U.S. Presidential election, Russia's use

---

[51] USA Patriot Act of 2001, (42 U.S.C. §5195c(e)).
[52] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[53] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, p. 1.
[54] EU Coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, October 9, 2019
[55] Milo Medin and Gilman Louie, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD", Defense Innovation Board, April 2019, p. 23.
[56] EU Coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, October 9, 2019, p. 19; Milo Medin and Gilman Louie, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD", Defense Innovation Board, April 2019, p. 24.
[57] The Honorable James Clapper, The Honorable Marcel Lettre & Admiral Michael S. Rodgers, Joint Statement for the Record to the Senate Armed Services Committee, "Foreign Cyber Threats to the United States", 5 January 2017
[58] National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace 2018".
[59] Ibid.
[60] Ibid.
[61] The Honorable James Clapper, The Honorable Marcel Lettre & Admiral Michael S. Rodgers, Joint Statement for the Record to the Senate Armed Services Committee, "Foreign Cyber Threats to the United States", January 5, 2017

of thousands of automated accounts across social media platforms that steered discussion and sowed doubt and discord.[62] China's ongoing efforts to spread disinformation around Taiwan elections, using hackers and bots across social media platforms to spread false stories.[63] Looking ahead, AI generated deep fake videos could be the next big source of disinformation.[64]

### Cybersecurity and its market failure

The targeting of private businesses is another major cybersecurity risk, given that 85-90 percent of critical infrastructure in the U.S. is privately owned.[65] Yet, there are inadequate incentives for business to invest in a level of protection that would safeguard the public interest. The fact that cybersecurity vulnerabilities in a network can become everyone's vulnerability creates a prisoner's dilemma that justifies business underinvestment in cybersecurity. Increasing cybersecurity in one company can be undermined by a lack of cybersecurity elsewhere. This is compounded by winner-take-all network effects which emphasize speed to market over security. There are also information sharing problems, as firms are either unable to detect malicious code or fail to communicate when a backdoor is found or an attack occurs, making it harder to address vulnerabilities or better understand the threat environment.[66]In addition, often, the costs of a cyberattack are not fully born by the firm under attack. For instance, the costs of the data leaked from a cyberattack on Target were also born by consumers whose credit card details were exposed. There are also vulnerabilities from supply chains. These market failures underscore a need for government regulation.

## 3. Cybersecurity policies in the United States and China

Over 50 percent of countries have some form of cybersecurity policy. Of those that do not, approximately 80 percent are Least Developed Countries or Small Island Developing States.[67] Given the importance of the U.S. and China to global trade and security and U.S. accusations of Chinese cybertheft, this section examines the approach taken to cybersecurity by the U.S. and China.

### United States cybersecurity policies

The U.S. has developed a range of approaches to increasing cybersecurity, focusing on key areas of vulnerability.

---

[62] P.W. Singer & Emerson T. Brooking, "Like War" (Eamon Dolan 2018)
[63] Joshua Kurlantzick, How China is Interfering in Taiwan's Election", In Brief, Council on Foreign Relations, November 7, 2019.
[64] Will Knight, "Facebook is making its own AI deepfakes to head off a disinformation disaster", MIT Technology Review, September 5, 2019.
[65] K. Stouffer, V. Pilliteri, S. Lightman, M. Abrams and A. Hahn, "Special Publication 800-2 Revision 2," NIST, 2015.
[66] Vinod K. Aggarwal and Andrew W. Reddie 2018, "Comparative industrial policy and cybersecurity: The US case", Vol 3. No. 3 Journal of Cyber Policy, p. 295.
[67] UNCTAD. Cybercrime Legislation Worldwide. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

*Cyber risk to the federal government*

The Department of Defense has specific programs aimed at reducing risk in the supply chain for information and communication technologies (ICTs).[68] This includes the assessment of supply chain risk for DoD national security systems.

Executive Order (EO) 13800 requires the federal government to implement risk management procedures to address the risk of harm resulting from unauthorized access to, use, disclosure, modification, or destruction of IT and data. EO 13800 focuses federal efforts on modernizing federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies.

*Critical infrastructure*

Executive Order 13636 outlines the U.S. approach to addressing risk to critical infrastructure. It defines the goals of the policy, which include the need to "enhance the security and resilience" of critical infrastructure and "to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity."[69] The key steps identified for achieving these goals are:

- increasing the volume, quality, and timeliness of cyber threat information sharing by the U.S. government with U.S. private sector entities to help them defend themselves;
- using a risk-based approach to identify critical infrastructure where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security; and
- tasking NIST with developing a critical infrastructure cybersecurity framework that is technologically neutral and consistent with voluntary international standards, and enables critical infrastructure sectors to benefit from a competitive market for products and services that meet cyber risks.

The resulting NIST Framework is for voluntary use by the owners of critical infrastructure. It helps organizations in the private and public sector to align and prioritize cybersecurity activities, risk tolerance, and resources. The Framework relies on global standards, guidelines, and practices, helping affected organizations to achieve economies of scale and drive development of cyber products and services to meet market needs.

These cybersecurity policies have implications for trade, including by restricting imports of network hardware, software, and data flows along supply chains that pose a risk of cyberattack.

Other trade-specific measures for cybersecurity purposes focus on reducing support for technology development outside the United States. They are related to cybersecurity goals in that they can in part be seen as restricting the capacity of other states to develop cybersecurity capacity. These include, for instance, a prohibition on government procurement of any

[68] Deputy Secretary of Defense Memo, Enhanced Section 806 Procedures for Supply Chain Risk management in Support of Department of Defense Trusted Systems and Networks, March 13, 2018.
[69] Executive Order 13636 Section 1.

supercomputer manufactured outside the U.S.[70] The Wassenaar Agreement imposes controls over exports of sensitive software and technology, including internet technology. Under the Export Control Reform Act, the U.S. is also undergoing a process to identify emerging and foundational technologies that will be subject to further export restrictions.

