GLOBAL ECONOMY & DEVELOPMENT
WORKING PAPER 132 | May 2020

Global Economy and Development at BROOKINGS

Cybersecurity, digital trade, and data flows

Re-thinking a 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 J. Benton Heath, Michael O'Hanlon, Shin-Yi Peng, Tom Stefanik and Tania Voon for their feedback and comments. All mistakes are my own.

Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rules

Joshua P. Meltzer

Working Paper #132
Global Economy and Development
Brookings Institution
May 2020

An earlier version of this paper titled "Cybersecurity and digital trade: What role for international trade rules?" was published in November 2019.

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] Global data flows enable artificial intelligence, the "internet of things," (IoT) and cloud computing. Such digital technologies accelerate the global connectivity of businesses, governments, and supply chains.[2]

As digital connectivity grows, however, so does exposure to the risks and costs of cyberattacks.[3] Moreover, the potential costs of cyberattack have underpinned a turn to conceiving cybersecurity risk as a national security threat.[4] As President Trump'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."[5] The scope of potential cybersecurity threats includes the digital space such as cybertheft of intellectual property (IP) and personal data and manipulation of online information, as well as the physical space, such as critical infrastructure (e.g., telecommunications, transport, and health care) and IoT, which relies on software to network services.

Many countries are adopting cybersecurity policies.[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 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]

This paper is focused on U.S.-China cybersecurity risks, measures taken to address these risks, and the implications for the bilateral trade and investment relationship. The U.S. and China are conceiving of cybersecurity risk broadly, potentially affecting large parts of the economy, including critical infrastructure, digital content, information, and interconnected goods—the IoT. In parallel, the emerging U.S. view of China as a strategic threat and competitor has highlighted how economic integration can be a source of vulnerability. There are two

[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] Helen Nissenbaum, "Where computer security meets national security", Ethics and Information Technology (2005) 7:61, p. 63
[5] NSTAC, Report to the President on a Cybersecurity Moonshot, Draft.
[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.

consequences to this development. One is the reduced scope for the U.S. and China to resolve cybersecurity concerns diplomatically. The other is the turn to using trade and investment restrictions as a preferred tool for addressing cybersecurity threats. These developments are undermining the post-World War II approach to dealing with trade-related security issues largely outside the GATT (and then the WTO). Yet, current trade rules are completely inadequate in addressing the challenges that cybersecurity measures will bring to international trade.

Many U.S. and Chinese cybersecurity measures are likely to restrict cross-border data flows and digital trade. These include data-localization requirements and import and investment restrictions on data and information technology (IT) products, particularly from countries or along supply chains where cyber risk is high. Import restrictions including higher tariffs are also being used to punish and deter cyberattacks.[10]

Treating goods, services, or data from high-risk countries like China 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, it can seek to justify the cybersecurity regulation under the treaty's security or general exception provision. Until recently, governments have largely avoided relying on the WTO security exception to justify trade restrictions. There had been no WTO case dealing with the security exception prior to 2018, when a WTO panel issued a decision on the scope of the GATT national security exception. The lack of WTO cases until recently reflected broad concern amongst WTO members of the potential for abuse of the national security exception to justify trade restrictions, and a preference for addressing the impact of national security measures on trade using negotiation and diplomatic channels. However, and as noted, deteriorating U.S.-China relations have reduced the scope for the U.S. and China to security resolve security/trade tensions diplomatically. This reflects not only a deteriorating bilateral relationship, but changes in the global security environment, including the extension of what constitutes national security to large segments of the economy, and the end of the notion that major powers would converge and stop treating each other as rivals.[11]

The conception of cybersecurity as a national security threat and the use of trade policy to address cybersecurity threats creates two distinct challenges for the rules-based trading system. The first is the capacity for trade rules in the WTO and in FTAs to distinguish 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, which also raises difficult questions for trade policy. Here, the trade policy challenge is to distinguish legitimate cybersecurity from protectionism, as well as to minimize the impact of legitimate cybersecurity regulation on digital trade.

As this paper will discuss, current trade rules in the WTO are not fit for purpose. 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. For instance, 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

[10] USTR s.301
[11] Tom Wright, "All Measures Short of War." Yale University Press, 2017.

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. This could include using trade policy to support the development of cybersecurity standards, commitments to good regulatory practice and to using risk assessments as a basis for cybersecurity regulation. In the absence of cooperation, cybersecurity policy risks becoming the core organizing principle for the digital economy, leading to increasing trade with trusted partners and less exposure to countries presenting cyber risk.

While this paper focuses on the cybersecurity and trade implications through the prism of the U.S. and China relationship, the legal and policy implications outlined in this paper are relevant for all countries as they address cybersecurity threats while also maximizing opportunities from data flows and digital trade. 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 policies 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 digitization of broad areas of industry and services. Understanding the scope 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.[12] 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.[13]

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 that could add trillions of dollars to global output over the next 10 years and accelerate the transition towards a services-driven global economy.[14] The McKinsey Global Institute estimates that AI could add around 16 percent, or $13 trillion, to global output by 2030.[15] AI requires access to large data sets as machine learning needs to incorporate as many past outcomes as possible into future predictions.[16] 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.[17]

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.[18] 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.[19]

---

[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] Generative adversarial networks or use of digital twins can minimize need for large data sets to train AI.
[17] 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.
[18] 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.
[19] 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.[20] 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.[21] 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.[22] According to the WTO, using digital technologies to reduce trade costs could increase world trade by up to 34 percent by 2030.[23] 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.[24]

Internet access and cross-border data flows are also increasing services trade.[25] Services can increasingly be purchased and consumed online. This is particularly true for IT, professional, financial, retail, and education services.[26] Many of the emerging technologies delivered online are themselves services. Cloud computing, for instance, offers software, applications, and IT infrastructure as a service.[27]

Data collection and analysis are adding value to goods exports through so-called "servicification."[28] Data flows enable digitization of the entire manufacturing enterprise, shorter production cycles, and collaborative and connected supply chains.[29] 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

