Cybersecurity and Trade: The Increasing Use of Cybersecurity Measures and their Impact on International Trade

Sydney Moulton

Graduate School of Public and International Affairs, University of Ottawa

Major Research Paper

Supervisor: Professor Patrick Leblond

19 April 2024

Table of Contents

Abstract *2*
Introduction *3*
The Intersection of Security and Trade *9*
Cybersecurity Risks *13*
Threat Actors **14**
Cyber Risks **15**
National Defense 15
Critical Infrastructure 16
Economic Cyber-Espionage 19
Collection and Falsification of Digital Information 20
Psychological Impacts **22**
Increase in Cyber Attacks **22**
Trade-Related Cybersecurity Measures *26*
Export-Related Trade Policies **28**
Import- and Investment-Related Policies **32**
Data Flow Restrictions **35**
Impact of Cybersecurity Measures *40*
Positive Effects: Market-Creating **40**
Negative Effects: Reduced Cybersecurity **41**
Negative Effects: Impact on Businesses **42**
Negative Effects: Impact on Trade **44**
Striking the Balance Through Global Cooperation *46*
Conclusion *48*
References *50*

Abstract

Rapid advancements in technology have resulted in the expansion of digital cross-border transactions, known as digital trade, which relies on cross-border data flows to facilitate the trade of goods and services around the world. Digital trade provides benefits for enterprises, allowing them to scale up faster, increase efficiency, and expand their customer base. However, the increased use of digital services that requires the large-scale collection of sensitive data has resulted in an increase in the frequency and scale of cyber-attacks as malicious actors attempt to exploit vulnerabilities in networks that lack the proper cybersecurity measures. This can be detrimental to national security, impacting national defense, critical infrastructure, and individual citizens whose information can be stolen and used for malicious purposes. To mitigate this risk, numerous governments have been imposing unilateral cybersecurity measures, such as restricting exports to and imports and investments from enterprises operating in certain countries that are deemed to pose higher risks to cybersecurity. Measures also include restricting cross-border flows of data to countries with insufficient cybersecurity standards or requiring that data be routed through certain countries. The requirement for more stringent cybersecurity increases opportunities for enterprises to fill existing market gaps. However, the multiple regulatory frameworks that enterprises are required to comply with depending on the market they are operating in increases costs, imposes barriers to trade, and has the potential to weaken cybersecurity, ultimately calling into question whether these measures achieve their objective. To prevent this and reduce tensions that may arise through allegations of digital protectionism, global cooperation is required to define the issue of cybersecurity and develop a framework for imposing measures that strengthen cybersecurity, with trade agreements being a useful tool to do so.

Introduction

International trade has been in a constant state of change due to the internet where every industry is now a digital industry, and the digital economy is now the economy (Ahmed, 2019). Digital cross-border transactions, known as digital trade, are becoming increasingly prevalent, enabled by cross-border data flows that reduce transaction costs and increase real-time resource management (Mishra et al., 2021). Digital trade can be defined as "digitally enabled transactions in trade in goods and services which can either be digitally or physically delivered and which involve consumers, firms, and governments" (Leblond, 2022: p.7). This is enabled using information and communication technology (ICT), which drives trade by reducing costs, creating new business opportunities, and makes it easier for small and medium-sized enterprises (SMEs) to do business internationally. Global digital trade, including e-commerce and digitally delivered services was valued at US $5.5 trillion in 2019 and amounted to approximately 25% of world exports (Tran, 2021). In 2019, Statistics Canada estimated that there was $336 billion worth of digitally ordered goods and services supplied in Canada, representing 6.8% of the total supply of goods and services (Leblond, 2022: p.13). Most of Canada's digital trade occurred domestically, with only 22% of Canadian businesses with online sales having customers in the US, and 11% with customers outside of Canada and the US (Leblond, 2022: p.14). Nonetheless, digital trade, whether done within or outside Canadian borders relies on the cross-border flow of data to facilitate transactions.

The digital economy relies on growth in the production and the use of data, requiring these global flows for innovation and access to hardware and software for production and delivery (Meltzer, 2020). Digital trade not only plays a crucial role in facilitating trade in digital goods and services, but as well as trade in tangible goods, underpinning global value chains and related customs processes (Lippoldt, 2023). This increased reliance on data and cross-border

flows greatly benefits the global economy, increasing interconnectivity (Ahmed, 2019). The use of cloud computing - the delivery of computing services over the internet - promotes innovation and efficiency for businesses and consumers alike as it provides on-demand self-service, enables communication between platforms, and supports multiple users simultaneously, overall increasing the provision of service (Akremi & Rouached, 2021).

However, as digital connectivity grows, enabled by the large-scale collection, storage and movement of data, so does the risk and cost of cyberattacks (Meltzer, 2020). Cybersecurity falls into four broad categories, including military cybersecurity, economic cybersecurity, political cybersecurity, and societal cybersecurity, where each risk impacts the ability of the state to function properly and jeopardizes trust in the institution (Huang et al., 2021). There is an increased concern around cybersecurity risks, with five main areas of concern for governments, each of which could result in physical and economic consequences: national defense, critical infrastructure, economic cyber-espionage, digital information (including the collection and falsification or manipulation of information), and access to technology that could be used to carry out future cyberattacks (Meltzer, 2020). In addition, attacks can create damage through undermining societal cohesion and trust in government institutions, resulting in longer term and more insidious consequences (Shandler and Gomez, 2023). As a result, governments have imposed certain cybersecurity regulations to mitigate the occurrence and effect of these attacks.

Cybersecurity is defined by the US National Institute of Standards as "the prevention of damage to, unauthorized use of, exploitation of, and - if needed - the restoration of electronic information and communication systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems" (Meltzer, 2020: p.7). It is the ability of an actor to protect itself and its institutions against cyber risks, such as those outlined

above. Cybersecurity covers three domains that must be protected to ensure unauthorized access into a network is prevented: computer security, data security, and network security (Dutta et al., 2022). Computer security refers to the protection of computer systems, in which the primary function is to protect, update, and patch the machine. Data security is the process of protecting data from unauthorized access ~~of~~ by malicious actors. Finally, network security is the protection of all ICT devices connected to the network. With each domain comes a unique ability for malicious actors to exploit security vulnerabilities and the global interconnectedness of networks poses a unique risk.

To protect against cyberattacks, governments can implement policies to regulate import and export activities, as well as data flows across borders to manage cybersecurity risks. Import-related policies on goods often prohibit certain imports, require authorization or registration to regulate imports, or require specific testing and inspections of the security mechanisms of the goods before entering the market. Cybersecurity has become a focus for export controls, preventing the export of certain items due to the possibility that they could be used for surveillance, cyber-espionage, or network-disrupting activities (Customs and International Trade Law, n.d.). Policies on digital services can include data flow restrictions or mandatory intellectual property disclosure. Data flow restrictions include data localization policies, which require the processing or storage of data in an electronic format to be limited to a particular geographical area or jurisdiction (Weber, 2018). Policies such as this are intended to increase security by ensuring that the data is stored in a country with adequate protections and is subject to domestic laws. Additional policies can also include the requirement of cybersecurity certifications for firms to conduct business in specific areas, demonstrating compliance with

specific legislation such as the European Union's General Data Protection Regulation (GDPR) (Process Unity, 2022).

Trade and cybersecurity are increasingly intertwined, in both positive and negative ways. The objective of cybersecurity is to protect a state's infrastructure and companies' intellectual property from malicious actors. Therefore, policies that increase cybersecurity can increase trust, playing a role in facilitating trade. There are significant benefits to having a secure cyber environment which can attract investment in certain jurisdictions. However, in certain instances, unilateral cybersecurity measures that have been imposed, such as data localization requirements and import and investment restrictions on data and ICT products, specifically from countries along supply chains where cyber risk is high, potentially violate trade agreement commitments and hinder trade. These measures can act as non-tariff barriers (NTBs), which are regulations or administrative measures that prevent a good or service from being traded internationally or impose additional costs to comply with regulatory or administrative requirements (Leblond, 2022). NTBs have a negative impact on trade, reducing market access.

Security requirements and international trade are often conflicting, where both demand that one takes precedence over the other (Pinchis-Paulsen, 2022). However, there is a general understanding that security concerns, national or global, trump international trade. This can be inferred from the inclusion of exceptions into trade agreements, modeled after Article XXI of the General Agreement on Tariffs and Trade (GATT) 1994. Exceptions used in trade agreements signal to parties that policy concerns such as security are not subordinate to trade objectives (Henckles, 2020). These measures often give governments greater discretion in defining security concerns, by permitting a government to adopt measures "it considers necessary" in the situation. Exceptions to treaty obligations are the main tools to achieve a balance between trade

liberalization and national interests, two ideas that again, may be contradictory (Mantilla Blanco & Pehl, 2020). In addition, World Trade Organization (WTO) members have been using security exceptions with more frequency, including those citing cybersecurity concerns (Pinchis-Paulsen, 2022). The increased interdependence of supply chains can result in what can be referred to as weaponized interdependence, where states with a large amount of power and control, relative to other states, can control and manipulate a supply chain for geostrategic objectives (Farrell & Newman, 2019). While in some cases this can reflect a valid security claim, it has resulted in an increase in claims of digital protectionism, in which certain measures such as those mentioned previously, are not justifiable security measures but instead are used to distort trade, favouring domestic producers over foreign competitors (Aaronson, 2019). This is an issue that is difficult to mitigate at a multilateral level for two reasons. First, there are conflicting opinions on what constitutes cybersecurity measures, as measures can cover a number of vulnerabilities, from infrastructure to data flows, and what one country may deem necessary to protect cybersecurity, another may label as protectionism (Meltzer, 2020) Second, cyber risks challenge the temporal requirement of the security exception in Article XXI, which states that trade-restrictive measures must be "taken in time of war or other emergency in international relations" (GATT, 1994: Article XXI(*b*)(*iii*)). To reduce the risk of attack, cybersecurity measures often need to be imposed continuously, potentially restricting trade on an ongoing basis.

The reality is that security concerns, and more specifically cybersecurity measures that address these concerns, impact international trade. These measures, both positive and negative, are analysed in the following chapters. While the paper's focus is on cybersecurity measures which is oftentimes directly associated with the digital realm, the impact is not just on digital

trade, but all forms of trade, including those in physical goods. This is an important consideration throughout the paper.

The paper is divided into four parts. First, it discusses the theoretical nexus of security and trade, specifically the national security exception in the GATT and its relevance to cybersecurity, providing some justification for why certain measures can be imposed and the challenges in determining the legality of these measures.

Next, it outlines the cyber environment, discussing the risks that exist and, therefore, the necessity for cybersecurity strategies that encompass policies to ensure a more secure environment. Specific policies are then discussed, leading into a discussion of their impact on trade, both positive and negative. The paper concludes with a discussion of building global consensus on cybersecurity measures through embedding principles into trade agreements, with the intention of pre-emptively outlining the accepted use of trade restrictive measures on the basis of protecting cybersecurity without engaging in digital protectionism.