### China's cybersecurity policies

China introduced its 2016 Cybersecurity Law "to ensure cybersecurity, to safeguard cyberspace sovereignty, national security, and social and public interests, to protect the lawful rights and interests of citizens, legal persons, and other organizations, and to promote the healthy development of the informatization of the economy and society."[71] Uncertainty remains regarding the scope of the law and how it will affect international trade, regulations are being developed to implement the legal framework it lays out. In brief, China's Cybersecurity Law:

- applies to traditional telecom operators as well as all entities that provide products and services through the internet;
- takes a risk-based approach to cybersecurity;
- imposes a testing and certification scheme for critical network equipment and cybersecurity products, requiring compliance with national standards and inspection and certification by a qualified institution;
- requires local storage for both "personal data" and "important data"[72] collected and generated by operators of critical information infrastructure; and
- compels critical information infrastructure operators to undergo a cybersecurity review when purchasing network products and services that may have an impact on national security. This review is to asses national security risks focusing on key factors such as[73]: the possibility that critical information infrastructure could be controlled; the impact on the defense industry; the product's or service' providers' response to the country's laws and regulations; and whether the product or service providers are funded or controlled by foreign governments.

## 4. Cybersecurity: The convergence of the security and economic realms

Security and trade have traditionally overlapped, in that trade has been seen as consistent with, and supportive of, broader national security outcomes. Indeed, lessons learned from raising U.S. tariffs under the 1930 Smoot-Hawley Tariff Act—which created fertile ground for the Nazis in Germany by spurring trade retaliation that devastated the economy—were a key driver of U.S. support for the GATT post World War II. More specifically, the GATT and its national security exception were negotiated against a Cold War backdrop, and the recent experience of

[70] Consolidated and Further Continuing Appropriations Act 2013, Section 516.
[71] China Cybersecurity Law Article 1.
[72] Likely refers to data with national security, economic, social stability, public health and safety concerns but not personal information – see May 2019 Draft Security Management Measures Article 28.
[73] China Cybersecurity Review Measures 2019 (Draft), Article 10.

World War II.[74] The view that closer trade ties would reduce conflict was also behind the 1951 formation of the European Coal and Steel Community, the precursor to the EU.

During the Cold War between the U.S. and the USSR, the Soviet Union was not a party to the GATT and there was very little economic interdependence between the two countries. This period was also characterized by a relative separation between the security and economic spheres at a government and economic level. Any overlaps, such as with trade in products with security applications, were dealt with separately, including by recourse to cooperative arrangements such as the Missile Technology Control Regime. From the end of the Cold War until this decade, the U.S. was dominant militarily and economically and saw globalization and growth in international trade as in its national interests.[75] In this environment, there was limited recourse to the GATT national security exception to justify trade restrictions.

Yet, this is not to say that the security exception was entirely unutilized. In fact, since the establishing of the GATT in 1947 there have been only six instances where national security was used as a justification for the trade restriction.[76] However, there was no panel decision as these cases were settled diplomatically. This exception has been used infrequently, in part because governments have been reluctant to put national security interests to the test of dispute settlement, for fear the exception could undermine the trading system.[77] As one commentator put it, "if norms are suspended, anything goes."[78]

Two developments threaten to significantly expand the use of the national security exception to justify trade restrictions—the rise of China and the growth in importance of cross-border data flows and digital technologies as drivers of growth and trade. The impact of data on growth and trade is outlined in Part 1. China is the first country since World War II that is not a U.S. military ally, is developing a political and economic system at odds with the U.S. and its allies, and seems intent on developing the military capacity to challenge U.S. predominance in the Western Pacific, at least.[79] At the same time, China is an economy with which the U.S. is deeply integrated. In 2018, over 20 percent of U.S. exports went to China and 13 percent of imports were from China, and total trade with China constituted almost 50 percent of the overall U.S. trade deficit.[80] This level of integration expands the scope for either government to use economic policy to achieve a broader range of goals with respect to each other, creating risks to both countries.[81] This has been most clearly demonstrated by Trump's decision to use tariffs on Chinese imports in order to pressure the government into reforming domestic economic policy, and the economic and political cost to the Trump from Chinese retaliatory tariffs on U.S. exports of agricultural products.

Using trade policy to achieve other non-trade goals, such as by raising tariffs or applying trade restrictions to only a subset of WTO members, is likely to be inconsistent with the countries

---

[74] Thomas W. Zeiler, Free Trade Free World: The Advent of GATT 138 (1999); Mona Pinchis-Paulsen 2019, "Trade Multilateralism and U.S. National Security", Mich J. Int'l L. Vol 41 (forthcoming)
[75] Erik Gartzke, "The Capitalist Peace", 51(1) American Journal of Political Science 166 (2007), p 169-170
[76] Roger Alford, The Self-Judging WTO Security Exception, 2011 Ital L. Rev. 697 (2011)
[77] Roger Alford, The Self-Judging WTO Security Exception, 2011 Ital L. Rev. 697 (2011); Tania Voon, Can International Trade Law Recover? The Security Exception In WTO Law: Entering A New Era", AJIL Unbound (2019) vol. 113, pp 45-50.
[78] Nomi C. Lazar, "States of Emergency in Liberal Democracies" Cambridge University Press 2009, p. 4.
[79] White House. "United States National Security Strategy." December 2017. www.whitehouse.gov/wp-content/uploads/2017/12/NSSFinal-12-18-2017-0905.pdf.
[80] United States Census Bureau, https://www.census.gov/foreign-trade/balance/c0004.html#2018
[81] Mark Leonard (ed), "Connectivity Wars: Why Migration, Finance and Trade and the Geo-economic Battlegrounds of the Future" (London: European Council on Foreign Relations, 2016); Robert D. Blackwill and Jennifer M. Harris, War by Other Means, Geoeconomics and Statecraft", Harvard University Press 2016, p. 20.