[20] 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.
[21] 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.
[22] Brynjolfsson, E, X Hui and Meng Liu. "Does Machine Translation Affect International Trade? Evidence from a Large Digital Platform." 2018.
[23] WTO Trade Report 2018.
[24] 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.
[25] Aaditya Mattoo and Sacha Wunsch-Vincent, "Pre-empting Protectionism in Services: The GATS and Outsourcing", Journal of International Economic Law 7(4), 2004.
[26] 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.
[27] United States International Trade Commission. *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*. Pub. No 4716, August 2017, pp. 58-66.
[28] Lucian Cernat and Zornitsa Kutlina-Dimitrova, THINKING IN A BOX: A 'MODE 5' APPROACH TO SERVICE TRADE, DG Trade Chief Economist Note, Issue 1 March 2014
[29] L. Yu, et al. "Current Standards Landscape for Smart Manufacturing Systems." *NIST*, NISTIR 8107, February 2016.

analytics as the key to a successful transformation toward smart manufacturing.[30] This reflects the importance of digital services for increasing productivity, which affects the capacity of firms to compete domestically and overseas.[31] 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.[32] 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.[33] 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.[34] Global data flows are also enabling so-called "supply chain 4.0"—where information flows are integrated and omnidirectional instead of linear.[35] 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.[36] 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.[37] 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.[38]

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

---

[30] PricewaterhouseCoopers 2016. Industry 4.0: Building the digital enterprise. 2016 Global Industry 4.0 Survey.
[31] 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.
[32] Baldwin, R. "The Great Convergence: Information Technology and the New Globalization." Boston: Harvard University Press. 2016.
[33] OECD. "Mapping Global Value Chains", TAD/TC/WP/RD(2012)9. 2012.
[34] Helpman E. "Understanding Global Trade." Cambridge, Mass: Harvard University Press. 2011.
[35] 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)
[36] Miroudot S., Charles Cadestin. Services in Global Value Chains: From Inputs to Value-Creating Activities." *OECD Trade Policy Paper 19*7, p. 16. 2017.
[37] Milo Medin and Gilman Louie, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD", Defense Innovation Board, April 2019.
[38] 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.

an IP app.[39] 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 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 commonly agreed definition of cybersecurity. However, the International Telecommunication Union broadly defines it as,[40]

> *"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."[41] In turn, the White House National Cyber Strategy focuses on increasing the security and resilience of the nation's information and information systems.[42]

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.[43] 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

[39] Tom Wheeler, 5G in five (not so) easy pieces, Brookings Report, July 9, 2019.
[40] ITU definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity.
[41] NISTIR 7298, Revision 3, "Glossary of Key Information Security Terms", July 2019.
[42] White House National Cybersecurity Strategy, September 2018.
[43] 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 five 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 fifth is access to data and technology through international investment.

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.

National defense

One area of risk is the use of cyberattack to hack into the defense industry.[44] 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.[45] A range of actions is 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.[46]

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. [47] The USA PATRIOT Act 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."[48] This definition was referenced in Executive

[44] 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
[45] Id.
[46] Enhanced Procedures for Enterprise-Wide Use of Section 806 Supply Chain Risk Management Authorities for DOD National Security Systems..
[47] EU Coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, October 9, 2019
[48] USA Patriot Act of 2001, (42 U.S.C. §5195c(e)) .

Order 13636, "Improving Critical Infrastructure Cybersecurity," and the NIST Framework for Improving Critical Infrastructure Cybersecurity.[49]

Vectors of attack on critical infrastructure include IT, industrial control systems, cyber-physical systems, and connected devices.[50] 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.[51] 5G will also underpin explosive growth in IoT. Yet IoT devices are also vulnerable, including to botnet denial-of-service attacks. Accessing 5G through software allows governments to include back doors that can be used to control a system or steal information.[52] Even if it is possible to confirm that the initial software is safe, future releases and patches can compromise security.

Economic cyber-espionage

Malicious actors can also use the internet to hack into commercial enterprises,[53] stealing trade secrets, and IP. Cyber-espionage will erode America's longer-term economic advantage.[54] 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.[55] 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.[56]

Digital information

There are two elements here. One is the collection by a foreign entity of sensitive personal information is now seen in both the U.S. and China as a national security threat.[57] The second element is the falsification or manipulation of information online to create confusion and distrust.[58] This would include, for example, in the lead-up to the 2016 U.S. Presidential election, Russia's use of thousands of automated accounts across social media platforms that steered discussion and sowed doubt and discord.[59] China's ongoing efforts to spread disinformation around Taiwan elections, using hackers and bots across social media platforms to spread false stories.[60] Looking ahead, AI generated deep fake videos could be the next big source of disinformation.[61] Moreover, the vast amount of data that will traverse the 5G network

[49] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[50] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, p. 1.
[51] EU Coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, October 9, 2019
[52] 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.
[53] 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
[54] National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace 2018".
[55] Ibid.
[56] Ibid.
[57] Foreign Investment Risk Review Modernization Act of 2018 (FIRMMA), Subtitle A of Title XVII of P.L. 115-232; China Cyber Security Law
[58] 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
[59] P.W. Singer & Emerson T. Brooking, "Like War" (Eamon Dolan 2018)
[60] Joshua Kurlantzick, How China is Interfering in Taiwan's Election", In Brief, Council on Foreign Relations, November 7, 2019.
[61] Will Knight, "Facebook is making its own AI deepfakes to head off a disinformation disaster", MIT Technology Review, September 5, 2019.

will present new opportunities to access and undermine the integrity, confidentiality, and privacy of information. Reliance on global suppliers of IoT from China also creates supply chain risk.[62]

Access to technology

Governments are also taking steps to limit access by foreign governments to local technology, in part to preempt the ability to use such technology to engage in future cyberattacks. This is not an entirely new approach to addressing national security risk from trade. For instance, under the 1996 Wassenaar Arrangement, participating governments agreed to limit exports of goods designed for military use as well as dual use technologies. Export restrictions are being updated for the digital economy and expanded as a new range of technology creates new national security risks.[63] In addition, the U.S. is restricting inward investment that provides access to data sets that could be used to develop the technology for cyberattacks as well as access to sensitive personal data that could be used to compromise individuals in ways that put national security goals at risk.

Cybersecurity and its economic challenges

One of the challenges for governments in developing cybersecurity policy is the role of the private sector as a target and a key source of much of the data and technology that other governments seek to obtain. In addition, in the U.S. for instance, 85-90 percent of critical infrastructure is privately owned.[64] Despite the central role of the private sector, there are inadequate incentives for business to invest in a level of protection that would safeguard the public interest. There are a number of reasons for this. One is that cybersecurity vulnerabilities in a network are everyone's vulnerability, creating a prisoner's dilemma that justifies business underinvestment in cybersecurity. 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. Second, 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. Third, there are 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.[65] These market failures underscore a need for government regulation.