The Intersection of Security and Trade

The multilateral trading order was built on three main ideas (VanGrasstek, 2013). First, countries are sovereign and control direction of their affairs, but the most effective way to exercise their sovereignty is to voluntarily enter into binding agreements with other states that place mutual limits on their sovereignty. Second, countries will mutually gain from freer trade. And third, the ideas underlying the world trading system would result in military power playing a less important role in international affairs, and countries would be bound and constrained in their actions by law or mutual self-interest. As a result, WTO members are expected to follow principles that liberalize trade, such as most-favoured nation (MFN) treatment outlining that countries cannot discriminate between trading partners,[1] and national treatment (NT) in which imported and domestic-produced goods are treated equally within the market (WTO, n.d.a). However, some exceptions to these principles exist, such as General Exceptions outlined in Article XX of the General Agreement on Tariffs and Trade (GATT), which revolve around the protection of the environment, human rights, and the like (GATT, 1994). In addition to the General Exceptions that allow members to derogate from their obligations, a number of security exceptions under the WTO umbrella allow governments to restrict trade when it is deemed necessary to protect their security interests (Peng, 2015). These provisions include Article XXI of the GATT 1994, Article XIV *bis* of the General Agreement on Trade in Services (GATS), Article 74 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS), and Article XXIII of the Agreement on Government Procurement (GPA). Additionally, provisions may be

[1] An exception to the non-discrimination principle occurs when two or more countries sign a Regional Trade Agreement (RTA), in which signatories have more favourable market-access conditions (WTO, n.d.b). WTO members can enter RTAs, provided they follow the rules set out in Article XXIV of the GATT 1994, the Enabling Clause, and Article V of the GATS. RTAs generally must cover almost all trade between signatories without raising barriers for non-signatories.

included in bilateral or regional trade agreements (RTAs) such as those outlined in Article 32.2: Essential Security in the U.S. – Mexico – Canada Agreement (USMCA) (USMCA, 2019).

The inclusion of exceptions in trade agreements demonstrates that while the fundamental principle is that states mutually gain from freer and open trade, it should not constrain them from protecting their essential security interests (Henckles, 2020). While this has been a long-existing principle, there was an understanding that liberalization of trade and increasing interdependence was the rule and measures to protect essential security interests were the exception (Pinchis-Paulsen, 2022). For years, this seemed to be the case. Since the WTO's establishment in 1995 until the 2010s, the security exception was rarely invoked by states (Mantilla Blanco & Pehl, 2020). However, there has recently been a shift, whereby security interests are increasingly used to justify trade-restrictive measures; trade policies are increasingly reflecting an underlying national security mindset (Pinchis-Paulsen, 2022).

Article XXI of the GATT poses challenges for interpreting security measures and whether they constitute valid exceptions. Article XXI(b) states that:

> *Nothing in this Agreement shall be construed*
>
> *(b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests*
>
> *(i) relating to fissionable materials or the materials from which they are derived;*
>
> *(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;*
>
> *(iii) taken in time of war or other emergency in international relations*

The seemingly self-judging nature of this exception, outlined by "which it considers necessary for the protection of its essential security interests" has made it difficult in determining how to test whether a measure invoked is sufficiently protecting an essential security interest. The WTO Panel Report in *Russia – Measures Concerning Traffic in Transit* was the first attempt by the WTO to clarify the security exception (Russia – Measures Concerning Traffic in Transit, 2019). In its report, the Panel made three important judgements (Vidigal, 2019). First, it determined that the Panel and the Appellate Body have jurisdiction to judge the security exception. Second, an event that constitutes an "emergency in international relations" can be subject to objective determination by a WTO Panel. And third, the Panel interpreted the self-judging aspect as subject to objective determination, setting out two requirements for a measure to be justified (Vidigal, 2019). First, the WTO Member must explain which 'essential security interest' that the measure seeks to protect, and second, the measure must actually be capable of protecting this security interest. They concluded that an emergency in international relations requires a higher threshold, involving 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 … giv[ing] rise to … defence or military interests or maintenance of law and public order interests" (Vidigal, 2019: p.212).

While the panel report may have further clarified the security exception relating to traditional security concerns and the balance of trade and security concerns, the unique nature of cyber-attacks and cybersecurity measures poses challenges for applying this interpretation (Meltzer, 2020). First, cybersecurity policies are based on the assessment of risk and often not in direct response to a significant and current attack, and therefore are adopted over a longer term. The risk is ongoing and constantly monitored by states that are implementing measures to protect

their essential security interests. As a result, the temporal nature of the WTO Panel Report requiring the objective assessment of whether the measures were in response to an "emergency in international relations" would automatically exclude cybersecurity measures even if they are deemed by the state as protecting essential security interests such as critical infrastructure or sensitive information through the restriction of trade flows.

As states increasingly adopt risk-based measures, which Pinchis-Paulsen (2022) argues increasingly resemble using trade and control of supply chains to advance geostrategic objectives, the issue remains in determining the legality of these measures due to the lack of clarity from the WTO on risks and measures such as these. As a result, there is currently no objective way to determine if states are balancing trade and security objectives in line with WTO obligations, and the issue remains in determining whether these policies are legally justified or protectionist. Regardless, the existence of security exceptions and the lack of legal clarity on the nature of these exceptions have provided states with the increasing ability to cite what they deem essential security interests to adopt trade-restrictive measures to protect their national interests, regardless of whether these violate WTO obligations. As cybersecurity risks grows, the prevalence of this situation will only increase. As a result, it is important to understand the factors prompting the emergence of cybersecurity policies and their potential implications on the flow of international trade.

Cybersecurity Risks

A cyber risk can be defined as “any risk that may result due to financial losses, any kind of disruption, or damage to the reputation of an organization” (Priyadarshini & Cotton, 2022: p.241). This can result in the failure of an organization’s information technology (IT) systems. The exponential and rapid innovation and growth of technology has heightened cyber risk, with malicious actors increasingly gaining unapproved access to an organization’s information (Priyadarshini & Cotton, 2022). This is due in part to: the increase in the collection and storage of data, including personally identifiable information (PII); the expansion of the Internet of Things (IoT), resulting in an increase in the number of devices that are connected in a data exchange; and the global interconnectedness of organizations that require employees, customers, and third-party vendors around the world to have near instant access to their network to function efficiently. The Internet of Things (IoT) is expanding quickly, where physical equipment is becoming more and more digitized, with networks established between machines, humans and the Internet, allowing the physical world to be controlled digitally (Tripathy & Anuradha, 2017). Experts predict that 41.6 billion devices will be connected by 2025, with 5G networks allowing more devices to connect to networks at higher speeds (CCCS, 2022b). The complexity of the code running these devices has increased, with software and firmware systems operating with codebases that are both large in size and dependent on third-party code.

This has resulted in an expanded threat surface, defined as “all information systems and services a cyber threat actor may exploit in trying to compromise an individual, organization, or network” (CCCS, 2022a: p.4). The threat surface includes networks, personal computers, mobile devices, IoT devices, and servers, as well as the processes that communicate with or rely on the information systems connected to the internet (CCCS, 2022a). This growth and reliance of

organizations, private and public sector alike, on technology increases the risk of a cyber-attack by threat actors (Priyadarshini & Cotton, 2022: 241).

Threat Actors

Cyber-threat actors are defined by the Canadian Centre for Cybersecurity (CCCS) as "groups or individuals who, with malicious intent, aim to exploit weaknesses in an information system or exploit its operators to gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks, including the authenticity of the information that flows to and from them" (CCCS, 2022a: p.2). These actors can be governments, cybercriminals, hacktivists, insider threats, terrorist groups, and thrill seekers; their motivation and level of sophistication varies. Advanced persistent threats (APTs) are those with the highest degree of sophistication, where they can use multiple ways of attacking, either through cyber, physical, or deceptive means, to achieve their objectives (CISA, n.d.). The objectives of APTs typically include establishing a presence within the information-technology infrastructure of targeted organizations, with the intention to export information, undermine or impede critical aspects of a mission, program, or organization. This can be done immediately when access to the network is gained, or APTs can position themselves to carry out these objectives in the future when the opportunity presents itself, avoiding detection in the meantime. These groups are often state actors or state-sponsored groups, with the intention of espionage, data theft, and network or system disruption or detection (CCCS, 2022a). Over the past few years, there have been several APT groups linked to attacks in Canada that have warranted federal policing investigations in the APTs that have been targeting Canadians, the Government of Canada, and critical infrastructure systems (Public Safety Canada, 2022).

A second prolific actor, cybercriminals, are those who are mainly financially motivated, operating on a broad mass of victims, often stealing personal or organizational data and selling it

on the dark web (Dutta et al., 2022). As cybercriminals become more advanced, so too do their ability to make profits, engaging more often in ransomware attacks on critical infrastructure due to the potential massive payoffs (CCCS, 2022b).

Cyber Risks

The risks posed by the actions of these threat actors can result in compromising national defense, attacking critical infrastructure, conducting economic cyber-espionage, collecting or falsifying digital information, and accessing critical technology (Meltzer, 2020).

National Defense

There is a risk that threat actors will use cyberattacks to hack into defense industries, compromising defense capabilities (Meltzer, 2020). Numerous examples of this exist, in which threat actors can target defense departments directly or indirectly through third parties connected to the network (Centre for Strategic and International Studies, n.d.). In September of 2023, Russian hackers, using a ransomware known as “LockBit”, stole thousands of documents from the British Ministry of Defense and uploaded them to the dark web. The breach occurred through a Windows 7 PC running software for Zaun, a British fencing company with multiple government contracts, providing fencing services for prisons, military bases, and utilities (Zaun, 2023). From there, hackers were able to gain backdoor access to Ministry files, where it was confirmed that some of the data was published on the Dark Web. While Zaun claimed that the data stolen was historic and that no classified information has been compromised, the intention of this attack to gain information relating to national defense was clear, and the results of which could have been potentially catastrophic. In another example, in November of 2023, Chinese cybercriminals targeted Cambodian government networks, including National Defense, disguising themselves as cloud storage services to hide their data exfiltration. Initial research

demonstrates that this is part of a broader Chinese espionage campaign, targeting government data (Centre for Strategic and International Studies, n.d.). Thus, the risk to national defense is one to be taken seriously.

Critical Infrastructure

Critical infrastructure is defined by the Canadian Centre for Cybersecurity as "the processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government" (CCCS, 2021: p.6). Operational technology (OT) manages critical infrastructure and plays an important role in national security. It is the hardware (and now software) that is integrated into devices that is used to monitor and create change in the physical world. OT is used in industry and in critical infrastructure within the industrial control systems that monitors mission-critical industrial processes. The automation of industrial processes across sectors like manufacturing and resource extraction, and infrastructure providing electrical, natural gas, and water services is due to the use of OT. As OT is being transformed, it is now being used to automate other important sectors like building management, municipal services, transportation, and healthcare – all of which are essential to the proper functioning of society.