WTO commitments. Increasingly, such restrictions are being justified as necessary for national security. The Trump Administration is relying on national security to justify tariffs on imports of steel and aluminum (and possible also on automobiles) [82]and has raised tariffs on China to pressure the government to reform its economy and stop stealing U.S. IP. Similarly, Russia relied on the WTO national security exception to justify restrictions on transit of Ukrainian exports, and the UAE had relied on the WTO security exception to justify trade restrictions with Qatar, though that case has now been settled following withdrawal of the trade restrictions.[83]

As outlined in Part 1, the growth in digital trade has made countries increasingly interconnected.[84] This level of digital interconnectedness creates an entirely new set of economic and security vulnerabilities, in particular exposing the growing digital economy to cyberattack.[85] This is true not only when it comes to countries with high levels of trade, but from any country with an internet connection. In this sense, digital trade has expanded the vulnerability to cyberattack across an economy as well as the opportunity for governments to use cyber to cause harm.

# 5. Cybersecurity within the WTO security exception and general exception

The growth in digital trade and parallel rise in cybersecurity concerns presents a real risk to the rules-based trading system. One is the risk is that cybersecurity becomes a stalking horse for new levels of trade protectionism. For example, China's indigenous WAPI standard for wireless was in part motivated by cybersecurity concerns with the global WLAN standard, but by forcing use of WAPI in the Chinese market has operated as a trade barrier.[86]

The other risk is that even where cybersecurity measures are genuine, the scope of the cybersecurity challenge could lead to a range of new trade restrictions across all areas of the digital economy, including access to information as well as the goods and services used in critical infrastructure. The vague definition in China's cybersecurity law of what constitutes critical infrastructure could be used to limit foreign firms' access to key sectors or require access to source code, under the justification of security, as a condition of entering a market, while exposing foreign companies to IP theft.[87] In addition, as some governments assert greater control over online information, cybersecurity is being used to justify a range of limits over digital content. For instance, Vietnam's cybersecurity law prohibits, among other things, "distorting history, denying revolutionary achievements, or destroying the fine tradition and customs of the people, social ethics, or health of the community."[88] A statement by the

[82] United States-Certain Measures an Steel and Aluminium Products, Communication from the United States, WT/DS544/3, 18th April 2018.
[83] https://www.mofa.gov.qa/en/statements/qatar-confirms-proceeding-with-dispute-settlement-over-uae's-illegal-measures
[84] McKinsey & Company. 2016. *Digital globalization: The New Era of Global Flows*. 2016. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-ofglobal-flows.
[85] Henry Farrell and Abraham Newman, "Weaponized Interdependence", 44(1) International Security 42 (2019).
[86] Ping Gao, WAPI: A Chinese Attempt to Establish Wireless Standards and the International Coalition that Resisted", Communications of the Association for information Systems, Vol 23, Article 8, July 2008
[87] Samm Sacks, Rogier Creemers, Lorand Laskai, Paul Triolo and Graham Webster, "China's Cybersecurity Reviews for 'Critical' Systems Add Focus on Supply Chain, Foreign Control (Translation) https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation/.
[88] Vietnam Law 24 on Cybersecurity, 12 June 2018.

Shanghai Cooperation Organization on cooperation in the field of international information security considers as a threat the "dissemination of information harmful to social and political, social and economic systems, as well as the spiritual, moral and cultural sphere of other states."[89] Looking ahead, the standards that apply to 5G could raise trade and cybersecurity concerns. As the U.S. and China aim to build 5G using different ends of the spectrum, this raises the prospect that interconnecting with overseas networks and software built by Chinese companies will create cybersecurity risks as well as trade barriers for U.S. companies, who would need to adapt to the lower spectrum when exporting.[90]

The core WTO rules are that members will not discriminate in favor of domestic over foreign goods and services—the national treatment (NT) commitment—or in favor of one WTO members over another—the most favored nation (MFN) treatment commitment. Yet, cybersecurity measures may require restricting trade with countries deemed a security risk, which may breach the NT and MFN commitments. For instance, global trade networks are vulnerable to attacks along digital supply chains. In some cases, a government may determine that the best policy response to this vulnerability is to prevent certain companies, suspected of being under government control, from participating in the supply of key technologies. For instance, a recent White House executive order prohibits the import of information and communication technology and services from entities controlled by a foreign adversary and where the import poses various risks—including of cyberattack.[91] Recent draft regulations out of China regarding its cybersecurity review process also identify services and products controlled by foreign governments as potentially being subject to cybersecurity review.[92]

Imports restrictions on goods from countries deemed a high security risk would violate GATT Articles I (MFN), III (NT), as well as Article III (NT) of the WTO Government Procurement Agreement (GPA)—a plurilateral agreement that includes the U.S. but not China.[93] Where a WTO member has scheduled a services commitment under the WTO's General Agreement on Trade in Services (GATS), then that member must accord that service NT and market access as well as allowing cross-border data flows to deliver that service.[94] The GATS MFN commitment applies to all services unless a member has scheduled an exception. WTO members have made relatively liberal commitments for computer-related services such as software, which would require NT, market access as well as MFN. Bans on data flows from specific countries could breach a member's GATS MFN commitment[95] Data localization measures that increase the burden on foreign suppliers could be inconsistent with the GATS NT commitment.[96] The Appellate Body finding in U.S.—Gambling that a complete prohibition

---

[89] NATO Cooperative Cyber Defence Center of Excellence. "Agreement between the Government of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security".
[90] Milo Medin and Gilman Louie, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD", Defense Innovation Board, April 2019, p. 4.
[91] White House Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019 https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.
[92] Samm Sacks, Rogier Creemers, Lorand Laskai, Paul Triolo and Graham Webster, "China's Cybersecurity Reviews for 'Critical' Systems Add Focus on Supply Chain, Foreign Control (Translation) https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation/.
[93] The GPA applies to the procurement of products or services that members schedule.
[94] Panel Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services (US–Gambling, WT/DS285/R (10 November 2004) ), paras. 6.285–87; Appellate Body Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WT/ DS285/AB/R (7 April 2005), para. 215.
[95] WTO Appellate Body Report, US–Gambling, paras. 238, 251.
[96] H. P. Hestermeyr and L. Nielsen (2014), 'The Legality of Local Content Measures under WTO Law', Journal of World Trade, 48(3): 588.

on the online supply of gambling services was a "zero quota" in breach of GATS article XCI:2(a) market access obligation.[97]

In the event that a cybersecurity measure breaches a WTO commitment, the member could seek to justify the measure under the WTO national security exception found in GATT Article XXI, GATS Article XIV *bis* and GPA Article XXIII.1, or in the general exception found in GATT Article XX, GATS Article XIV or GPA XXIII.2. Trade restrictions on content, data flows and access to software will likely constitute services trade restrictions and will need to be justified under GATS and will be the focus of this section. The analysis under GATS would also apply to trade restriction on goods imports or on the procurement of goods or services, such as equipment used in 5G for instance, and which would need to be justified under the relevant GATT and GPA exceptions provisions.