Another challenge to getting cybersecurity policy right is ensuring that cybersecurity policy that restricts trade and investment is not undermined by business in third countries exporting competing technologies For instance, for reduced U.S. exports of technology to China to be effective in reducing cybersecurity risk require other countries producing competitive technologies to also limits exports. The costs of getting it wrong can be significant, both in terms of failure to achieve the desired security goal and in terms of lost economic opportunity. For example, U.S. export controls on satellites technology not only did not achieve the goal of preventing access by non-allied countries to such technology, but also provided the opportunity

[62] Milo Medin and Gilman Louie, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD", Defense Innovation Board, April 2019, p. 23.
[63] U.S Export Control Reform Act 2018
[64] K. Stouffer, V. Pilliteri, S. Lightman, M. Abrams and A. Hahn, "Special Publication 800-2 Revision 2," NIST, 2015.
[65] Vinod K. Aggarwal and Andrew W. Reddie 2018, "Comparative industrial policy and cybersecurity: The U.S. case", Vol 3. No. 3 Journal of Cyber Policy, p. 295.

for competitors (often in allied countries) to develop their own capabilities, capturing global market share from the US.[66] One of the lessons here is that for export restrictions to be effective in preventing access to technologies that could increase cyber risk, such restrictions should be targeted and combined with international cooperation.[67]

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.[68] 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.

Cyber risk to the government

The Department of Defense has specific programs aimed at reducing risk in the supply chain for information and communication technologies (ICTs).[69] 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. For example, the U.S. government will not procure any supercomputer manufactured outside the U.S.[70]

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

[66] U.S. Department of Commerce, Bureaus of Industry and Security, Defense Industrial Base Assessment: U.S Space Industry, August 2007 https://www.bis.doc.gov/index.php/documents/technology-evaluation/38-defense-industrial-base-assessment-of-the-u-s-space-industry-2007/file
[67] U.S Space Industry "Deep Dive" Assessment: Impact of U.S. Export Controls on the Space Industrial Base, Department of Commerce Bureau of Industry and Security, 2014
[68] UNCTAD. Cybercrime Legislation Worldwide. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.
[69] 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.
[70] Consolidated and Further Continuing Appropriations Act 2013, Section 516.

efficiency, innovation, and economic prosperity".[71] 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.[72] 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 the development of cyber products and services to meet market needs.

Digital information

The U.S. sees the collection of forms of personal data as "sensitive personal data" as a cybersecurity risk and more broadly a risk to national security.[73] Reform of CFIUS now includes screening of foreign investment that provides access to sensitive personal data. Given the use of data across the economy, this is a potentially expansive investment restriction into sectors such as finance, insurance, health, transport, retail, and software. For example, the Administration used its new authority under FIRRMA to pressure Chinese company Kunlun Tech to sell Grindr—a gay dating app and forced Chinese company icarbonx to divest from PatientsLikeMe—which collects personal health care data.

U.S. action to limit access to domestic technology

The U.S. has increased scrutiny of investments in technology and is in the process of tightening regulations affecting technology exports. Specifically, the 2018 Foreign Investment Risk Review and Modernization Act (FIRRMA) extends the range of investments in the U.S. by foreign persons that are subject to CFIUS review, to non-controlling "other investments" by a foreign person where the U.S. business 1) owns or operates critical infrastructure, produces, designs, tests or manufactures critical technologies (defined broadly to include "emerging and foundational technologies"); and 3) maintains or collects sensitive personal data of U.S. citizens that may be exploited in a way that threatens U.S. national security.[74] CFIUS also allows for the government to discriminate amongst countries by designating a country as being "of special concern" when it has demonstrated a declared strategic goal of acquiring critical technology or critical infrastructure that would affect the U.S. in areas related to national security.

---

[71] Executive Order 13636 Section 1.
[72] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018
[73] Foreign Investment Risk Review Modernization Act 2019
[74] Foreign Investment Risk Review Modernization Act 2019

Another form of cybersecurity trade measures have restricted the ability for U.S. companies to sell technology to Chinese companies. The most recent high profile of such restrictions arose from the decision to place Huawei on the Department of Commerce Entities Lis due to the U.S. government's belief "that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States."[754]. Being on the Entity List has the effect of prohibiting exports or re-exports of U.S. goods, technology or software subject to the U.S. Export Regulations. The U.S. is also pursuing more broad technology export restrictions pursuant to the Export Control Reform Act, which calls for export restrictions on emerging and foundational technologies.

China's cybersecurity policies

China introduced its 2016 Cybersecurity Law to "ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society" [76] 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'[77] 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:[78] 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.

[75] BIS, Final Rule, Addition of Entities to the Entity List, 84 FR 22961
[76] China Cybersecurity Law Article 1, translation at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/
[77] 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.
[78] China Cybersecurity Review Measures 2019 (Draft), Article 10.

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

Security and trade have traditionally overlapped yet been dealt with separately. This state of affairs is now at an end. The following outlines how the system worked and the changes that destabilized the security/trade arrangement.

Since the end of the cold war, the U.S. and its allies have seen trade 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.[79] More specifically, the GATT and its national security exception were negotiated against a Cold War backdrop as well as the recent experience of World War II.[80] 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. The U.S. view that international trade is good for its economic and national security has various strands to it. For one, as trade raises economic welfare it leads to increased demand for more of the products in which the U.S. has a comparative advantage such as high-end manufactured goods and sophisticated services. Second, rising growth and expanding middle classes tend to foster more stable political systems which often trend democratic as well, over time.[81] For a hegemon with global security responsibilities, global stability is a public good and in the U.S. interest as it helps avoids calls on the U.S. military. Third, as countries benefit from trade and the rules-based system which underpins it, countries buy-into the system in a normative sense – which in the trade context is the set institutions and rules centered around the WTO. As a system, the U.S. had an outsized role in creating and leading, and which embodies core U.S. goals, this effectively expands U.S. soft power—the capacity to get other countries to do what the U.S. wants because they also see compliance with the WTO as being in their national interest.[82]

The view that economic integration is good for security survived the cold war, Japan's economic challenges to the U.S., and until recently, the rise of China. Indeed, China's accession to the WTO in 2001 was characterized as important for U.S. national security.[83] During the Cold War, the USSR was a security competitor to the U.S. but there was very little economic interdependence. The USSR was not a party to the GATT, enabling the economic and security spheres when it came to U.S.-USSR relations, to be kept relatively separate. 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. On the flip side, U.S. concern about the spread of communism contributed to ongoing U.S. support for international trade and investment as a bulwark against communist influence in third countries. 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