Operational technology systems were required before the internet and therefore were not created with cybersecurity principles embedded due to the isolation from external threats (CCCS, 2021). However, in order to improve processes and create smarter and more efficient operations, OT has adopted data processing and communications capabilities, with the global market for smart OT devices growing at approximately 8% a year. As more OT is accessible from the Internet or untrusted networks the exposure to cyber threats grows. These systems are uniquely exposed to cyber threats for a number of reasons.

The systems were designed to prioritize personal safety and process reliability over data security due to the nature of the operations. OT systems oftentimes manage equipment that are exposed to extreme conditions such as high temperatures and pressures, dangerous chemicals, radiation, or high voltages, and the failure of the OT could result in the costly shutdown of an entire industrial process. As cybersecurity principles were not the main consideration, OT hardware and software may be upgraded and patched less frequently, communication protocols may lack encryption, authentication, or integrity protection features, and may lack general security functions like intrusion detection. These security functions could delay communication or take the system offline for a period of time, and this, in combination with being permanently connected to the network, increases susceptibility for cyber threat activity by expanding the threat surface (CCCS, 2021).

Critical infrastructure providers store large amounts of sensitive or valuable information that can be targeted directly or indirectly from a variety of actors (CCCS, 2022b). Direct threats often come from two main sources: financially motivated, medium-sophistication cybercrime groups, and politically motivated, high-sophistication state-sponsored cyber threat actors (CCCS, 2021). Cybercriminals recognize the importance of critical infrastructure and, thus, choose targets in which the ransom payoff could be larger, and the amount of either personal or business data stolen could be greater for higher profits on the Dark Web. Ransomware attacks by cybercriminals could be enough to force OT asset owners to shut down some or all of their industrial operations for safety or business reasons. In May of 2021, the hacking group DarkSide forced the shutdown of Colonial Pipeline, the largest pipeline for transporting petroleum products in the United States (Wood, 2023). This resulted in the shutdown of Colonial Pipeline’s operations for five days, creating gasoline shortages, record prices, and panic buying.

State-sponsored cyber activity against critical infrastructure has become more prominent in global cyber-threat activity in the last decade (CCCS, 2021). There are several reasons governments would target critical infrastructure, including espionage, theft of commercial IP, messaging of intent, and prepositioning for sabotage. The CCCS assesses that the targeting of critical infrastructure is likely done to collect information and pre-position cyber tools for follow-on activities, or as a way to demonstrate state cyber power (CCCS, 2021). State-sponsored cyber-attacks on critical infrastructure began in 2015, when cyber actors hacked into three power distribution centres, cutting off power for over 230,000 Ukrainian residents (CCCS, 2021; Zetter, 2016). Ukraine's intelligence community attributed the attack to Russian hackers, with cybersecurity experts arguing that the way the attack was carried out was a form of power-signaling to Ukrainians by the Russian government (Zetter, 2016).

Indirect attacks against critical infrastructure target the supply chain, typically for two reasons: to obtain commercially valuable IP and information about the system or to indirectly access the OT network and eventually the critical infrastructure (CCCS, 2021). As supply chains are increasingly integrated and digitized, critical infrastructure operators rely on a wide variety of supply-chain products and services, both physical and digital. The increased use of the Internet, cloud, and outside service providers increases dependency, resulting in more vulnerabilities in the supply chain and giving actors inside information and the ability to find new ways to access critical systems. A supply-chain compromise occurs when products are purposefully exploited and transformed before they reach the final customer, and can include actions such as adding malicious additions to legitimate software used by companies, tampering with the end product of a given vendor so that it carries a valid signature allowing it to access various organizations without the end-user knowing, or altering hardware to manipulate access to sensitive

information. The CCCS assesses that supply-chain compromises are very likely an active and increasing threat to OT and, by proxy, critical infrastructure security, mainly through software compromises that can include malicious hardware alterations.

A prominent example of this is that which affected SolarWinds, a large software company based in the United States, providing system management tools for network and infrastructure monitoring, as well as technical services to organizations around the world (Oladimeji & Kerner, 2023). Orion is SolarWind's performance monitoring system, which has privileged access to IT systems for more than 30,000 public and private organizations. Hackers perpetrated a supply-chain attack, inserting malicious code into the Orion system, allowing them to gain backdoor access to 18,000 SolarWinds customers when the company unknowingly sent out Orion software updates with malicious code embedded. This attack affected both public and private organizations, including the US Departments of Homeland Security, State, Commerce, and Treasury, as well as companies such as Microsoft, Intel, Cisco, and Deloitte.

The number of attacks from cybercriminals on critical infrastructure is growing. In its 2023-24 National Cyber Threat Assessment, the CCCS highlights the increase in attacks on healthcare organizations, with over 400 organizations since March 2020 in Canada and the US experiencing a ransomware attack (CCCS, 2022b: p.11). This is in addition to an increase in activity against municipal and provincial governments, with over 100 cases of cyber-threat activity targeting Canadian municipalities since the beginning of 2020 (CCCS, 2022b: p.11).

Economic Cyber-Espionage

Malicious actors, most frequently including state-sponsored actors and cybercriminals, can use the interconnectedness of the Internet to hack into commercial enterprises, stealing intellectual property, information on foreign intelligence operations, covert equipment and materials, and

violate export controls (Meltzer, 2020; CCCS, 2022b). The purpose of these operations is to share stolen information with state-owned enterprises or domestic industries to bolster their economy and increase competitiveness. The consequences of this can be lost revenue, reputational damage, or lost investment in research and development. In 2021 and 2022, it was observed by the CCCS that state-sponsored actors are conducting such operations for financial gain, oftentimes to reduce the impact of international economic sanctions. Chinese, Russian, Iranian, and North Korean state-sponsored cyber actors pose the biggest risk to Canadian organizations, with the likelihood that these states will continue targeting Canadian organizations for their domestic economic development. The threat from China is identified as the most significant in volume, capability, and intent and will very likely continue to target Canadian industries and technologies that can contribute to their strategic priorities.

Collection and Falsification of Digital Information

As data is collected, analyzed, and disseminated at ever-increasing speeds, including personal, consumer, and government data, it increases the risk for personal information to be stolen or falsified (for misinformation, disinformation, and malinformation [MDM] purposes) by malicious cyber actors (CCCS, 2022b). There is a significant value for actors who invade the privacy of individuals and steal data. The incentives for cybercriminals are profits, where customer information can be stolen and sold on the Dark Web (Mikalauskas, 2023). Pieces of Personally Identifiable Information (PII) can be linked together by cybercriminals, creating real or fake identities and used to access credit cards or steal funds from bank accounts. Information that includes a full range of documents required for identity theft could be worth USD$1,010 on the Dark Web. Information can also be stolen by state-sponsored actors for the purpose of

identifying government spies or blackmailing government officials into committing espionage (Fazzini, 2019).

The collection of sensitive personal information by a foreign entity, whether state-sponsored actors or cybercriminals, is now seen as a national security threat (Melzter, 2020). The CCCS outlines the threats impacting Canadians, including foreign states targeting Canadian individuals in two main ways (CCCS, 2022b). First, the targeting of diasporic populations and activists in Canada, in which adversarial states have interests in monitoring and disrupting the activities of Canadians who are believed to threaten their domestic security and stability.

Second, the targeting of personally identifiable information that could compromise individuals, including Canadians in widespread data-theft campaigns. There has been a rising occurrence of state-sponsored actors targeting widely used platforms to access information of sometimes hundreds of thousands of victims around the world. Two incidents highlight this risk. In March of 2021, Microsoft discovered vulnerabilities that were being exploited by hackers, which they attribute as HAFNIUM, a Chinese state-sponsored hacking group (Microsoft, 2021). In what is thought to be an attempt to steal IP and acquire personal information, 400,000 servers globally were affected by this activity (CCCS, 2022b). Emails were stolen from multiple targets and malware was installed by the hackers to continue surveillance of targets (Conger & Frenkel, 2021).

In September of 2017, Equifax, a US credit reporting agency, announced it had experienced a data breach, exposing the personal information of 147 million people, including the names, date of birth, and Social Security numbers of almost all these individuals (Sloan & Warner, 2019). A vulnerability, known to Equifax, alerted to them by both the software provider and the Department of Homeland Security United States Computer Emergency Readiness Team,

was not patched, leading to the data breach. However, this information has not surfaced on the Dark Web, leading senior intelligence officials to believe that whoever stole the data, likely a state actor, is combining the information with other stolen data, using it to identify US spies to gather information on who could be targeted to commit espionage against the United States.

Psychological Impacts

The impacts of cyberattacks are not only financial or physical, but can have longer term, psychological impacts, like undermining societal cohesion and trust in government institutions (Shandler & Gomez, 2023). A study done following a ransomware attack in Germany that disrupted operations at a hospital provided strong evidence that exposure to cyber-attacks lowers the public's confidence in their government. The public perceives the government as ultimately responsible for defending critical infrastructure and public institutions against cyber-attacks, and when an attack occurs, trust in government is lost. After cyber-attacks, governments do not benefit from the "rally around the flag" effect, which argues that foreign attacks against domestic targets increases public support in the short-term for leaders and government institutions. The nature of cyber-attacks differs as it is difficult to attribute the attack to certain actors, and the increasing quantity of cyber-attacks is leading the public to believe governments cannot combat them, creating an overwhelming sense of helplessness. Each of these factors can lead to a lack of public confidence and increased distrust in governments, which can be part of foreign adversaries' strategy and the ultimate, long-term goal of cyber-attacks.

Increase in Cyber Attacks

The increase in the frequency and scale of cyber-attacks can be explained by a number of reasons. First, the amount and availability of data is growing rapidly, which has resulted in the creation of "big data" (Google, n.d.). Big data is defined as "extremely large and diverse collections of structured, unstructured, and semi-structured data that continue to grow

exponentially over time" (Google, n.d.: para. 1). As a result of their large-scale data collection, datasets have grown so large and complex in volume, velocity, and variety that traditional data-management systems are unable to store, process, and analyze them. Big data provides significant benefits for internet users, including individuals and businesses, because it allows for improved decision-making, provides better customer experiences, makes operations more efficient, and improves risk management, among other things. However, managing this data also poses some risks. The sheer volume requires big storage, whether this is stored in the cloud or on the premises of the provider. The dispersion of the data across many storage platforms, oftentimes in multiple jurisdictions makes it difficult for providers to continuously ensure that data processing and storage meet data privacy and regulatory requirements. Most notable, it contains complex and valuable business and customer information, making it a high-value target for attacks. Because the data can be stored in various forms, it can be harder to implement the required strategies and policies to protect them. This expands the threat surface, resulting in a higher risk.