## The WTO security exception

The security exception in the GATT, GATS and GPA allows members to adopt measures for security purposes, which would otherwise be inconsistent with these agreements.[98] The need for a security exception was articulated by the U.S. delegation in 1947 during the negotiation of the International Trade Organization (ITO)—the predecessor to the GATT.[99] The exception would have to recognize members' right to take measures for national security reasons without allowing any country to use national security as a pretext for protectionism.[100]

The original GATT security exception has been replicated throughout the WTO, including in the GATS[101] and the Agreement on Trade-Related Aspects of Intellectual Property Rights.[102] Exceptions for national security requirements are also found in the GPA and throughout the Technical Barriers to Trade Agreement.[103]

The security exception in GATS Article XIV bis is as follows:

> *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;*

[97] WTO Appellate Body Report, US–Gambling, paras. 238, 251.
[98] This exception is replicated in for services in GATS Article XIV bis.
[99] Mona Pinchis-Paulsen 2019, "Trade Multilateralism and U.S. National Security", Mich J. Int'l L. Vol 41 (forthcoming)
[100] Second Session of the Preparatory Committee of the United Nations Conference on Trade and Employment, Verbatim Report, Third Meeting of Commission A Held on Thursday, 24 July 1947, E/PC/T/A/PV/33, p.21
[101] GATS Article XIV bis.
[102] TRIPS Article 73.
[103] TBT Articles 2.2, 2.10.5.4 and 5.7

> *(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.*

The text of GATS Article XIV bis can admit of a range of interpretations, from fully self-judging—where it is up to each government to determine its security needs, leaving no space for panel security—through to various roles for a WTO panel, including determining whether a measure was taken in good faith and complies with objective standards.[104] Moreover, key terms in GATS Article XIV bis are undefined, including what is meant by "essential security interest" or "emergency in international relations."

A recent dispute brought to the WTO for settlement serves to illustrate some of the tensions inherent in applying the security exception, and the way in which its language has been interpreted to meet various tests. The case, known as Russia - Measures Concerning Traffic in Transit, involved a challenge by Ukraine to restrictions imposed by Russia on Ukrainian imports and exports transiting through Russian territory. Russia sought to justify these restrictions under the GATT Article XXI security exception.[105]

The WTO panel first turned to the question of justiciability of the security exception, as Russia, with the United States as a third party, claimed that there was no role for the panel.[106] These arguments were rejected.[107] The panel then focused on the extent to which the security exception is self-judging. Russia had claimed that the adjectival clause "which it considers" in XXI(b) makes all of GATT Article XXI self-judging. The panel reasoned that finding all of Article XXI to be self-judging would render subparagraphs (i)-(iii) unnecessary or to no effect —an outcome that should be avoided as a matter of treaty interpretation.[108] To give effect to these subparagraphs, the panel concluded that the events referred to in each subparagraph were "objective facts that are amenable to objective determination" and which qualify the scope of "essential security interests". In addition, the panel found that each subparagraph requires a connection between the measure taken for the protection of essential security interests and the end described in each subparagraph.[109] The first two subparagraphs are relatively specific, relating to fissionable material and traffic in arms. The third subparagraph refers to "an

[104] Wesley A. Cann Jr 2001. "Creating Standards and Accountability for the Use of the WTO Security Exception: Reducing the Role of Power-Based Relations and Establishing a New Balance Between Sovereignty and Multilateralism", Yale J. Int'l L. Vol 26. Issue 2; Roger Alford, The Self-Judging WTO Security Exception, 2011 Ital L. Rev. 697 (2011), p. 705-706; Shin-yi Peng 2015, Cybersecurity Threats and the WTO National Security Exceptions", Vol 18. J. Int'l Econ. L. Issue 2; J. Benton Heath, The New National Security Challenge to the Economic Order", Yale Law Journal (forthcoming 2019)
[105] WTO Panel Report, Russia-Measures Concerning Traffic in Transit, WT/DS512/R (April, 5 2019).
[106] Third Party Oral Statement of the United States of America, Russia-Measures Concerning Traffic in Transit DS512, January 2018, para 5.
[107] WTO Panel Report, Russia-Transit, para 7.58.
[108] Id., para 7.65.
[109] Id., para 7.69-7.70.

emergency in international relations" and is what Russia claimed was the case with respect to Ukraine.

The panel had to decide what events would qualify as an emergency in international relations. The panel noted that the phrase "war or other emergency in international relations" showed that war is an example of a larger category of emergency in international relations.[110] Using other sources of treaty interpretation, including a dictionary definition of "emergency" and the context of the subparagraph which included subparagraphs (i) and (ii), the panel concluded that all subparagraphs refer to "similar or convergent concerns," creating a category of matters that are all about "defense and military interests as well as maintenance of law and public order interests,"[111] that mere political and economic differences are insufficient to constitute an emergency in international relations.[112] This led the panel to find that an emergency in international relations refers generally "to a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state.[113] In reaching this finding, the panel took into account views of the U.S. delegation to the ITO in the early 1940s which described an emergency in international relations as including events preceding World War II in 1939 when the U.S. had not formally joined the war effort but had to impose trade restrictions nevertheless.[114] In this case, the panel found that the situation between the Ukraine and Russia, which the U.N. General Assembly had recognized as involving armed conflict, constituted an emergency in international relations.[115]

The next step was for the panel to determine whether the measure—the restrictions on transit—was "taken in time of" the emergency in international relations. The panel found that this required that action must be taken "during the war or other emergency in international relations."[116] As Russia had introduced the measures in 2014 and 2016, the panel found that they satisfied this temporal need.