[79] Thomas W. Zeiler, Free Trade Free World: The Advent of GATT 138 (1999)
[80] 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)
[81] Robert J. Barro, 1999. "Determinants of Democracy." Journal of Political Economy, 107(6): S158–83.
[82] Joseph Nye, Soft Power, Foreign Policy, No. 80, Twentieth Anniversary (Autumn, 1990), p. 166
[83] President Clinton, Statement on Permanent Normal Trade Relations with China, April 11, 2000

interests.[84] In this position, the U.S. could focus on the absolute gains from trade, being less concerned about changes in relative gains from rivals.[85]

While trade has been seen as broadly supportive of national security, trade restrictions have been justified under the GATT with reference to this security exception.[86] Indeed, as early as 1949 Czechoslovakia challenged U.S. export controls that selectively applied to Eastern European countries. Moreover, the parties did not intend for national security measures to be totally excluded from review. Indeed, the negotiating record of the ITO showed concern amongst the delegates that a completely self-judging national security exception could become an exception that could swallow the rules.[87] The U.S. delegation at the time also considered a role for a GATT panel to identify abuse of the exception.[88] Yet, while trade restrictions were seen at times as necessary, state practice was to settle these issues diplomatically outside of the trading system, instead of resorting to the more formal dispute settlement mechanism in the GATT.[89] Until recently, the establishment of the WTO with its binding dispute settlement mechanism did not disrupt this pattern of dealing with security claims.

Two developments threaten to significantly expand reliance on national security to justify trade restrictions—the rise of China, and the breakdown in a common understanding of what are security issues, which incudes the expansion of national security from state-state matters to include non-state actors, terrorism, the environment and cybersecurity.[90] When it comes to China, it is the first country since WWII 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.[91] At the same time, China is an economy with which the U.S. is deeply integrated. In 2019, 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.[92] This level of integration is no longer seen merely as a driver of economic efficiency, but increasingly as a source of leverage and vulnerability.[93] In the digital economy and trade space specifically, the U.S. and China have turned to restricting bilateral trade and investment in part to reduce exposure to cyberattacks. This move to "weaponize interdependence" is leading to digital connectivity and cross-border data flows being assessed in zero-sum national security terms.[94] There is also no common understanding of what are cybersecurity measures. As outlined above, cybersecurity measures cover a wide range of potential vulnerabilities, from infrastructure to information and include a range of risks to human life and social and political stability. The potential scope of cybersecurity threatens to overwhelm the trading system. As will be elaborated upon,

---

[84] Erik Gartzke, "The Capitalist Peace", 51(1) American Journal of Political Science 166 (2007), p 169-170
[85] Robert O. Keohane. After Hegemony: Cooperation and Discord in the World Political Economy (Princeton, NJ: Princeton University Press, 1984).
[86] See Russia: Transit Case; Roger Alford, The Self-Judging WTO Security Exception, 2011 Ital L. Rev. 697 (2011)
[87] See generally Mona Pinchis-Paulsen, Trade Multilateralism and U.S. National Security: The Making of the GATT Security Exception, forthcoming Michigan Journal of International Law, p 16-32
[88] Commission A, Verbatim Report, 33rd Meeting of the Commission A, 1947, E/PC/T/A/PV/33, WTP Archives at 26
[89] 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.
[90] J. Benton Heath, "The National Security Challenge to the Economic Order", Yale L.J 2020, p. 28
[91] White House. "United States National Security Strategy." December 2017. www.whitehouse.gov/wp-content/uploads/2017/12/NSSFinal-12-18-2017-0905.pdf.
[92] United States Census Bureau, https://www.census.gov/foreign-trade/balance/c0004.html#2018
[93] 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; Anthea Robert, Henrique, Choer Moraes and Victor Ferguson, "Towards a Geoeconomic Order (22 J. Int'l Econ. L. 4 (2019)
[94] Henry Farrell and Abraham Newman, "Weaponized Interdependence", 44 (1) International Security 42 (29109)

existing trade rules provide no meaningful parameters to distinguish legitimate cybersecurity from protectionism or to channel legitimate cybersecurity measures into least trade restrictive outcomes. Failure to remedy this risks undermining the digital economic opportunity that cybersecurity is meant to support.

5. Cybersecurity within the WTO security exception and general exception

The growth in digital trade and the parallel rise in cybersecurity concerns presents a real risk to the rules-based trading system. One 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 the use of WAPI in the Chinese market has operated as a trade barrier.[95]

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, for instance, 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.[96] 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."[97] A statement by the Shanghai Cooperation Organization on cooperation in the field of international information security considers as a threat to 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."[98] 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.[99]

The WTO has long recognized that a measure can raise both goods and services issues.[100] The range of measures to address cybersecurity risk will apply to trade in goods and services and

---

[95] 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
[96] 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/.
[97] Vietnam Law 24 on Cybersecurity, 12 June 2018.
[98] 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".
[99] Milo Medin and Gilman Louie, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD", Defense Innovation Board, April 2019, p. 4.
[100] Appellate Body Report, European Communities – Regime for the Importation, Sale and Distribution of Bananas, WT/DS27/AB/R, adopted 25 September 1997

as a result could raise GATT/TBT and GATS issues. In many cases, cybersecurity will address a combination of goods/services issues, such as software embedded in control systems used in critical infrastructure or in IoT raise trade in goods issues. Yet, due to the interconnected nature of critical infrastructure and IoT, the software in these goods may be vulnerable to malware and hacking, raises issues relating to trade in services and cross-border data flows.

The GATT

First, with respect to trade in goods, the core GATT commitments are that of national treatment—not to discriminate in favor of domestic over foreign goods and the MFN commitment—not to favor one WTO member's goods over another WTO member.