Second, advancements in technology, as previously discussed above, have resulted in more devices being digitally connected, expanding the network and ultimately the threat surface and the way malicious actors can access the network (CCCS, 2021). Additionally, the proliferation of the use of generative Artificial Intelligence (AI) has the potential to increasingly expose companies to vulnerabilities that can be exploited (Zaki, 2023). 75 percent of cybersecurity professionals saw an increase in attacks in 2023 and 85 percent of these attributed this rise to malicious actors using generative AI, and its ability to make organizations more vulnerable to cyber-attacks (Deep Instinct, 2023).

Third, current geopolitical instability has increased the risk of cyberattacks. Approximately 93 percent of cybersecurity experts and 86 percent of business leaders believe that geopolitical instability will lead to a catastrophic cyberattack in the next two years (Raina, 2023). Cyberattacks are an important part of the geopolitical risk outlook, as they can be used by actors to achieve political or financial ends (S&P Global, n.d.). The large-scale accumulation of data has provided the opportunity to shape political discourse through disinformation, where adversarial states are using data as a strategic resource (Office of the Director of National Intelligence, 2023). States can focus on collecting Personally Identifiable Information that can make their espionage, influence, and cyber-attack operations more effective. In recent years, critical infrastructure has been an attractive target. In its risk outlook, S&P Global (n.d.) alleges that hackers have maintained a campaign of cyber-attacks against Ukrainian, NATO, EU, and other Western entities, often targeting government and defense-related organizations, with cyber-security analysts suggesting that hackers affiliated with Russian military intelligence are becoming more aggressive and direct in their attacks. The NotPetya attack of 2017 can be used as a cautionary tale of the catastrophic damage that could occur once again with an attack of this scale. NotPetya is described as “the most destructive cyberattack in history,” causing over US$10 billion in quantifiable damages (Buchanan, 2020: p.302). NotPetya was a Russian attack on Ukraine, striking more than 300,000 major organizations in the country, affecting nearly every federal government agency in Ukraine. It damaged everyone conducting business in Ukraine and paying taxes to the Ukrainian government. However, the attack was not contained to Ukraine, affecting global corporations including Maersk, a major shipping company with approximately 15 percent of the global market, FedEx, and Merck, a major pharmaceutical company that was required to temporarily shut down production of an HPV vaccine due to the

attack. The attack was intended as a reminder of the strength of Russian hackers and the aggressiveness of the Russian state and highlighted the reality that “ordinary people and businesses cannot escape geopolitically motivated cyber operations” (Buchanan, 2020: 302).

The reality is that the cyber-threat surface is expanding, actors are becoming more sophisticated, and large-scale collection and storage of data along with technological advancements have increased the risk of cyber-attacks. With an increase in geopolitically motivated cyber-attacks, states are increasingly imposing cybersecurity measures to mitigate these risks. These measures are explored in the next chapter.

Trade-Related Cybersecurity Measures

Three main domains of cybersecurity need to be protected to mitigate risks: computer security, data security, and network security (Dutta, 2022). Computer security refers to the protection of the computer system – hardware, firmware, and software – from unauthorized access. Data security refers to the measures used to protect critical data from unauthorized access. Network security protects the entire network – made up of wired, wireless, and cellular connections – from unauthorized access. The "CIA triad" – confidentiality, integrity, and availability – is the guiding model for information security and outlines three principles that are to be maintained (Wilson, 2021). Confidentiality refers to the principle of keeping information confidential by encryption. Integrity refers to ensuring that information transferred is correct and reliable. Availability requires that data is accessible when required. These three principles are to be kept in consideration when organizations are implementing cybersecurity measures.

Cyber risks pose issues for governments in terms of national security; therefore, oftentimes governments take a leading role in ensuring that cybersecurity is up to a certain standard (Huang et al, 2021). Government strategies to address cybersecurity risks can be divided into three categories: information disclosure, implementation of trade policies, and cyber-trade norm development in the international arena.

Information disclosure refers to the government's use of guidance to share information and direct private actions on cybersecurity issues to increase awareness and the minimum standards of cybersecurity needed (Huang, 2021). Often, this requires imposing regulations on the private sector, which plays an important role in maintaining cybersecurity, as it owns and operates the majority of cyberspace (Hoffman & Nyikos, 2018). A substantial amount of defense and domestic security work is carried out by the private sector; it supplies and maintains a significant amount of technology used by governments; and it is responsible for the operation

and maintenance of critical infrastructure (Etzioni, 2014). While the adoption of strong cybersecurity measures by a private company can attract more customers, oftentimes there is not a strong enough business incentive to have the adequate high level of cybersecurity measures required. Etzioni (2014) outlines four reasons why the private sector may have a weak response to cyber-attacks and not have adequate cybersecurity measures. First, while corporations are mainly profit-driven and it may be presumed that they would want to enact strong cybersecurity measures to protect trade secrets and profits, this rational decision is not always made. Business decisions are increasingly made while considering the short-term costs of increased cybersecurity measures instead of the long-term benefits of protection; therefore, firms fail to make the proper investment on their own accord. Second is the argument that government mandates reduce cybersecurity and private-sector innovations by failing to allow private companies flexibility through the imposition of stringent or inefficient cybersecurity measures. Third, some private-sector representatives have argued that the cybersecurity measures that would be imposed would be a significant cost to the private sector, which would be incapable of meeting profitably. They also argue that, as the provision of security is the government's role, then the private sector should be compensated for cybersecurity costs. Finally, the private sector has expressed concern that reporting regulations for cybersecurity breaches result in damaging publicity and lead to lawsuits alleging damages to private citizens. As a result, the private sector has been reluctant to adopt stringent cybersecurity standards.

Governments can also promote the development of cyber trade norms through international bodies such as the WTO and through harmonized trade policies that incorporate cybersecurity (Huang et al., 2021). While trade agreements have included security exceptions as noted previously, the incorporation of cybersecurity measures into trade policy have become

more common since the Trans-Pacific Partnership (now the Comprehensive and Progressive Agreement for Trans-Pacific Partnership) was signed in 2018, because of its chapter on electronic commerce (Keitner & Clark, 2019). The USMCA, which entered into force on July 1, 2020, includes a chapter on digital trade, which is based on the CPTPP's chapter on electronic commerce; it takes a risk-based approach to cybersecurity and increased personal information protection. Singapore has concluded four Digital Economy Agreements, with Chile and New Zealand, Australia, the United Kingdom, and Korea (Ministry of Trade and Industry – Singapore, n.d.). The purpose of these agreements is three-fold: 1) to align digital rules and standards and create interoperable systems; 2) to support cross-border data flows and protect personal data and consumer rights; and 3) to encourage cooperation in terms of digital identifies, Artificial Intelligence (AI), and data innovation, allowing for the trialling of technologies across countries.

For the most part, however, trade agreements have not kept pace with the complexities of the digital economy and the requirements for cybersecurity measures (Claussen, 2020). This has resulted in measures taken outside of these agreements being imposed to manage cybersecurity risk. These measures include import- and export-related trade policies, data-flow restrictions, foreign-investment restrictions, mandatory intellectual-property disclosure, licensing requirements, and supply-chain reviews. These measures are this chapter's focus.

Export-Related Trade Policies

Export controls can include export licenses, quotas, prohibitions, certifications, and quantitative restrictions that control export numbers or prohibit certain identified exports (Huang, 2020). These controls are domestic mechanisms that are used to control a country's outbound trade of military-use and dual-use goods because of national security concerns (Whang, 2020). Export controls have existed since WWII, aligned with the national security policies of states to restrict

the international proliferation and limit the development of military-use technology by so called hostile states. A number of multilateral agreements outlines the goods and technologies that are subject to export controls, including the Wassenaar Arrangement, the Nuclear Suppliers Group, the Missile Technology Control Regime, and the Australia Group relating to chemical or biological weapons (Government of Canada, 2023). The Wassenaar Arrangement on Export Controls for Convention Arms and Dual-Use Goods and Technologies focuses on the transfer of conventional arms and dual-use items that are not banned for transfer but rather subject to export control regimes by over 40 participating states (Korzak, 2020). There has been an increased focus on cyber technologies added to the Arrangement's export-control list, specifically those items concerning IP network surveillance systems and items related to intrusion software. While the implementation of these controls is at the discretion of the participating state, it demonstrates the beginning of cybersecurity measures being considered by export control regimes.

The United States has imposed stringent export controls on various technologies, citing national security and cybersecurity motivations (Diaz, 2022). US agencies have collectively administered and enforced export-control laws to protect national security interests and promote foreign policy objectives. The US Department of Commerce's Bureau of Industry and Security (BIS) is responsible for governing the export and re-export of commodities, software, and technology that fall under the jurisdiction of the Export Administration Regulations and has recently established export controls that have a strong cybersecurity consideration. On October 21, 2021, the BIS published its Interim Final Rule on export controls for cybersecurity intrusion and surveillance tools, requiring licenses for the export, re-export, and in-country transfer of some cybersecurity items to certain countries, including China and Russia, depending on the items for export, the recipients, and the anticipated uses of the export (Boria & Burgess, 2021).

Additionally, it prohibits the export, re-export, and in-country transfer of cybersecurity items to Cuba, Iran, North Korea, and Syria if there is knowledge or reasons to suspect that the item will affect the confidentiality, integrity, or availability of the information or the information systems (Boria & Burgess, 2021). The rule came into force in January 2022, stating that the new export controls are due to national security and anti-terrorism reasons, and that the specific items are subject to controls as they could be used for surveillance, espionage, or any other actions that "disrupt, deny or degrade the network or devices on it" (Diaz, 2022: para. 2). The cybersecurity items on the export-control list include: "systems, equipment, software, and other technology specifically designed or modified to develop, generate, command and control, or deliver 'intrusion software'", "Internet Protocol network communications surveillance systems or equipment that meet specified criteria, including the ability to capture and analyze application data", and "Other related items, software, and technology, as specific in new and review Export Control Classification" (Diaz, 2022: para. 3). The purpose of these controls is to reinforce the multi-agency effort by the US government in combatting ransomware, state-sponsored hacking, and other cybersecurity threats, making it more difficult for other actors to have these capabilities.

In addition to specific cybersecurity-related export controls, the United States, in October 2022, imposed export controls on advanced computing semiconductors, semiconductor manufacturing equipment, and supercomputing items (BIS, 2023). These controls were intended to restrict China's access to high-end semiconductor devices manufactured in the United States that have potential military applications, representing a transition in the US and allied export control strategy (Shivakumar et al., 2022). The purpose of the measures, to freeze or slow Chinese developmental capacity, was reinforced by an updated package of export controls in

October 2023, which sets tighter restrictions on AI semiconductors, strengthens restrictions to semiconductor manufacturing equipment, and adds Chinese firms to the Entity List (firms on the list are subject to license requirements to receive US exports). There are four main objectives for these export controls: to limit AI semiconductor access, to limit China's design capability for high-end semiconductors, to restrict advanced semiconductor manufacturing capability by blocking access to US-made semiconductor manufacturing equipment with no foreign alternative, and, finally, to limit China's ability to build manufacturing equipment with US-made semiconductors (Shivakumar et al., 2022). The motivation for updating these export-control regulations is characterized by the fear of Chinese access to advanced semiconductors, which can be used to build supercomputing technologies which can facilitate advanced AI capabilities, cited as a US national security concern due to their ability to make military decisions faster and more accurately, and carry out planning and logistics. There is a risk that this technology additionally could be used for cognitive electronic warfare, radar, signals intelligence, and jamming, all of which pose security risks. US firms such as Nvidia Corp, a semiconductor manufacturer along with other US firms have been restricted from selling their most advanced semiconductors to China, with US Commerce Secretary Gina Raimondo stating: "What we cannot allow them is to ship the most sophisticated, highest-processing power AI chips, which would enable China to train their frontier models" (Shepardson, 2023, para. 3). This underscores the US concern about the ability of other actors to conduct cyber-attacks with advanced technology and therefore their reasoning for imposing export controls.