The panel then turned to the chapeau in GATT Article XXI(b), which states overriding considerations that subsequent clauses are subject to. Here, the panel found that "essential security interest" refers to "the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally."[117] The panel also noted that a state's security interests will change according to circumstances and that it is up to members to define their own essential security interests—i.e., this element is self-judging such that a panel will accept members' own determinations. Yet even here, this determination is limited by the requirement that it must be made in good faith.[118] In practice, this means that members will be required to explain *why* the interest so identified is an essential security interest—it is not enough merely to state that it is one.[119] In this case, Russia was found to have satisfied this requirement.[120]

---

[110] Id, para 7.71.
[111] Id, para 7.74.
[112] Id, para 7.74.
[113] Id, para 7.76.
[114] Id, para 7.99.
[115] Id, para 7.122.
[116] Id, para 7.70.
[117] Id, para 7.130.
[118] Id, para 7.132.
[119] Id, para 7.134.
[120] Id, para 7.137.

Finally, while it is up to the member to determine the "necessity" of the measure, the panel found that the obligation of good faith also requires some minimal plausible relation between the measure adopted and the essential security interest.[121] This was a hurdle that Russia's ban on transit was able to satisfy.[122]

## The WTO general exceptions

The WTO GATS Article XIV general exception provision (largely replicated in GATT Article XX) is also available to justify trade restrictions for cybersecurity purposes, along with measures to protect critical infrastructure and supply chains considered necessary for public morals (including public order in the case of GATS), privacy or to protect human life or health.[123] Yet, governments would be subject to the more rigorous disciplines of these general exceptions, as compared with the national security exception.

Were WTO members to rely on the GATS general exception to justify cybersecurity measures, it would likely claim that the measure is necessary to protect public morals, as covered under GATS XIV(a), or as necessary to secure compliance with laws and regulations not inconsistent with the GATS, including those relating to the protection of the privacy of individuals, as covered under Article XIV(c)(ii).

The defending member government then needs to show that the cybersecurity measure is "necessary." The WTO Appellate Body has found that whether a measure is deemed necessary requires weighing or balancing factors, including the contribution of the measure to the purported policy goal, the importance of the common interests, or values, protected by the measure, and its impact on imports.[124] This is where the contribution of the measure to its objective is assessed. Evidence that the cybersecurity measure is in fact improving security would be relevant here. Conversely, a cybersecurity measure that includes data localization requirements but which has the effect of undermining or reducing cybersecurity, would support a finding that such a measure is not "necessary."[125]

In the event that the cybersecurity measure passes this weighing and balancing stage, the complainant could then seek to show that there is a less trade restrictive alternative that could achieve the responding WTO member's goal that is reasonably available, taking into account resources and technical capacity.[126] The Appellate Body has found that, to qualify as a genuine alternative, the proposed measure must not only be less trade restrictive than the original measure at issue, but should also "preserve for the responding member its right to achieve its desired level of protection with respect to the objective pursued."[127] Here, the complaining member could seek to show that the measure's goal could be achieved in ways that are less

[121] Id, para 7.138.
[122] Id, para 7.145
[123] GATS Article XIV(a),(b) & (d), GATT Article XX(a) & (b).
[124] WTO Appellate Body Report, *Brazil – Measures Affecting Imports of Retreaded Tyres*, WT/DS33December 2007; Appellate Body Report, US–Gambling, paras. 306–308.
[125] A. Chander and P. Le Uyen (2014), 'Breaking the Web: Data Localization vs. the Global Internet', UC Davis Legal Studies Research Paper Series No. 378, April 2014, p. 5.
[126] WTO Appellate Body Report, European Communities - Measures Prohibiting the Importation and Marketing of Seal Products, WT/DS4-00/AB/R, 22 May 2014, para 5.261.
[127] WTO Appellate Body Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, WT/DS4-00/AB/R, 22 May May 2014, para 5.261.

restrictive on digital trade, including ways that reduce restrictions on cross-border data transfers.[128]

Having established that a data localization requirement is "necessary," it would still need to be assessed for consistency with the requirement in the chapeau that it is not applied in a manner that constitutes a "means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services." The WTO Appellate Body has stated that the assessment of the consistency of a measure with the chapeau is about "locating and marking out a line of equilibrium between the right of a Member to invoke an exception … and the rights of other Members under varying substantive provisions."[129] The focus on the application of the measure emphasizes how the measure works in practice rather than the measure's justification.[130]

## Assessing cybersecurity under the national security exception or the general exception

It is up to each WTO member to decide whether a measure for cybersecurity purposes is to be justified under the security exception and/or the general exceptions. Yet, and as will be discussed, the national security exception is poorly suited to dealing with the challenges that cybersecurity will present for international trade. As outlined, the negotiating history shows an awareness amongst the GATT contracting parties of the need for flexibility to restrict trade for national security reasons as well as the potential for abuse of a fully self-judging exception. The panel's rejection of the claim that the security exception is totally self-judging reserves a role for the security exception to distinguish protectionism from legitimate security claims.

The view of WTO exceptions as being aimed at distinguishing legitimate reasons for trade restrictions from disguised protectionism has been at the heart of the disciplines in the general exception.[131] The challenge under the general exception provision is that determining whether a measure is for the claimed legitimate purpose, or is instead protectionist, requires assessing whether the objective design or purpose of the measure is linked closely enough to the claimed goal. For instance, in Brazil-Retreaded tires the Appellate Body had to determine whether a law banning imports of retreaded tires from WTO members not party to MERCOSUR was in fact about reducing environmental and health risks or protecting the domestic tire industry.[132] In Seal Products dispute, the AB had to decide whether an EU measure banning most imports and exports of seal products for animal welfare reasons, nevertheless was protectionist.[133]

In contrast, the very nature of the range of security issues that fall under the GATT or GATS security exceptions—such as trafficking in arms or even an emergency in international relations - makes it harder for governments to use claims of national security to disguise what are really protectionist aims. For instance, in the Russia-Transit case, the tensions between Russia and