Cybersecurity measures may require various trade restrictions, which may breach the NT and MFN commitments. For instance, global trade networks are vulnerable to cybersecurity attacks along 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.[101] 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.[102]

Imports restrictions on goods from countries deemed a high security risk would violate GATT articles I (MFN), III.4 (NT) which applies to 'all laws, regulations and requirements affecting … internal sale, offering for sale, purchase, transportation, distribution or use'. The Appellate Body has found that the general principle in GATT art III:1 that laws, regulations and requirements 'should not be applied to imported or domestic products so as to afford protection to domestic production' informs GATT art III:4,[103] revealing that the national treatment commitment is aimed at preventing protectionism—measures that discriminate between domestic and imported goods based on national origin. Whether products are like should be determined on a case-by-case basis, applying the criteria for likeness, drawing on the 1970 GATT Working Party report on Border Tax Adjustments: (i) physical properties, nature and quality; (ii) product end uses in a given market; (iii) consumers' tastes and habits; and (iv) tariff classification.[104] The Appellate Body followed this approach in later cases applying GATT art III:4.[105] While rejecting an inquiry into regulatory purpose, the Appellate Body did find that where art III:1 'informs' the national treatment obligation, panels should analyze the measure's structure and application, in order to determine whether it affords protection to the like domestic products.[106] Whether two products are like is essentially an inquiry into whether

[101]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/.
[102] 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/.
[103] Appellate Body Report, European Communities — Measures Affecting Asbestos and Asbestos-Containing Products, WTO Doc WT/DS135/AB/R, AB-2000-11 (12 March 2001) [100] ('EC — Asbestos'), citing GATT 1994 art III:1.
[104] Border Tax Adjustments, GATT Doc L/3464 (2 December 1970) (Report of the Working Party) GATT BISD 18S/97 [18].
[105] Appellate Body Report, European Communities — Regime for the Importation, Sale and Distribution of Bananas, WTO Doc WT/DS27/AB/R, AB-1997-3 (9 September 1997) [215]–[216].
[106] Appellate Body Report, Japan — Taxes on Alcoholic Beverages, WTO Doc WT/DS8/AB/R, WT/DS10/AB/R, WT/DS11/AB/R, 29.

these products compete in the market.[107] However, the WTO Appellate Body has recognized that what determines competition can include product characteristics such as the impact on health.[108] Where products are like, the GATT NT and MFN commitments require that no less favorable treatment is accorded to the domestic product over the like imported product (NT), or to a like importer product over another like import (MFN). The Appellate Body did suggest that regulatory distinctions can be drawn between groups of otherwise like products without necessarily according less favorable treatment.[109] However, more recent jurisprudence has affirmed that detrimental impact on conditions of competition will amount to less favorable treatment.[110] The implications for cybersecurity measures is that where consumers perceive otherwise like goods as having different cybersecurity risks, this could support a finding that products do not complete and therefore are not like products. However, there are limits to this approach.

One limit is that consumers may lack the information or the incentive to become informed about cyber risks, particularly where the cyber risk from individual IoT products may be low, but the cyber risk grows where large number of devices are hacked and used for DDOS attacks. Another limit is the lack of incentive for the private sector to adequately address cybersecurity risk. For these reasons, consumers may not reflect the full cost of cyberattacks in their purchasing decisions, requiring regulation that targets particular products or countries.

Cybersecurity measures are also likely to seek to reduce risk by addressing how goods are produced or accepting goods only from countries that are allies as one way of minimizing cybersecurity risk. This could include some form of oversight by the importing state of the production process - whether it is oversight of the supply chain or development of the software. For instance, China's cybersecurity law includes an assessment of whether the goods or service is controlled or funded by a foreign government, opening the door to country-based restrictions.

From a legal perspective, the question is whether a cybersecurity measure that conditions imports on how they are produced, can make otherwise like goods, unlike. Whether WTO allows for regulation which targets how the good is produced rather than the product itself, remains unsettled.[111] Where differences are how products are produced is not relevant for a finding of likeness, such measures by virtue of the *ad note* to Article III are subject to and prohibited by the GATT article XI commitment to avoid quantitative restrictions.

The net result is that a lot of cybersecurity regulation is likely to discriminate amongst "like products", and violate the WTO NT and/or MFN commitments, requiring that such measures are justified under the WTO security or general exception provisions.

---

[107] See Joel P. Trachtman -WTO Trade and Env Jurisprudence: Avoiding Environmental Catastrophe. Vol 58. No. 2, Spring 2017, p 281-284
[108] Appellate Body Report, EC — Asbestos, WTO Doc WT/DS135/AB/R
[109] Appellate Body Report, EC — Asbestos, WTO Doc WT/DS135/AB/R, para 100
[110] Appellate Body, European Communities-Measures Prohibiting the Important and Marketing of Seal Products, WT/DS400/AB/R, 22 May 2014, para 5.101
[111] Robert Howse and Donald H. Regan 2000, "The Product/Process Distinction – An Illusory Basis for Disciplining 'Unilateralism' in Trade Policy", University of Michigan Law School Scholarship Repository; Joel Trachtman 2017, "WTO Trade and Environment Jurisprudence: Avoiding Environmental Catastrophe", No. 2 Harv. Int'l L. J., Vol 58, 283

The TBT agreement

The TBT agreement is also relevant for cybersecurity measures affecting trade in goods. The TBT Agreement requires members accord NT and MFN to all technical regulations affecting trade in products.[112] Under the TBT Agreement, technical regulations "lay down product characteristics or their related process and production methods, including applicable administrative procedures with which compliance is mandatory."[113] China's development of testing and certification schemes for critical network equipment and cybersecurity products would likely constitute technical regulations. The WTO has taken a similar approach to assessing the TBT NT/MFN standards for likeness as in the GATT, focusing on whether there is a competitive relationship between the products.[114] However, unlike the NT/MFN commitment in the GATT, this TBT commitment is not subject to an exception provision. The WTO Appellate Body has found that the balance between the MFN/NT commitment and the exceptions provision is to be found within TBT article 2.1.[115] According to the Appellate Body, under TBT article 2.1 there is no less favorable treatment where the detrimental impact on the like imported goods stems exclusively from a legitimate regulatory distinction.[116] There are two challenges here to applying this to cybersecurity measures. One is that as cybersecurity measures will be risk-based, in many instances a WTO panel will need to assess whether the regulation appropriately calibrates the discriminatory aspects with the cybersecurity risk. Yet as the Appellate Body has noted in another context, the higher the risk, the more deference will be given the government decision how to address such risk.[117] When it comes to high risk cybersecurity, then this assessment of whether the regulatory distinction is appropriately calibrated could cash out as extensive deference. On the other hand, when dealing with lower risk products, the TBT could require a high level of calibration

TBT article 2.2 is another relevant provision, which requires that regulations are not more trade restrictive than necessary to fulfill a legitimate regulatory objective, and which explicitly includes national security requirements as a legitimate objective. The requirement of "necessary" is that there is no less trade restrictive means for achieving the government's regulatory goal.[118] Showing whether there are less trade restrictive alternatives will raise challenging evidentiary demands, particularly when cybersecurity measures are being assessed using national security classified information and are part of a broader cybersecurity policy.