In addition to the United States, the European Union has begun to explore export controls to mitigate rising geopolitical tensions and the deeper economic integration that may pose a risk to EU economic security (European Commission, 2023). The European Economic Security

Strategy includes four categories that require further assessment of risks: supply chain resilience, including energy security; physical and cybersecurity of critical infrastructure; technology security and leakage; and the weaponization of economic dependencies and economic coercion. As a result, in October of 2023, the European Commission recommended conducting a risk assessment on four technology areas that are the most sensitive and likely to pose risks related to technology security and technology leakage. This includes advanced semiconductors, due to their enabling and transformative nature and their use for civil and military purposes; artificial intelligence, including AI software, high-performance computing, cloud and edge computing, and data analytics; quantum technologies, with the large-scale potential to completely transform civil and military sectors; and biotechnologies which can be mobilized in a harmful way if misused. These four areas are to be assessed through a broad lens and are not country specific, but the purpose will be to determine if the EU should control or ban the export of these specific items to certain countries, to defend its economic security, and inherently its cybersecurity (Bounds, 2023). While this is currently an assessment of the risk the export of these items poses, the trend has increasingly been toward imposing controls on technologies such as these.

Import- and Investment-Related Policies

While there are a number of policies that regulate the export of goods due to concern around their usage by foreign adversaries, governments can impose import-related policies that restrict the access of foreign companies and governments to domestic industries. These policies can include a complete ban on certain imports, can require authorization or registration for importing, or require that products undergo specific testing and inspections before they are allowed to enter the domestic markets (Meltzer, 2020). This can also include investment restrictions that prohibit foreign companies from participating in the domestic market of certain industries that are deemed sensitive for security reasons (Veyet et al., 2023).

There has been a recent proliferation in the banning of Chinese technology companies, specifically Huawei and ZTE, from supplying technology and providing telecommunications services. Concerns revolve around cyberespionage risks, elevated by the use of Huawei's 5G infrastructure, and intellectual property theft in which Huawei has been found guilty of stealing intellectual property from US telecommunications company, T-Mobile (Berman et al., 2023). The risk is amplified due to the adoption of 5G technology, which allows more devices to connect to networks at higher speeds including those that were previously disconnected from the network. The concern surrounding 5G is the integration of devices, making it difficult to monitor the security checkpoints for each device as traffic is routed through many different points (Kaspersky, n.d.). The speed and volume of data transmitted poses challenges in identifying and stopping threats in a timely manner. Finally, the increased connection of Internet of Things (IoT) devices poses security risks, as often these devices are not manufactured with security as the main priority and this lack of encryption can increase the number of vulnerabilities that can be exploited. As a result, the information can be much more open, and the infrastructure provider must be trusted to not violate the security and expose any vulnerabilities found. The US government has expressed concerns that Huawei's 5G infrastructure could include backdoors which allow the Chinese government to "collect and centralize massive quantities of data and give Beijing the necessary access to attack communications networks and public utilities" (Berman et al., 2023: para. 6). Due to this lack of trust, the United States has banned or restricted Huawei and ZTE products from their 5G networks.

The Government of Canada has also cited concerns about telecommunications suppliers such as Huawei and ZTE and their potential to be compelled to comply with extrajudicial directions from foreign governments, which could conflict Canadian laws and be detrimental to

Canadian interests (ISED, 2022). This has resulted in the Canadian government prohibiting the procurement of 4G or 5G Huawei and ZTE products and services, the removal of existing Huawei and ZTE products and services in 5G networks by June 2024, and the removal of any Huawei and ZTE 4G services by December 2027. Other countries have similar bans, whether total bans or bans on government procurement, including Japan, Australia, Germany, Britain, Estonia, Denmark, France, Italy, Latvia, Lithuania, and Portugal (Veyet et al., 2023).

The Canadian Government has taken further steps to regulate the telecommunications industry due to cybersecurity concerns (Chong et al., 2022). While still going through the Parliamentary process, Bill C-26 *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts* would provide the government increased options to take actions, securing the telecommunications industry and systems from a number of threats. These options including prohibiting a telecommunications service provider (TSP) from using a specified product or service, directing a TSP to remove a product or service, prohibiting a TSP from upgrading a product or service, reviewing the use of a TSP's networks, facilities or procurement plans, and so on. These greater powers are intended to be used by the Government of Canada to block the use of telecommunications products that could pose a risk to the Canadian telecommunications system, such as those of Huawei and ZTE.

In addition, the Chinese government has taken steps to mitigate the cybersecurity risks of imports or investments. In February of 2022, new measures came into effect under the Measures for Cybersecurity Review, requiring that Critical Information Infrastructure Operators in China apply for a cybersecurity review if they are procuring network products or services for their operations which may impact national security (Guo & Li, 2022). For those that operate network platforms, their data processing activities require a cybersecurity review if the activities may

impact national security. Additionally, if a network platform operator that stores personal information of over one million users plans to be listed in other countries, it must apply for a cybersecurity review.

Data Flow Restrictions

For cybersecurity reasons, countries have imposed data flow restrictions, regulating cross-border flows of data to certain jurisdictions or imposing data-localization requirements (Ji, 2018). The restrictions on data flows have risen in concurrence with "Big Data" and the use of cloud computing. Due to the large-scale interconnectivity of the digital world, a massive amount of data is generated from online activities, such as emailing, using search engines, and social media networking, as well as data from IoT devices (Mushtaq et al., 2022). The mass volume of data cannot be handled by modern database systems and requires the use of cloud-computing services for processing and storage, in which services are provided over the Internet, and the physical computing resource becomes invisible, with cloud services distributed across multiple locations. Multiple different cloud services can be provided, including Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Data as a Service (Daas), with each providing a different functionality but essentially allowing clients to use the services provided by the host, conducting their operations through the cloud platform. Cloud services can be private, public, community, or hybrid clouds. Private cloud services are deployed by a single organization for use within that organization only. Community cloud services are shared by organizations with similar strategies and morals. Public cloud services are the most common type in which the cloud owner has complete ownership of the cloud. Examples of public clouds includes Amazon Web Services, which holds 31 percent of the world cloud-computing market share, and Microsoft Azure, which holds 24 percent (Richter, 2024).

The use of cloud computing to store massive amounts of data results in several security concerns, including infrastructure security, data privacy, data management, and data integrity and security (Mushtaq et al., 2022). These issues are mainly due to vulnerabilities, misconfigurations, or flaws within the system. Government concerns revolve around data sovereignty, which is the idea that data are subject to the laws and regulations of the countries within which it is collected and located (Taylor, 2020). The concern is that large clouds have their operations distributed over multiple different countries and therefore there is a sense of lost ownership over the physical storage facilities and personal information of citizens. The legal status of the data is in question, with the concern that other countries may invoke their jurisdiction over data that is stored in a data processing centre in their country but did not originate there. Additionally, the wide distribution of data may result in the data being compromised, and sensitive information potentially accessed by malicious actors through vulnerabilities in the cloud computing network as it travels from point to point, within and across geographic boundaries. As a result, a number of countries have imposed data-flow restrictions, with the most restrictive being data-localization requirements.

Data localization can be defined as "any measure that specifically encumber(s) the transfer of data across national borders" (Mishra, 2020: p.341). It has two meanings for government policies: 1) a policy where governments require Internet cloud providers to store data about Internet users in their country on servers geographically located within the country and 2) a policy where government require Internet service providers to route data packets sent between Internet users in their jurisdiction through networks that are located only within their jurisdiction (Selby, 2017). The premise of data localization is that government control over data processing, access, and transfer increases substantially if data is located within a nation's borders

(Mishra, 2020). It is seen as an opportunity to protect national data; not just that of citizens but data related to national security, governmental activities, financial activities, business, and civil society. For example, under China's Cyber Security Law, companies that handle critical information infrastructure (CII) are required to keep all data collected and processed within Chinese borders, due to the data being seen as sensitive to China's national security and economy (InCountry, 2023). Data that must be transferred by CII operators outside of borders must undergo a security assessment before the transfer is approved by the Chinese government. Under the Chinese Personal Informational Protection Law, companies that store sensitive personal information that is collected and generated in China above a certain threshold must store data inside China and must also undergo a security assessment if wishing to transfer outside of China (Kumayama et al., 2023).

Restrictions on data can manifest in ways other than data localization. They can include regulations around data protection, geolocation data privacy, online censorship, forced transfer of intellectual property, and traffic routing (Taylor, 2020). The European Union's General Data Protection Regulation (GDPR), effective May 2018, imposes restrictions on the transfer of personal data outside of the EU to non-EU countries or international organizations (European Data Protection Board, n.d.). Data can be transferred to 15 countries where adequacy decisions have been made by the European Commission as containing the proper level of data protection or to organizations that contain the appropriate safeguards to protect personal data (e.g. standard data protection clauses, binding corporate rules, codes of conduct, certification mechanisms, and ad hoc contractual clauses). The purpose of this legislation is to ensure that the level of protection of individuals' data that is upheld by the GDPR is the same, regardless of where the data is stored.

In the United States, on February 28, 2024, President Biden issued an Executive Order that authorizes the Attorney General to prevent the large-scale transfer of data to what are deemed countries of concern, with the reasoning that these countries can rely on advanced technologies to analyze and manipulate data to engage in espionage, influence kinetic or cyber operations, or to gain a strategic advantage over the United States (White House, 2024). The Order focuses on the most sensitive personal information, such as genomic data, biometric data, geolocation data, financial information, and other types of Personally Identifiable Information. It does not authorize generalized data-localization requirements, however; it only prevents transfers of data to specific countries of concern.

Traffic-routing measures can be demonstrated by Russia's Sovereign Internet Law, which went into force in 2019 (Human Rights Watch, 2019). The law builds on previous data-localization laws, which require that companies that process the personal data of Russian citizens store them in Russia and hand over the information upon request by security services, with the justification that it is required to protect state security. The Sovereign Internet Law requires that Russian Internet Service Providers install equipment to route Russian internet traffic through servers in Russia, for the purpose of ensuring the stability of the internet in the event it was cut off by the United States or another Western country (Taylor, 2020). Russia's Deputy Prime Minister, Dmitry Chernenko, stated that these measures are taken to protect Russia from cyberattacks, not just from states but hacking groups that they claim have been attacking and breaching Russian networks since the invasion of Ukraine (Flashpoint, 2022).