---

[128] J. P. Meltzer and P. Lovelock, 'Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia', Brookings Working Paper 113, March 2018 for a discussion of how to achieve legitimate policy goals while minimizing restrictions on cross-border data transfers.
[129] WTO Appellate Body Report, *US–Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, adopted 6 November 1998, para. 159.
[130] WTO Appellate Body Report, '*US–Shrimp*', WT/DS58/AB/R (12 October 1998), paras. 115–116.
[131] Robert E. Hudec 1998, "GATT/WTO Constraints on National Regulation: Requiem for an "Aims and Effects Test", The International Lawyer; Robert Howse and Donald Regan 2000, "The Product/Process Distinction – An Illusory Basis for Disciplining 'Unilateralism' in Trade Policy", Vol 11. EJIL, No. 2, 249
[132] WTO Appellate Body Report, "Brazil-Measures Affecting Imports of Retreaded Tyres", WT/DS332/AB/R, 3 December 2007
[133] WTO Appellate Body Report, "European Communities-Measures Prohibiting the Importance and Marketing of Seal Products," WT/DS400/AB/R, 22 May 2014

Ukraine were internationally recognized—there was a U.N. resolution on the matter. In other words, the very seriousness of the security interests that could fall within the security exception makes it relatively straightforward to distinguish legitimate claims from disguised protectionism.

However, cybersecurity, unlike more traditional security issues, does challenge how to distinguish legitimate concerns from disguised protectionism. As outlined, cybersecurity policy is increasingly risk based and will need to be adopted over the long-term. As a result, cybersecurity measures are often not in response to the types of security event that are observable and which help ground national security claims.

Yet, the approach of the panel in the Russia-Transit case to defining what constitutes an "emergency in international relations" as well as the temporal link in the text that requires the measure to be "taken in time of" the emergency in international relations, would also seem to exclude from the scope many of the risk-based cybersecurity measures that the U.S. and China for instance are implementing. As a result, the national security exception is not available. As noted, cyber risks can emanate from any country with an internet connection and through global supply chains. The diffuse and ongoing nature of the risk requires countries to adopt continuous cybersecurity measures that can minimize risk and deter attacks, irrespective of whether there is an emergency in international relations with the country affected by the measures. It is also unlikely that most cybersecurity measures would fall under either of the other subparagraphs (a) and (b) in Article XIV bis.

The member must also show that measure is "taken in time of" the emergency in international relations. In the Russia-Transit case, this test was satisfied because the measure was taken during Russian-Ukraine tensions. This temporal link can help avoid retroactive justification of a trade restriction by pointing to a past emergency in international relations, and limits reliance on the security exception for the duration of the emergency in international relations. Yet, such a temporal link maps poorly onto measures to reduce cybersecurity risk, which as noted are about adopting longer-term risk management practices over time.

For example, the trade war between the U.S. and China was initiated in part to raise the costs and thereby deter Chinese cyberattacks, in this case cyber theft of IP and trade secrets. Yet, it would seem strange for this to constitute an emergency in international relations, as it would allow the tariffs that created the emergency in international relations to serve as justification for those same tariffs. Alternatively, the U.S. could seek to point to the Chinese cyberattacks as constituting the emergency in international relations, however, this would require showing that prior to the trade war there was "a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state." Moreover, even once the trade war subsides, the U.S. will continue to expand cybersecurity measures to reduce the risk of cyberattack from China, which will likely reduce trade in various digital products, including 5G equipment, software, and data flows. Yet, the absence of an emergency in international relations between the U.S. and China as outlined by the Panel in Russia-Transit, would seem to would seem to foreclose genuine cybersecurity measures being justified under the GATS or GATT security exception.

In this case, a range of cybersecurity measures will likely have to be justified under the general exceptions of GATS Article XIV. Under the general exceptions provision, panels and the Appellate Body have read the GATS Article XIV (a) exception for public morals or public order

widely, and instead focused on whether the measure is necessary.[134] So in practice, a member may find it easier to satisfy the first stage of the GATS Article XIV analysis by seeking to show that a cybersecurity measure is intended to address public morals or order, than by seeking to establish that there is an emergency in international relations under GATS Article XIV *bis*.

Having shown that a given cybersecurity measure is for a policy goal enumerated in a general exception in GATS Article XIV, the measure must also be "necessary." This means the complaining member can seek to show that there is a less trade restrictive alternative.

Yet, the necessity requirement could be challenging for a panel to apply effectively. Determining whether there is an alternative, less trade-restrictive measure will require a panel to assess the relative importance of the values or interests at stake, the contribution of the cybersecurity measure to reducing risk, and the acceptable costs. In addition, given the market failures that cybersecurity measures address, a panel will also need to assess the impact of the measure on private sector incentives and gauge the effectiveness of alternative approaches in terms of their impact on the market. Moreover, where the cybersecurity measure is part of a broader suite of measures to reduce cyber risk, the WTO Appellate Body has signaled the need to consider the overall system and its impact over time, further complicating the analysis.[135] This raises significant evidentiary requirements. Moreover, the burden of proof is on the complaining member to identify a less trade restrictive alternative, a particular challenge where cybersecurity measures are based on national security classified information.[136]

Finally, the measure also needs to be justified under the chapeau of either the general exception or the security exception. As noted, the panel in Russia-Transit found that the chapeau to the GATT security exception is self-judging. Based on this approach, it will be up to the defending member to establish that the measure is necessary to protect its essential security interest, and based on the approach in Russia-Transit, panels will largely accept member's claims that cybersecurity measures are necessary to protect its essential security interests. In contrast, under the general exception, the measure must not be arbitrary and unjustifiable or a disguised restriction on international trade. One situation where this chapeau has had purchase was in the Shrimp-Turtle case. In that case the U.S. had successfully negotiated a treaty with some countries for the conservation of turtles from fishing yet failed to embark on a good faith attempt to find a negotiated outcome with another countries, instead preferring to restrict trade unilaterally. The WTO Appellate Body found that this constituted arbitrary and unjustifiable discrimination inconsistent with the GATT Article XX chapeau.[137]