TBT article 2.4 is also relevant as it requires members to use international standards, where they exist, as a basis for their technical regulations, unless the international standards would be an ineffective or inappropriate means for fulfilling the legitimate objectives pursued. As discussed, the U.S. NIST has developed a cybersecurity framework based on international standards. In this respect, NIST may present a useful approach to developing cybersecurity practice in the private sector that is also TBT compliant.

---

[112] TBT Agreement Article 2.1
[113] TBT Annex 1.1
[114] Appellate Body Report, US — Clove Cigarettes, WTO Doc WT/DS406/AB/R, para 112
[115] Appellate Body Report, US — Clove Cigarettes, WTO Doc WT/DS406/AB/R, para 109
[116] Appellate Body Report, US — Clove Cigarettes, WTO Doc WT/DS406/AB/R, para 174. See also Appellate Body Report, Dominican Republic — Measures Affecting the Importation and Internal Sale of Cigarettes, WTO Doc WT/DS302/AB/R, AB-2005-3 (25 April 2005), para 96
[117] WTO Appellate Body, European Communities-Measures Affecting Asbestos and Asbestos-Containing Products, WT/DS135/AB/R, 12 March 2001
[118] WTO Appellate Body Report, *Brazil – Measures Affecting Imports of Retreaded Tyres*, WT/DS33December 2007

The WTO Government Procurement Agreement (GPA) may also be relevant when it comes to cybersecurity measures that restrict which countries governments can procure from but is not addressed further in this paper as China is not a party to the WTO GPA.

The GATS

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.[119] 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.[120] Data localization measures that increase the burden on foreign suppliers could be inconsistent with the GATS NT commitment.[121] In U.S.—Gambling, the Appellate Body found that a complete prohibition on the online supply of gambling services was a "zero quota", in breach of GATS article XCI:2(a) market access obligation.[122]

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* , or in the general exception found in GATT Article XX, GATS Article XIV. Trade restrictions on goods will need to be justified under GATT Article XX/XXI, whereas restrictions on content, data flows and access to software will likely constitute services trade restrictions and will need to be justified under GATS Article XIV/XIV bis.

Digital trade commitments in FTAs

Recent FTAs include digital trade commitments not found in the WTO, and which commitments may also be at odds with cybersecurity measures. For example, the USMCA includes a commitment by the parties not to "prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person."[123] Another important digital trade commitment in the USCMA is that the parties agreed not to require the domestic location of computing facilities as a condition for doing business.[124]

There is also a specific non-discrimination commitment modeled on the GATT MFN/NT that applies to digital products. Digital products mean "a computer program, text video, image, sound recording or other products that is digitally encouraged, produced for commercial sale or discrimination, and that can be transmitted electronically."[125] This would include, for instance, software, or online which are subject to U.S. and Chinese cybersecurity laws.

---

[119] 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.
[120] WTO Appellate Body Report, US–Gambling, paras. 238, 251.
[121] H. P. Hestermeyr and L. Nielsen (2014), 'The Legality of Local Content Measures under WTO Law', Journal of World Trade, 48(3): 588.
[122] WTO Appellate Body Report, US–Gambling, paras. 238, 251.
[123] USMCA Article 19.11
[124] USMCA Article 19.12
[125] USMCA article 19.1

The USMCA financial services chapters also include a commitment to the free flow of information as well as a prohibition on data localization requirements, subject to appropriate exceptions.[126] The prohibition against data localization is subject to the party's financial regulatory authorities, for regulatory and supervisory purposes, having immediate, direct, complete, and ongoing access to relevant information used by a covered person outside its territory. Before imposing data localization, the parties also commit to providing a reasonable opportunity to covered entities to remediate any lack of information access.

Cybersecurity measures can restrict cross-border data flows, require data to be stored domestically, and discriminate between digital products. In the event of a breach, the cybersecurity measure would need to be justified under either the national security or general exceptions provision. The data flow commitment is subject to an exception modeled on the GATT articles XX/GATS Article XIV exceptions provision. There is no specific exception in the USMCA digital trade chapter to the data localization requirement or non-discrimination commitment, however, the USMCA general exception provision applies GATS Article XIV in both cases.[127] In addition, USMCA has a specific exception for national security discussed below in part xx.

The WTO Security Exception

The security exception in the GATT and GATS is identical and allows members to adopt measures for security purposes, which would otherwise be inconsistent with these agreements. The following addresses the security exception in GATS article XIV bis, but the analysis would also apply to GATT article XXI.

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;*
> >
> > *(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.

---

[126] USMCA, supra note 57, at art. 17.17.
[127] USMCA, supra note 57, at art. 32.1.2.

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, through to various roles for a WTO panel, including determining whether a measure was taken in good faith and complies with objective standards.[128] 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 WTO decision highlights 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.[129]

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.[130] These arguments were rejected by the Panel on the ground it had 'inherent jurisdiction' as a result of its adjudicative function.[131] 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. Based on the ordinary meaning of Article XXI in its context and in the light of the object and purpose of the GATT, the Panel found that the words 'which it considers" in the chapeau of GATT article XXI(a) do not qualify the subsequent paragraphs. The panel also 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.[132] 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.[133] The first two subparagraphs are relatively specific, relating to fissionable material and traffic in arms. The third subparagraph refers to "an 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.[134] 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

---

[128] 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)
[129] WTO Panel Report, Russia-Measures Concerning Traffic in Transit, WT/DS512/R (5 April, 2019).
[130] Third Party Oral Statement of the United States of America, Russia-Measures Concerning Traffic in Transit DS512, January 2018, para 5.
[131] WTO Panel Report, Russia-Transit, para 7.58.
[132] Id. para 7.65.
[133] Id. Para 7.69-7.70.
[134] Id. para 7.71.

that are all about "defense and military interests as well as maintenance of law and public order interests"[135], that mere political and economic differences are insufficient to constitute an emergency in international relations.[136] 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."[137] 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.[138] In this case, the panel found that the situation between Ukraine and Russia, which the U.N. General Assembly had recognized as involving armed conflict, constituted an emergency in international relations.[139]

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."[140] 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."[141] 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.[142] 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.[143] In this case, Russia was found to have satisfied this requirement.[144] 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.[145] The Panel found that the measures at issue were not so remote from or unrelated to the 2014 emergency that it is implausible that Russia implemented them to protect its essential security interests arising from that emergency.[146]