In addition, certain measures have been implemented or proposed to block foreign involvement in cloud-service industries and access to cloud platforms. In January of 2024, the US Department of Commerce proposed the imposition of "Know Your Customer" requirements

onto US cloud infrastructure providers and their foreign resellers (BIS, 2024). The purpose of this is to address the risk that foreign malicious actors pose if they access US cloud services and use them for malicious cyber-enabled activity to harm US critical infrastructure or national security. The proposal authorizes the US government to impose certain measures that restrict access to US cloud infrastructure, including the data centres that store sensitive information. The main concern cited is about access to AI technology, with US Commerce Secretary Gina Raimondo stating that "We use export controls on chips, those chips are in American cloud data centres so we also have to think about closing down that avenue for potential malicious activity" (Shepardson, 2024; para. 2).

Similarly, in China, foreign companies are restricted from having sole ownership of cloud-computing services and are required to play a subordinate role if wanting to enter the market by partnering with a Chinese-based firm (Yang, 2020). This is because cloud services are described as value-added telecoms services (VATS). The operation of such services requires a license that only Internet Data Centre (IDC) businesses can hold; IDC businesses are not open to foreign investment.

These measures that restrict the import and export of goods, foreign investment, and data flows all cite cybersecurity and national security concerns as their main justification. While malicious actors and exploitation of cyber vulnerabilities pose significant risks, these measures have a broader impact on international trade and the global economy. They can disrupt the global trading order and can cause situations in which allegations of protectionism are thrown. The impact of these measures, both positive and negative, is discussed in the next chapter.

Impact of Cybersecurity Measures

While the widespread implementation of cybersecurity measures is a relatively recent phenomenon to mitigate the rapidly growing risk, the potential impacts of these measures on enterprises, consumers, and international trade can already start to be identified. As will be discussed in this section, the global market for cybersecurity solutions is growing, having a positive impact on digital services trade. However, the negative effects need to be identified, highlighting how the objectives the measures seek to achieve may in fact result in weaker cybersecurity, increased costs, and serve as barriers to trade.

Positive Effects: Market-Creating

The emphasis on cybersecurity and the growing risk of a cyberattack has had governments and businesses seeking cybersecurity solutions. This presents a significant opportunity for businesses to provide solutions, not just in their home market, but globally, representing a part of digital services trade. Current research shows that at the rate and growth of cyberattacks, damages from cyberattacks will cost approximately US$10.5 trillion annually by 2025, amounting to a 300 percent increase from 2015 (Aiyer et al., 2022). The costs associated with cyberattacks include damage and destruction of data, theft of money and intellectual property, theft of personal and financial data, fraud, and embezzlement (Morgan, 2020). These costs also include the after-effects, including lost productivity, disruption to the normal course of business, forensic investigation, the restoration and removal of hacked data and systems, and reputational damage. The rapid technological advancements of malicious actors to carry out cyberattacks also means that currently available commercial solutions are not fully equipped to meet customer security demands, specifically in terms of automation, pricing services, and other capabilities (Aiyer et al., 2022).

Enterprises are required to spend more and more on increasing their cybersecurity, which means rapid market growth for cybersecurity solutions, such as providing secure cloud services, expanding the provision of managed security services for SMEs, and improving automation and AI systems by integrating security products into them (Aiyer et al., 2022). Consulting firm Gartner reports that global spending on security and risk management is expected to increase 14.3 percent in 2024, with IT spending increasing by only 8 percent (Irei, 2024). McKinsey & Company has approximated that the global cybersecurity market opportunity amounts to between US$1.5 trillion and $2 trillion. The Security-as-a-Service (SaaS) industry is growing exponentially, due to the continuing expansion of cyber threats, growing regulatory pressures on businesses, and the ongoing digitization of the global economy which increase costs and risks when managing on-premises security programs (Irei, 2024).

Negative Effects: Reduced Cybersecurity

However, the effects are not only market-creating. Certain measures imposed, such as restrictions on data flow, may actually result in weaker cybersecurity. Data localization policies may result in data that is less secure, as there is a reduced opportunity for cloud service providers to distribute information across multiple servers in different locations (Taylor, 2020). This prevents cloud providers from “sharding”: a practice that involves dividing data into pieces of independently useless data and dispersing it across storage locations, ultimately becoming useless unless combined (Bauer, 2023). The localized information provides an easier opportunity for malicious actors to access full sets of data.

Additionally, data-localization policies result in weaker security infrastructure, due to the lack of an integrated management approach to detect cybersecurity risks (Bauer, 2023). Cloud-service providers share security data between operations centres and use this for easier threat detection. The prohibition on data sharing can result in loopholes being exploited by malicious

actors. As many cloud-service providers are global companies, they benefit from a higher degree of knowledge from data sharing and experience from ICT professionals, and are consistently updating their security practices (Taylor, 2020). Removing this infrastructure due to data being stored outside of certain jurisdictions could result in a security deficit where the infrastructure to provide solutions to the public and private sector does not exist or is not at the capacity required, thereby reducing cybersecurity. As a result, government policies to increase cybersecurity and privacy may have the opposite effect.

Negative Effects: Impact on Businesses

The cybersecurity measures previously outlined have an impact on businesses and therefore consumers: inefficiencies in supply chains, reduced competition and innovation, and increased costs.

The Internet, which facilitates trade in both digital and physical goods and services, relies on autonomous data routing, which moves data through the most efficient route from its start to end destinations (Mishra, 2020). Any manipulation of data flows based on territory, such as data-localization or data-routing policies, interferes with the technical and logical Internet infrastructure, and hence its reliability as a service that transfers data. Large multinational corporations (MNCs) and small and medium-sized enterprises (SMEs) rely on cross-border transfers of data when conducting business globally, starting with the purchase of a good or service online to the delivery and service follow-ups (Casalini & López González, 2019). MNCs and SMEs are reliant on data transfers regarding business activity at the design, production, delivery, and use stage of their operations. Many times, this information is geographically dispersed, relying on cross-border data transfers. Day-to-day operations such as HR tasks for MNCs with affiliates geographically dispersed or efficient supply chain management are disrupted by government prescriptions on cross-border data flows. Data flows allow SMEs to

scale-up faster, offering an advantage in the global marketplace through the access of IT services and better and faster access to information, allowing them to overcome barriers that may have previously hindered their ability to engage in international trade. Firms may lose the efficiency gains of cloud computing by being required to build local servers or use local services in each country implementing data-flow restrictions, ultimately losing what can be described as network economies of scale (Mishra, 2020).

In addition, this can result in a lack of competition in two ways. First, domestic companies that use cloud or other digital services lose access to foreign service providers that could offer a better service at a lower cost for the business and the consumer (Mishra, 2020). Second, it can reduce the incentive for domestic providers to innovate or price more competitively to win business (Bauer, 2023). The reduced competition and the more stringent requirements mean that the end result for businesses, and ultimately consumers, are higher costs. An OECD-WTO Business Survey found that data-localization measures allowing cross-border flows would increase costs to businesses by approximately 16 percent while data-localization measures with flow restrictions would increase costs by 55 percent (Del Giovane et al., 2023). For example, data localization in the e-payments sector has led to an overall increase in operating costs, domestically and across borders, and additional capital and personnel are required in order to keep local copies of data and comply with regulations. Similar to enterprises relying on cross-border data transfer, cloud-service providers may be unable to take advantage of economies of scale by operating globally and may have to reduce their services provided or increase costs. These costs may be passed down to the consumer, potentially resulting in less secure and reduced services for a higher price (Del Giovane et al., 2023). These impacts are not limited to business operations and costs but extend further to international trade.

Negative Effects: Impact on Trade

The increased regulation and divergence in policies, specifically in the cross-border flow of data, can result in firms leaving markets or being unable to participate in trade across borders (Bauer, 2023). A study showing the potential effects of the proposed Cybersecurity Certification Regime for Cloud Services (EUCS) in the EU found that requiring EU businesses to assess the laws and practices of non-EU countries that they share data with would cause 40 percent of businesses to stop their cross-border flows of data (Bauer, 2023). The EUCS also sets out requirements that would impact other regulated sectors, which many businesses stated would lead them to consider leaving the EU internal market to avoid dealing with the separate laws and guidelines for different entities and types of data. An example of this impact can be seen through the impact of data-flow restrictions on the air travel industry (Del Giovane et al., 2023). The process of purchasing an airline ticket through to landing in the destination requires a large amount of personal data to be transferred across borders in real time, with all data being transferred and stored in a single geographic location. Data-localization requirements may have significant impacts on an airline's ability to operate in countries that require data localization, with increased organizational complexity and costs, potentially leading to airlines stopping their operations, disrupting trade and travel flows. The lack of harmonized standards on data-flow restrictions can lead to businesses exiting certain markets, reducing the flow of capital, goods, and services across borders.

In addition, some of these policies can be considered discriminatory by design, shutting out foreign companies from markets (Bauer, 2023). The EUCS establishes an EU-wide certification regime for cloud services, with three levels of "basic", "substantial" and "high" security assurances that can be provided. However, the EUCS prevents non-European providers from providing high-assurance services in the EU. In effect, this means that only companies

globally headquartered in the EU are eligible for certification. EU vendors headquartered outside of the EU are excluded from the EU market, data cannot be stored and processed outside of the EU, and only employees located in the EU can provide customer support capabilities. While the certification is currently voluntary, there is an expectation that they may become mandatory under the NIS2 Directive, the EU-wide legislation on cybersecurity. The effects of these foreign ownership restrictions on receiving a high certification excludes many cloud-service providers from the market, including those that provide the vast number of services globally. These, along with other certification requirements, can impose burdens on foreign companies from operating in specific markets, ultimately restricting trade flows to a level that may not be proportional to the risk (Bauer, 2023).

The restrictions on exports and data crossing borders due to insufficient cybersecurity standards may result in a reduction in goods and services being provided, ultimately having a negative impact on international trade, especially as digitally enabled trade in goods and services is constantly increasing.

Striking the Balance Through Global Cooperation

As digital trade in goods and services is increasing, global cooperation will be required to mitigate the tension between the increase in cybersecurity measures and maintaining trade flows. Relying on the security exception outlined in Article XXI of the GATT will not be enough to ensure that cybersecurity measures are not imposed for protectionist reasons. Not only does the security exception fail to adequately account for cybersecurity risks, but the United States blocking appointments to the WTO's Appellate Body, responsible for reviewing appeals of dispute settlement body panel reports, has left a number of cases in limbo and unable to be reviewed while the Appellate Body has vacant positions (WTO, n.d.c). As a result, the current trade system is not equipped to deal with the effects of these measures implemented and rule on how cybersecurity fits into the security exception even if a country were to initiate a complaint.