Such a requirement may be inappropriate when it comes national security issues, and cybersecurity specifically. National security is defined by discrimination in favor of allies. Governments often manage security issues with allies and fail to do so with others. Addressing cybersecurity risks will similarly require working with allies and like-minded governments to develop global norms, rules and standards for cybersecurity. While the chapeau does not

---

[134] US-Gambling, supra note 49, para 6.465; This approach was confirmed in WTO Panel Report, China-Audiovisuals, para 7.759; see also WTO Appellate Body Report, European Communities-Measures Prohibiting the Important and Marketing of Seal Products, WT/DS400/AB/R, 22 May 2014, para 5.199.
[135] Appellate Body, Brazil-Retreaded Tyres, para 155.
[136] J. Benton Heath, The New National Security Challenge to the Economic Order", Yale Law Journal (forthcoming 2019)
[137] WTO Appellate Body Report, "U.S.-Import Prohibition of Certain Shrimp and Shrimp Products", WT/DS58/AB/R (Oct. 12th, 1998), para 115-116.

require a negotiated outcome, only a good faith attempt at negotiation, this requirement maps awkwardly onto how governments conduct national security policy.

A brief turn to how some FTAs address national security. Various FTAs have dispensed with the subparagraphs in the WTO security exception, and instead their security exceptions appear largely self-judging, though an international tribunal has yet to rule on their scope. For example, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) security exceptions state that nothing in this agreement "shall be construed to prevent a Party from applying measures that it consider necessary for the fulfillment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests."[138] This security exception is replicated in the U.S.-Mexico-Canada Agreement (USCMA) and the U.S.-Japan Digital Trade Agreement.[139] One consequence is to widen the scope for governments to justify a cybersecurity measure under such a FTA security exception. This raises the prospect that parties to FTAs with updated e-commerce rules on data flows will increasingly rely on the security exception to justify cybersecurity measures, including restrictions on data flow.[140]

# 6. Using trade policy to improve cybersecurity

Relying on the security exception is not a stable basis for managing the impact that cybersecurity is going to have on the rules-based trading system. The WTO security exception does not map onto the reality of cybersecurity, and FTA security exceptions seem broad enough to justify most if not all cybersecurity measures. The general exceptions in the WTO and FTAs are useful provisions that could help countries balance reducing cybersecurity risk and trade, but they too are not well suited to cybersecurity, given the complexity of the issues. In addition, more technical issues, such as requiring the complaining WTO member to show evidence of less trade-restrictive alternatives, may set too high an evidentiary burden when it comes to cybersecurity regulation, which may be based on confidential security information.

These challenges and limits highlight why new trade rules for cybersecurity are needed. This could entail developing a shared global understanding of cybersecurity and the different risks involved. A commitment to providing an administrative record supporting cybersecurity regulations consistent with security needs, affirming that less trade-restrictive alternatives were considered, would help build trust that cybersecurity measures are not disguised protectionism. Trust—along with rules that link cybersecurity measures to risk—could be reflected in a trade commitment that all cybersecurity measures be based on a risk assessment, drawing on a similar requirement in the WTO Agreement on the Application of Sanitary and Phytosanitary Measures.[141] In addition, a commitment to use international standards as a basis for cybersecurity measures—a process already being developed under the NIST Framework—would minimize unnecessary regulatory diversity and attendant costs on

[138] CPTPP Article 29.2.
[139] USMCA Article 32.2, US-Japan Digital Trade Agreement, Article 4.
[140] Mattoo, Aaditya and Joshua P. Meltzer. "Data Flows and Privacy: the conflict and its resolution." Journal of International Economic Law. Vol 21, Issue 4.
[141] See SPS Agreement Article 5.1.

digital trade, and deepen confidence that the cybersecurity measures were not for protectionist purposes.[142]

Finally, good-faith but novel cybersecurity regulations are likely affecting a growing amount of digital trade, potentially undermining many of the gains governments thought they had bargained for in the WTO or in FTAs.[143] Addressing the impact of cybersecurity on trade requires cooperation and building norms around behavior in cyberspace. Trade policy is one tool for developing common goals and appropriate courses of action. The following steps, pursued collectively, could be the basis for a new understanding around cybersecurity and trade.[144]

### Support a risk-based approach to cybersecurity.

According to the OECD, cybersecurity should "aim to reduce the risk to an acceptable level relative to the economic and social benefits expected from those activities, while taking into account the legitimate interests of others."[145] As outlined, the NIST Framework relies on risk assessments tailored to each organization's needs, and the EU's Network and Information System Directive requires security measures that are "appropriate and proportionate … to manage the risks posed to the security of network and information systems." A risk assessment should then inform decisions as to what measures to adopt, what risk reduction can be expected, and at what cost. The rapidly changing nature of cybersecurity threats means that addressing risk is a dynamic process that requires regular reassessment of risk and consideration of what else might be needed to reduce risk to acceptable levels. In contrast, an overly prescriptive regulation can become quickly outdated or lead to box-checking instead of thoughtful assessment of whether the steps taken are in fact reducing risk.

Building an effective approach to cybersecurity also requires engaging government and business leaders and building cyber risk management into the core of corporate and government practice.[146] The USMCA includes a recognition of the importance of taking a risk-based approach to cybersecurity instead of proscriptive approaches, including risk-based approaches that rely on consensus-based international standards and best practices.[147] Drawing on the WTO SPS Agreement which includes a commitment that SPS measures be based on a risk assessment, consideration should be given to building on the USMCA to include a commitment that cybersecurity measures are based on a risk assessment.