This panel report has not been appealed and the current hobbling of the WTO Appellate Body will prevent any such move in the near future. Panel or Appellate Body reports do not have any formal precedential value and are only binding on the parties to the dispute.[147] However, WTO

[135] Id, para 7.74.
[136] Id, Para 7.74.
[137] Id, para 7.76.
[138] Id, para 7.99.
[139] Id. para 7.122.
[140] Id. para 7.70.
[141] Id. para 7.130.
[142] Id. para 7.132.
[143] Id. para 7.134.
[144] Id. para 7.137.
[145] Id. para 7.138.
[146] Id. para 7.145
[147] Appellate Body Report, US-Stainless Steel (Mexico), WT/DS344/AB/R (April 30, 2008, para 158

panel reports do create "legitimate expectations amongst WTO members and should be 'taken into account' where relevant.[148]

The WTO general exception provision

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.[149] 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.[150] 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."[151]

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.[152] 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."[153] Here, the complaining member could seek to show that the measure's goal could be achieved in ways that are less restrictive on digital trade, including ways that reduce restrictions on cross-border data transfers.[154]

---

[148] WTO Appellate Body report, Japan – Alcoholic Beverages II, WT/DS8/AB/R. WT/DS10/AB/R, WT/DS11/AB/R (Oct. 4, 1996), p. 14

[149] GATS Article XIV(a),(b) & (d), GATT Article XX(a) & (b).

[150] WTO Appellate Body Report, *Brazil – Measures Affecting Imports of Retreaded Tyres*, WT/DS33December 2007; Appellate Body Report, US–Gambling, paras. 306–308.

[151] 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.

[152] 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.

[153] 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.

[154] 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.

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."[155] The focus on the application of the measure emphasizes how the measure works in practice rather than the measure's justification.[156]

Assessing cybersecurity under the national security 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.[157] 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.[158] In the 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.[159]

In contrast, the very nature of the range of traditional security issues likely to fall under the GATT or GATS security exceptions—such as trafficking in arms or even an emergency in international relations—are in most cases objectively identifiable, making 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 Ukraine were internationally recognized—there was a U.N. resolution on the matter. In other words, the very

[155] WTO Appellate Body Report, *US–Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, adopted 6 November 1998, para. 159.
[156] WTO Appellate Body Report, '*US–Shrimp*', WT/DS58/AB/R (12 October 1998), paras. 115–116.
[157] 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
[158] WTO Appellate Body Report, "Brazil-Measures Affecting Imports of Retreaded Tyres", WT/DS332/AB/R, 3 December 2007
[159] WTO Appellate Body Report, "European Communities-Measures Prohibiting the Importance and Marketing of Seal Products", WT/DS400/AB/R, 22 May 2014

seriousness of the security interests that could fall within the security exception helps 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. Addressing high risk potentially catastrophic cyberattacks by restricting data flows and trade in digital products, would likely be considered an "essential security interest".[160] However, in many cases cybersecurity measures are not in response to imminent catastrophic attack, nor are they observable in the way 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 seem to exclude from the scope many of the risk-based cybersecurity measures that the U.S. and China for instance are implementing. 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. As a result, the national security exception is not available. It is also unlikely that most cybersecurity measures would fall under either of the other subparagraphs (a) and (b) in Article XIV bis.

The WTO 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.

An alternative view is less that cybersecurity might be excluded from the scope of GATS article XIV bis, but that GATS article XIV bis is so broad as to provide almost no limits on when governments can justify security measures (including cybersecurity measures).[161] According to this view, the reference by the Panel to an emergency in international relations including, along with defense and military interests "the maintenance of law and public order", as extending to a broad range of events could include cybersecurity measures.[162] In addition, the temporal link that the measure be taken in a time of the emergency in international relations could extend to time-unlimited cybersecurity measures.[163] In this event, the only effective boundaries in GATS Article XIV bis would be the requirement in the chapeau of good faith.

On any of the interpretations of GATS Article XIV bis, a cybersecurity measure also needs to be justified under the chapeau. 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

[160] Joel Trachtman, "The internet of Things Cybersecurity Challenge to Trade and Investment: Trust and Verify", p 26
[161] J.Benton Heath, "The National Security Challenge to the Economic Order", Yale Law Journal, Vol. 129
[162] Shin-yi Peng, "Cybersecurity Threats and the WTO National Security Exception, J. Int'l Econ. L. Vol 18, Issue 2
[163] J. Benton Heath, "The National Security Challenge to the Economic Order", Yale Law Journal, Vol. 129

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 effect, both approaches to the security exception lead to much the same outcome, namely a lack of an effective governance mechanism to mediate the cybersecurity/trade tradeoffs. However, should cybersecurity measures not fall within the scope of the security exception, governments will have to justify such measures under the general exceptions. Where this fails then the outcome is that a range of cybersecurity measures may be deemed WTO inconsistent.

Assessing cybersecurity measures under the general exceptions provision

A range of cybersecurity measures may 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.[164] Cybersecurity measures might also fall within, subparagraphs c(i) and c(iii) where aimed to protecting consumers from cybercrimes; c(ii) for measures aimed to protecting privacy on cybersecurity grounds, and c(iii) in the case of measures addressing network security. 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. The necessity requirement includes a weighing a balancing of the importance of common interests or values. Yet, without a common understanding of what is at stake, panels are either faced with making complex assessments about whether the risk say, of access to politically sensitive online content justifies a complete content ban? Given the political sensitivities of such decisions, a panel is more likely to defer to government claims of risk. In addition, 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 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.[165] 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.[166]

---

[164] 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.

[165] Appellate Body, Brazil-Retreaded Tyres, para 155.