The increased adoption of trade policies that reflect a national- and cybersecurity mindset not only has implications for enterprises in countries that have imposed the measures, but can lead to developing economies, including many low-income countries that benefit from the interconnectedness of digital trade, falling behind when trying to ensure their practices comply with various regulations (Ruta & Jakubik, 2023). The complex and differing legal and regulatory environments that businesses must comply with, coupled with existing gaps in connectivity and reduced information and communication technology infrastructure and legal skills increase this divide and the barriers to trade. Increased international cooperation is necessary, which must include the participation of developing economies, to continue developing proactive trade policies that address the issues that arise from digital trade and cybersecurity (WTO, 2023).

A number of global initiatives could help proactively resolve some of these issues (Meltzer, 2020). First, having a shared understanding of what constitutes a cybersecurity risk and cybersecurity measures, and adopting a risk-based approach where measures are implemented in

order to adequately respond to the risk can help to mitigate the overly prescriptive measures that countries have been using. With a shared understanding comes less uncertainty when measures are imposed and a risk-based approach with different levels of measures implemented depending on the risk would provide procedural discipline to ensure overly restrictive measures are not imposed. Second, developing global cybersecurity standards would help to regulate the current patchwork environment that reduces efficiencies and poses challenges to businesses attempting to operate in multiple jurisdictions. While there is difficulty gaining consensus at the multilateral level, trade agreements such as those that already exist and include digital trade and cybersecurity provisions, can help to generate agreement around which measures are reasonable to be imposed that are as least trade restrictive as possible. Trade agreements can be a useful tool to advance cybersecurity standards for enterprises, real-time information sharing that can help to bring awareness to threats and vulnerabilities, and prevent the restriction of data flows across borders in order to advance both digital trade and cybersecurity objectives (Meltzer, 2020). However, attention must be paid to the way these agreements are structured, avoiding the tendency of deferring authority to more developed economies that can use the size of their economies and share of global trade flows to exert their influence.

Ultimately, having these issues outlined in trade agreements could help to identify when trade policies are used for protectionist purposes, rather than their ultimate objective to advance cybersecurity. As there is an already increasing trend to including digital trade provisions into trade agreements, the inclusion of cybersecurity discussions, an issue that each country must address, can help to advance global cooperation and harmonization of policies in order to continue promoting international trade.

Conclusion

The signing of the GATT and the eventual creation of the World Trade Organization intended to liberalize trade, with the increased interdependence of economies promoting economic development and global cooperation. While global trade flows are continually increasing, with a significant portion made up through digital trade growth, the shift toward governments adopting trade-restrictive policies increasingly justified by national security concerns is alarming. This trend has the potential to increase global fragmentation and may reduce the benefits for enterprises and consumers that follow from liberalized international trade.

This paper has attempted to map this issue, first outlining the rise of cyber risks and the importance of protecting critical systems and important business, government, and consumer data from cyber threat actors who can use this information for malicious purposes, posing a threat to national security. Next, by identifying the measures that have been imposed, from export controls, import- and investment-related policies, and data flow restrictions, it is clear that government policies that restrict trade flows to increase cybersecurity are on the rise. While the full impact of these effects cannot yet be known, thus far, the patchwork regulatory environment increases costs for enterprises, introduces barriers to trade, and ultimately can result in weaker cybersecurity. As a result, it is unclear whether the benefits of these regulations outweigh the costs when considering their main objective to protect security. This calls into question whether governments are taking advantage of the lack of legal clarity around trade-restrictive measures justified by cybersecurity in order to engage in protectionism, violating WTO commitments.

Cybersecurity is an ever-growing topic of concern as the risk is continually increasing with the digitization of almost every aspect of daily life. However, the solution that currently exists, in which unilateral policies are imposed by governments, is likely the incorrect approach to take when attempting to identify and stop threats that exist across global networks. Global

cooperation is required to mitigate this risk that is amplified through digital trade, whether this be through multilateral organizations such as the WTO or through trade agreements that can help to build global consensus. Whatever the solution, it cannot be developed and implemented in isolation.

References

Aaronson, S.A. (2019). What Are We Talking about When We Talk about Digital Protectionism? *World Trade Review, 18*(4), 541-577.

Agreement Between the United States of America, the United Mexican States, and Canada. U.S. – Can. – Mex. Nov. 30, 2018. https://can-mex-usa-sec.org/secretariat/assets/pdfs/usmca-aceum-tmec/agreement-eng.pdf.

Ahmed, U. (2019). The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade. *World Trade Review, 18*(1), 99-120.

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers#/.

Akremi, A., & Rouached, M. (2021). A comprehensive and holistic knowledge model for cloud privacy protection. *The Journal of Supercomputing*, 77, 7956-7988.

Bauer, M. (2023, November 1). Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements, European Centre for International Political Economy, Policy Brief. https://ecipe.org/wp-content/uploads/2023/02/ECI_23_PolicyBrief_01-2023_LY07.pdf.

Berman, N., Maizland, L., & Chatzky, A. (2023, February 8). *Is China's Huawei a Threat to U.S. National Security?* Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security#:~:text=What%20is%20Huawei%3F&text=It%20is%20the%20world%27s%20largest,its%20products%20domestically%20and%20internationally.

Borgia, M.T. & Burgess, M. (2021, November 16). *Commerce Publishes Export Controls for Cybersecurity Intrusion and Surveillance Tools*. Davis Wright Tremaine LLP. https://www.dwt.com/blogs/privacy--security-law-blog/2021/11/commerce-department-cybersecurity-export-controls.

Bounds, A. (2023, October 3). *EU to assess export controls on sensitive tech to China*. Financial Times. https://www.ft.com/content/2b7a97ab-f563-434e-8d01-70ff9fa9efa6.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA and London, England: Harvard University Press. https://doi-org.proxy.bib.uottawa.ca/10.4159/9780674246010.

Bureau of Industry and Security (BIS). (2023, October 17). *Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern*. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-acs-and-sme-rules-final-js/file.

Bureau of Industry and Security (BIS). (2024, January 29). *Commerce Proposes Rule to Advance U.S. National Security Interests and Implement Biden-Harris Administration's AI Executive Order and National Security Strategy*. https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3443-2024-01-29-bis-press-release-infrastructure-as-as-service-know-your-customer-nprm-final/file.

Canadian Centre for Cybersecurity (CCCS). (2021). *Cyber Threat Bulletin: The Cyber Threat to Operational Technology*. https://www.cyber.gc.ca/sites/default/files/cyber/2021-12/Cyber-Threat-to-Operational-Technology-white_e.pdf.

Canadian Centre for Cybersecurity (CCCS). (2022a). *An Introduction to the Cyber Threat Environment*. https://www.cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf.

Canadian Centre for Cybersecurity (CCCS). (2022b). *National Cyber Threat Assessment 2023-2024*. https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf.

Casalini, F. and J. López González (2019, January 23), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris. http://dx.doi.org/10.1787/b2023a47-en.

Centre for Strategic and International Studies. (n.d.). *Significant Cyber Incidents*. Accessed January 18, 2024. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Chertoff, M. (2023, April 13). *Cyber Risk is Growing. Here's How Companies Can Keep Up.* Harvard Business Review. https://hbr.org/2023/04/cyber-risk-is-growing-heres-how-companies-can-keep-up.

Chong, J., Heminthavong, K., & Porteous, H. (2022, October 6). *Legislative Summary of Bill C-26: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.* Library of Parliament. https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/44-1/44-1-C26-E.pdf.

Claussen, K. (2020). Economic cybersecurity law: A short primer. In *Routledge Handbook of International Cybersecurity* (1st ed., pp. 341–353). Routledge. https://doi.org/10.4324/9781351038904-34.

Conger, F. & Frenkel, S. (2021, August 26). *Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China.* New York Times. https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html

Customs and International Trade Law. (n.d.). *Export Controls & Cybersecurity.* Accessed January 13, 2023. https://customsandinternationaltradelaw.com/2022/02/15/export-controls-cybersecurity/#:~:text=The%20Interim%20Rule%20creates%20a,and%20transfers%20of%20cybersecurity%20items.

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.) *Advanced Persistent Threats and Nation-State Actors*. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors.

Deep Instinct. (2023). *Generative AI and Cybersecurity: Bright Future or Business Battleground?* https://www.deepinstinct.com/pdf/voice-of-secops-4th-edition?hsCtaTracking=982e81ff-d1a0-47a4-9adf-6e279398d361|1d16a471-1022-4dff-8d07-dd79dac66a52.

Del Giovane, C., Ferencz, J. & López-González, J. (2023, November). The Nature, Evolution and Potential Implications of Data Localisation Measures. OECD Trade Policy Paper (No. 278). https://www.oecd-ilibrary.org/docserver/179f718a-en.pdf?expires=1711039775&id=id&accname=guest&checksum=11B147D0953CB0FC7952282777D03266.

Diaz, J. (2022, February 15). *Export Controls and Cybersecurity.* Customs & International Trade Law. https://customsandinternationaltradelaw.com/2022/02/15/export-controls-

cybersecurity/#:~:text=The%20Interim%20Rule%20creates%20a,and%20transfers%20of%20cybersecurity%20items.

Dutta, Nitul, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, and Emil Pricop. *Cyber Security: Issues and Current Trends*. Singapore: Springer, 2022. https://doi.org/10.1007/978-981-16-6597-4.

Etzioni, A. (2014). The Private Sector: A Reluctant Partner in Cybersecurity. *Georgetown Journal of International Law, 15*(3), 69-78.

European Commission. (2023, October 10). *Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States*. https://defence-industry-space.ec.europa.eu/document/download/31c246f2-f0ab-4cdf-a338-b00dc16abd36_en?filename=C_2023_6689_1_EN_ACT_part1_v8.pdf.

European Data Protection Board. (n.d.). *International data transfers*. Accessed March 3, 2024. https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en.

Farrell, H. & Newman, A.L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security, 44*(1), 42-79.

Fazzini, K. (2019, Feburary 14). *The Great Equifax Mystery: 17 Months Later, the Stolen Data Has Never Been Found, and Experts Are Starting to Suspect a Spy Scheme*. CNBC. https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html.

Flashpoint. (2022, March 11). *Understanding Russia's "Sovereign Internet": What Happens If Russia Isolates Itself from the Global Internet?* https://flashpoint.io/blog/russian-runet-sovereign-internet/.

Google Cloud. (n.d.). *What is Big Data?* Accessed January 18, 2024. https://cloud.google.com/learn/what-is-big-data.

Government of Canada. (2023). *Backgrounder: Amendment to A Guide to Canada's Export Control List.* Accessed February 9, 2024. https://www.international.gc.ca/trade-commerce/controls-controles/ecl-lec/backgrounder-document-information-2023.aspx?lang=eng.

Guo, B., & Li. B. (2022, February 8). *China Issued New Measures for Cybersecurity Review in 2022*. White & Case. https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022.