### Develop global cybersecurity standards.

Cybersecurity standards can build a common approach to addressing cybersecurity risks based on best practice. For instance, the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) have developed a number of cybersecurity-

---

[142] Shin-yi Peng, "Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime", Vol 51. Cornell Int'l L. J. No. 2 Art 4, Spring 2018
[143] J. Benton Heath, "The National Security Challenge to the Economic Order", Yale Law Journal, Vol. 129.
[144] The following draws from Joshua P. Meltzer and Cameron F. Kerry, "Cybersecurity and digital trade: Getting it right", Brookings Working Paper, September 18th, 2019.
[145] OECD (2015) Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD 2015.
[146] Thomas Poppensieker et al, 2018. "Digital and Risk A new posture for cyber risk in a networked world", McKinsey & Company.
[147] USMCA Article 19.15.

related standards, including the jointly developed ISO/IEC 27000 series, as well as sector specific-standards for electric utilities, health care, and shipping.[148]

Standards are needed to address cyber risks from IoT. This would include common security features. The Internet Engineering Task Force is developing relevant standards. Standards are most effective when they don't prescribe a particular approach but instead are frameworks for managing risk, relying on business and government to design cybersecurity measures most suitable to their business practices and risk profiles. In turn, the NIST Framework relies on international standards such as ISO 27001 as references for its cyber risk management framework, with the result that the Framework is not U.S. specific and can be adopted globally.[149]

Trade agreements can be used to reinforce the role of consensus-based standards, with commitments to develop international standards and to use those that already exist as a basis for domestic regulation. These agreements should be flexible enough to include 'bottom-up' stakeholder developed standards, such as the NIST cybersecurity framework.[150] Tying cybersecurity policy to international standards will also support the development of globally consistent and least trade-restrictive approaches to cybersecurity. Using international standards as a basis for cybersecurity policy can also help address concerns that cybersecurity regulation is a disguised restriction on trade aimed at supporting domestic industry.

### Ensure compliance with cybersecurity standards.

Compliance certification can give consumers and businesses confidence in the cybersecurity of government and private organizations. Under the EU Cybersecurity Act, which came into force in June 2019, the European Union Agency for Cybersecurity will establish an EU-wide cybersecurity certification scheme.[151] NIST has developed a different approach in the Baldridge Performance Excellence Program, which encourages self-assessment of compliance. Trade agreements can support conformity assessment regimes, while aiming to minimize the burden they impose on trade, by requiring governments to allow other parties to undertake the conformity assessment of products (to meet country-of-import regulations) in the country of export. Further commitments that conformity assessment requirements are non-discriminatory and not disguised restrictions on international trade would provide additional requirements that lead to the consideration of trade impacts on the development of cybersecurity regulation.

### Enhance information sharing.

As reflected in the U.S. Cybersecurity Information Sharing Act, real-time sharing of information on threats and vulnerabilities—to promote awareness, plan responses, and help targets adapt and respond—has become an important feature of cybersecurity policies. The trust issues implicit in sharing proprietary or classified information in the domestic context are compounded when dealing with governments or organizations across national borders. Nevertheless, the U.S. is seeking to improve information sharing with international partners and allies and along supply chains. Trade agreements can include commitments to building

[148] IEC 61850, ISO/IEC 80001, IEC 61162.
[149] NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, April 25, 2019.
[150] Shin-yi Peng, "Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime", Vol 51. Cornell Int'l L. J. No. 2 Art 4, Spring 2018.
[151] Regulation (EU) 2010/881 of the European Parliament and of the Council of 17 April 2019 on ENISA.

public and private sector information-sharing mechanisms. For example, the U.S.-Mexico-Canada trade agreement includes a commitment to sharing information and best practices as a means of addressing and responding to cyberattacks.[152]

**Improve access to data.**

As cybersecurity defense becomes more sophisticated, use of analytics and machine learning to monitor network activity plays a growing role in the analysis of risks and anomalies.[153] In fact, requiring data to be localized reduces opportunities for companies to use big data analytics to assess risk across global operations and supply chains. Forcing data into specific locations also increases the risk and cost of a data breach. The CPTPP and USMCA commitments to information flows across borders (subject to appropriate exceptions) and to avoiding data localization requirements, advance digital trade opportunities and cybersecurity outcomes.[154]

# 7. Conclusion

There is a deteriorating international security landscape among the major powers, and in contrast with the Cold War between the U.S. and Russia, the U.S. and China are also deeply connected via trade and investment. The global internet has increased such connectivity along with the scope for attack. This makes cybersecurity a point where the pulls of connection and push of competition converge. Reducing cyber risk is now a focus for many countries, as the risk of cyberattacks is a key point of security as well as economic and social vulnerability. These developments have upended the traditional approach in international trade to national security issues, which relied on government forbearance in using national security to justify new trade measures. It is also becoming apparent that the international trade rules used to channel security-based measures are not well-suited to addressing the risk-based, long term, and possibly economy-wide nature of cybersecurity measures.

The WTO security exception is likely too limited in scope for governments to use in justifying many measures taken to prevent economic espionage, cyberattacks on critical infrastructure, or manipulation of online information. While the general exception provision can accommodate a broader range of cybersecurity measures, the provision is also not well suited to balancing trade and cybersecurity goals. For one, members may be unwilling to tolerate the third-party scrutiny of what they see as national security measures. Second, cybersecurity raises complex issues that WTO panels are not well suited to address, including the risk of a cyberattack, potential harm and the political and social salience of cybersecurity measures. Third, the confidential nature of information use to justify cybersecurity measures will make it particularly difficult for a complaining member to establish that the cybersecurity measure is necessary, i.e., that there is a less trade restrictive alternative. In the FTA context, security exceptions are more generously drafted and would seem to provide scope for justifying most, if not all cybersecurity measures. Yet, this raises the prospect of FTA commitments being avoided through heavy reliance on the security exceptions provision to justify cybersecurity

[152] USMCA article 19.15(b).
[153] OECD (2015) Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD 2015 Publishing, Paris, Principle 7.
[154] CPTPP Articles 14.11, 14.13; USMCA Articles 19.11, 19.12.

measures that restrict trade. This similarly raises the question of whether the security exception undermines the bargain governments thought they struck in these trade agreements.

Moving forward, new trade policies are needed. A first priority is to develop specific trade rules for cybersecurity, and, as this paper has outlined, a range of issues must be considered, including cybersecurity standards, commitments to risk-based cybersecurity measures, better sharing of information, and access to data. Consideration should also be given to developing an exception provision tailored for cybersecurity measures. In the interim, a common understanding of cybersecurity and its risks can help governments determine whether to justify cyber measures under the general exception or security exception in the WTO or in FTAs. All of these rules should be developed and included in a new cybersecurity agreement or in cybersecurity chapters within FTAs.