[166] J. Benton Heath, The New National Security Challenge to the Economic Order", Yale Law Journal (forthcoming 2019)

Under the chapeau to GATS article XIV, 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 country, 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.[167]

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 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 the national security exception. 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."[168] This security exception is replicated in the U.S.-Mexico-Canada Agreement (USCMA) and the U.S.-Japan Digital Trade Agreement.[169] One consequence is to widen the scope for governments to justify a cybersecurity measure under such an 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.[170]

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. Moreover,

[167] WTO Appellate Body Report, "U.S.-Import Prohibition of Certain Shrimp and Shrimp Products", WT/DS58/AB/R (Oct. 12th, 1998), para 115-116.
[168] CPTPP Article 29.2.
[169] USMCA Article 32.2, US-Japan Digital Trade Agreement, Article 4.
[170] Mattoo, Aaditya and Joshua P. Meltzer. "Data Flows and Privacy: the conflict and its resolution." Journal of International Economic Law. Vol 21, Issue 4.

even where such evidentiary hurdles can be overcome, state practice suggests an unwillingness to give independent tribunals the authority to adjudicate and assess the complex factors that would be required under a 'necessary" analysis under a GATT/GATS general exception. This points to the need for international cooperation to establish standards and rules that can bound cybersecurity measures and channel cybersecurity measures into least trade restrictive alternatives. Some countries have started to develop cybersecurity trade rules in FTAs, though these are limited and more is needed.[171] What is clear is that given the expansion of what might constitute cybersecurity measures and the increasing economic importance of the digital economy, greater articulation of cybersecurity specific trade rules are needed, Yet such rules need to also be sensitive to what governments are willing for trade panels to adjudicate, taking into account the move towards making FTA security exceptions entirely self-judging. The following outlines what more is needed.

Develop a shared understanding of cybersecurity risk

As a first step, governments need to develop a common understanding as to the scope of cybersecurity and what could constitute a cybersecurity measure. While the nature of cybersecurity threats are evolving, there are doing so within the constraints of how technology exposes people and the economy to cyber threats through connections to the internet and the free flow of data. This paper outlines five key areas where governments see cybersecurity threats. These areas provide a workable starting point for a conversation as to what should constitute cybersecurity subject to specific trade rules.

Agree to a risk-based approach to cybersecurity

The notion of risk is central to cybersecurity. It is risk which animates cybersecurity measures and risk also provides a framework for its calibration. Risk-based cybersecurity measures are increasingly a global norm. Moreover, how to assess risk and determine what is needed to reduce it requires a risk assessment. 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."[172] 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." 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.[173]

A risk assessment could inform what cybersecurity 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 a thoughtful assessment of whether the steps taken are in fact reducing risk. Building an

[171] USMCA article 19.15
[172] OECD (2015) Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD 2015.
[173] USMCA Article 19.15.

effective approach to cybersecurity also requires engaging government and business leaders and building cyber risk management into the core of corporate and government practice.[174]

Trade rules that require regulation to be based on a risk assessment is not new. The WTO (and replicated in FTAs) includes a requirement that SPS measures are based on a risk assessment.[175] Risk assessment could help distinguish legitimate and tailored cybersecurity measures from protectionist and overly broad measures. Drawing on the use of risk assessments in the SPS agreement, requiring that cybersecurity measures are based on a risk assessment would not prevent governments from setting their desired level of risk, which could include zero risk.[176] Instead, a risk assessment is better seen as providing a procedural discipline, where evidence submitted and reasoning employed as part of the risk assessment can clarify what is at stake, what the alternative cybersecurity options are to achieve the desired level of risk, and makes it harder for governments to use cybersecurity as a form of disguised protectionism.

Develop global cybersecurity standards

Cybersecurity standards can build a common approach to addressing cybersecurity risks based on best practice.[177] For instance, the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) have developed a number of cybersecurity-related standards, including the jointly developed ISO/IEC 27000 series, as well as sector specific-standards for electric utilities, health care, and shipping.[178]

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. 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.[179] 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.

---

[174] Thomas Poppensieker et al, 2018. "Digital and Risk A new posture for cyber risk in a networked world", McKinsey & Company.
[175] SPS Article 5.1
[176] WTO Appellate Body Report, Australia-Measures Affecting the Importation of Salmon, WT/DS18/AB/R (Oct, 20, 1998), para 199
[177] Shin-yi Peng, "Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime", Cornell Int'l L. J. Vol 51, No. 2 Spring 2018
[178] IEC 61850, ISO/IEC 80001, IEC 61162.
[179] 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

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.[180] 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 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.[181]

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.[182] 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.[183] The challenge here of course is that these exceptions provisions are so broad as to justify most if not all restrictions on data flows for cybersecurity purposes.

Commit to good regulatory practice specific to cybersecurity

The development of good regulatory practice (GRP) has received some attention in the WTO TBT Committee and is an increasing feature of more recent FTAs.[184] Indeed, developing WTO

[180] Regulation (EU) 2010/881 of the European Parliament and of the Council of 17 April 2019 on ENISA.
[181] USMCA article 19.15(b).
[182] OECD (2015) Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD 2015 Publishing, Paris, Principle 7.
[183] CPTPP Articles 14.11, 14.13; USMCA Articles 19.11, 19.12.
[184] WTO, G/TBT/26; USMCA Article 28.2; see Benedick Kingsbury et al, "The Emergence of Global Administrative Law", IILJ Working Paper 2004/1

rules on good regulatory practice such as requirements of increased transparency and reason-giving are well articulated in administrative law and need to be extended, where appropriate, to the regulation making process used by the national security state.[185] In addition, GRP is likely a building block towards some of the forms of international regulatory cooperation outlined above.[186] Good regulatory practice can include process elements, such as transparency, consultation, and reason giving as well as commitments aimed at improving regulatory outcomes, such as being welfare maximizing and cost-effective, and when it comes to cybersecurity affecting digital trade, being least trade restrictive and not creating unnecessary barriers to trade.[187] From a narrower digital trade perspective, GRP should be developed to mainstream consideration of the impact of regulation on data flows as well as access to data. This can be done by requiring regulators to conduct a regulatory impact assessment that includes the impact on cross-border data flows. Having regulators consider digital trade effects as part of the process of developing the regulation can also help identify less trade restrictive options. In the digital trade context, the increasing economy-wide use of data means that GRP should also emphasize the importance of coordination among government agencies when developing cybersecurity regulation that effects data flows and digital trade.

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 justify 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

[185] Elena Chachko 2020, Administrative National Security, Georgetown Law Journal *forthcoming*
[186] OECD. "International Regulatory Co-operation and Trade: Understanding the Trade Costs of Regulatory Divergence and the Remedies." OECD Publishing, Paris., p. 34. 2017
[187] Basedow, Robert and Celine Kauffmann 2016. 'International Trade and Good Regulatory Practices: Assessing the Trade Impacts of Regulation." OECD Regulatory Policy Working Papers No 4.

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 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 specific trade rules for cybersecurity are needed. This paper has outlined, a range of possible issues to be addressed, including cybersecurity standards, commitments to risk-based cybersecurity measures, better sharing of information, and access to data. 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.