Henckles, C. (2020). Permission to Act: The Legal Character of General and Security Exceptions in International Trade and Investment Law. *The International and Comparative Law Quarterly, 69*(3), 557-584.

Hoffman, W. & Nyikos, S. (2018, December). *Governing Private Sector Self-Help in Cyberspace: Analogies From the Physical World.* (Carnegie Endowment for International Peace: Working Paper).

Huang, K., Madnick, S., Choucri, N., and Zhang, F. (2021). A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade. *Global Policy, 15*(5), 625-638.

Huang, K., Madnick, S., Zhang, F., & Siegel, M. (2022). Varieties of public-private co-governance on cybersecurity within the digital trade: implications from Huawei's 5G. *Journal of Chinese Governance, 7*(1), 81-110.

Human Rights Watch. (2020, June 18). *Russia: Growing Internet Isolation, Control, Censorship*. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

InCountry. (2023, October 9). *Complete Guide on Data Residency and Cross-Border Transfers in China.* https://incountry.com/blog/complete-guide-on-data-residency-and-cross-border-transfers-in-china/.

Innovation, Science and Economic Development (ISED) Canada. (2022, May 19). *Policy Statement – Securing Canada's Telecommunications System*. Government of Canada. https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html.

Irei, A. (2024, March 6). *Cybersecurity market researchers forecast significant growth*. TechTarget. https://www.techtarget.com/searchsecurity/feature/Cybersecurity-market-researchers-forecast-significant-growth.

Ji, C. (2018). Cybersecurity and Data Protection. *The International Lawyer, 51*(3), 527-552.

Kaspersky. (n.d.). *Is 5G Technology Dangerous? – Pros and Cons of 5G Network*. Accessed February 29, 2024. https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons.

Keitner, C.I. & Clark, H.L. (2019). Cybersecurity Provisions and Trade Agreements. *Harvard Business Review, 10*, 1-8.

Korzak, E. (2020). Export Controls. In *Routledge Handbook of International Cybersecurity* (1st ed., pp. 341–353). Routledge. https://doi.org/10.4324/9781351038904-34.

Kumayama, K.D., Kwok, S., Ridgway, W.E., Simon, D.A., & Zhang, S. (2023, November 7). *China Intends to Ease Control Over Cross-Border Data Transfers*. Skadden. https://www.skadden.com/insights/publications/2023/11/china-intends-to-ease-controls.

Leblond, P. (2022). A Digital Trade Strategy for Canada. *Prepared for the CN-Paul M. Tellier Chair on Business and Public Policy*. University of Ottawa. https://www.uottawa.ca/faculty-social-sciences/sites/g/files/bhrskd371/files/2022-12/Digital%20Trade%20Strategy%20for%20Canada.pdf.

Lippoldt, D. (2023, January). *Mitigating Global Fragmentation in Digital Trade Governance: A Case Study*. (Centre for International Governance Innovation Papers No. 270).

Lord, N. (2020, August 7). *The Cost of a Malware Infection? For Maersk, $300 Million*. Digital Guardian. https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-million.

Mantilla Blanco, S., & Pehl, Alexander. (2020). *National Security Exceptions in International Trade and Investment Agreements: Justiciability and Standards of Review*. Springer International Publishing. https://doi.org/10.1007/978-3-030-38125-7.

Meltzer, J.P. (2020, May). *Cybersecurity, digital trade, and data flows: Re-thinking a role of international trade rules*. (Global Economy and Development: Brookings Institution Working Paper #132).

Microsoft. (2021, March 2). *HAFNIUM targeting Exchange Servers with 0-day exploits*. https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

Mikalauskas, E. (2023, November 15) *What's Your Identity Worth on the Dark Web?* Cybernews. https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

Ministry of Trade and Industry – Singapore. (n.d.). *What are Digital Economy Agreements (DEAs)?* Accessed February 9, 2024. https://www.mti.gov.sg/Trade/Digital-Economy-Agreements.

Mishra, N. (2020). Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? *World Trade Review, 19*, 341-364.

Mishra, N. (2020). Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? *World Trade Review, 19*, 341-364.

Morgan, S. (2020, November 13). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Mushtaq, M. S., Mushtaq, M. Y., Iqbal, M. W., & Hussain, S. A. (2022). Security, integrity, and privacy of cloud computing and big data. In *Security and Privacy Trends in Cloud Computing and Big Data* (1st ed., pp. 19–51). CRC Press. https://doi.org/10.1201/9781003107286-2.

Office of the Director of National Intelligence. (2023). *Annual Threat Assessment of the US Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

Oladimeji, S. & Kerner, S.M. (2023, November 3). *SolarWinds hack explained: Everything you need to know*. TechTarget. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Peng, S. (2015). Cybersecurity Threats and the WTO National Security Exceptions. *Journal of International Economic Law*, 18, 449-478.

Pinchis-Paulsen, M. (2022). Let's Agree to Disagree: A Strategy for Trade-Security. *Journal of International Economic Law, 25*, 527-547.

Priyadarshini, I., & Cotton, C. (2022). *Cybersecurity: Ethics, Legal, Risks, and Policies* (1st Edition.). Apple Academic Press. https://doi-org.proxy.bib.uottawa.ca/10.1201/9781003187127

Process Unity. (2022, August). *Which Cybersecurity Certification Does Your Business Need? https://www.processunity.com/cybersecurity-certification-does-your-business-need/.*

Public Safety Canada. (2022, April 20). *Parliamentary Committee Notes: Ransomware and Russian State-sponsored Advanced Persistent Threat Actors.* https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20220930/05-en.aspx.

Rainia, S. (2023, January 18). *Geopolitical Instability Raises Threat of 'Catastrophic Cyberattack in Next Two Years'.* World Economic Forum. https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/.

Richter, F. (2024, February 5). *Amazon Maintains Cloud Lead as Microsoft Edges Closer*. Statista. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

S&P Global. (n.d.). *Cyber attacks: What the hack.* Accessed January 18, 2024. https://www.spglobal.com/en/enterprise/geopolitical-risk/cyber-attacks/.

Selby, J. (2017). Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology, 25*(3), 213-232.

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, *20*(4), 359–374. https://doi.org/10.1080/19331681.2022.2112796.

Shepardson, D. (2023, December 12). *US in talks with Nvidia about AI chip sales to China – Raimondo.* Reuters. https://www.reuters.com/technology/us-talks-with-nvidia-about-ai-chip-sales-china-raimondo-2023-12-11/.

Shepardson, D. (2024, January 26). *Eyeing China, US proposes 'know your customer' cloud computing requirements*. Reuters. https://www.reuters.com/technology/us-propose-know-your-customer-requirements-cloud-computing-companies-2024-01-26/.

Shivakumar, S., Wessner, C., & Howell, T. (2022). *A seismic shift: The new U.S. semiconductor export controls and the implications for U.S. firms, allies, and the innovation ecosystem.* Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221114_Shivakumar__ExportControlImplications_v2.pdf?VersionId=1SyaKGTyhKCu0jkMw1ePtAkAPoSOw4f1.

Shivakumar, S., Wessner, C., & Howell, T. (2024, February 21). *Balancing the Ledger: Export Controls on U.S. Chip Technology to China*. Center for Strategic & International Studies. https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china.

Sloan, R. H. & Warner, R. (2019). *Why Don't We Defend Better?: Data Breaches, Risk Management, and Public Policy* (1st Edition) CRC Press/Taylor & Francis Group. https://www-taylorfrancis-com.proxy.bib.uottawa.ca/books/mono/10.1201/9781351127301/defend-better-robert-sloan-richard-warner.

Taylor, R.D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy, 44* (8), 1-15.

The General Agreement on Tariffs and Trade, 1994, https://www.wto.org/english/docs_e/legal_e/06-gatt.pdf/.

The White House. (2024, February 28). *Executive Order on Preventing Access to American's Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

Tran, H. (2021, November). Competing Data-Governance Models Threaten the Free Flow of Information and Hamper World Trade. *Atlantic Council Geoeconomics Centre: Issue Brief*, 1-11.

Tripathy, B., & Anuradha, J. (2017). *Internet of Things (IoT) : Technologies, Applications, Challenges and Solutions* (1st Edition.). Taylor and Francis. https://doi.org/10.1201/9781315269849.

VanGrasstek, C. (2013.) *The History and Future of the World Trade Organization*. The World Trade Organization. https://www.wto.org/english/res_e/publications_e/historyandfuturewto_e.htm.

Veyet, T., Pothitos, A., & Lenkiewicz, L. (2023, September 29). *European countries who put curbs on Huawei 5G equipment*. Reuters. https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/.

Vidigal, G. (2019). WTO Adjudication and the Security Exception: Something Old, Something New, Something Borrowed - Something Blue?' *Legal Issues of Economic Integration, 46*(3), 203-244.

Weber, R.H. (2018). Free flow of data and digital trade from an EU perspective. In S. Peng, H.W. Liu & C.F Lin (Eds.), *Governing Science and Technology under the International Economic Order: Regulatory Convergence and Divergence in the Age of Megaregionals* (pp. 47-63). Edward Elgar Publishing.

Whang, C. (2020). Trade and Emerging Technologies: A Comparative Analysis of the United States and the European Union Dual-Use Export Control Regulations. *Security and Human Rights, 31*, 11-34.

Wilson, D. C. (2021). *Cybersecurity* (1st ed.). MIT Press. https://doi.org/10.7551/mitpress/11656.001.0001

Wood, K. (2023, March 7). *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack.* The Georgetown Environmental Law Review. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/ - :~:text=A hacker group known as,diesel fuel, and jet fuel.

World Trade Organization. (n.d.a). *Principles of the trading system*. Accessed January 28, 2024. https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm#:~:text=without%20discrimination%20—%20a%20country%20should,giving%20them%20“national%20treatment”)%3B.

World Trade Organization. (n.d.b). *Regional trade agreements and the WTO*. Accessed January 18, 2024. https://www.wto.org/english/tratop_e/region_e/scope_rta_e.htm.

World Trade Organization. (n.d.c.). *Appellate Body*. Accessed April 2, 2024. https://www.wto.org/english/tratop_e/dispu_e/appellate_body_e.htm.

World Trade Organization. (2023). Digital Trade for Development. https://www.wto.org/english/res_e/booksp_e/dtd2023_e.pdf.

World Trade Organization Panel Report. (2019, April 29). *Russia – Measures Concerning Traffic in Transit*. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/512R.pdf&Open=True.

Yang, S. (2020, October 13). *Regulation of cloud computing in China.* AnJie Broad. https://www.chinalawvision.com/2020/10/intellectual-property/cybersecurity/regulation-of-cloud-computing-in-china/.

Zaki, A. (2023, August 30). *85% of Cybersecurity Leaders Say Recent Attacks Powered by AI: Weekly Stat.* CFO. https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/.

Zaun. (2023, September 1). *Zaun Data Breach – Update*. https://www.zaun.co.uk/zaun-data-breach-update/.

Zetter, K. (2016, March 3). *Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.* Wired. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.