Framework for Understanding Cybersecurity Impacts on International Trade

Keman Huang, Stuart Madnick, Simon Johnson

Working Paper CISL# 2019-23

December 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Framework for Understanding Cybersecurity Impacts on International Trade

Keman Huang, Stuart Madnick, Simon Johnson
MIT Sloan School of Management

Cybersecurity concern is becoming a key issue for trade policy

Issues of international trade policy have recently gained increased attention. Of course, restrictions on international trade regarding technology have long existed – on imports and exports, as well as on direct foreign investment in the United States. But cybersecurity has not been a key issue for trade policy – until now. This is because of the wide adoption of information and communications technologies (ICTs), like the Internet-of-Things (IoT), cloud computing, and big data analysis in the digital society. Almost every product is (or can be) Internet connected, including the critical infrastructures which military security, economic security and culture security heavily rely on. Hence cybersecurity has increasingly been invoked as a perspective of "national security," which has been considered an important factor that impacts international trade and investment policy (Friedman, 2013; Kshetri, 2016; Mata, 2015)[1].

Furthermore, more than 30 countries are developing offensive and defensive cyber attack capabilities (Clapper, Lettre, & Rogers, 2017; Ranger, 2017) although it is widely accepted that "*in cyberspace, the offense has the upper hand*"(Lynn, 2010)[2]. According to news reports, various governments, typically working with private sector companies in their respective countries, have incorporated various forms of spyware, malware, or similar programs in computer-based products that are then exported around the world[3]. This will introduce significant cyber threats for the countries that purchase and install such products, and it can then raise cyber conflicts (Maness & Valeriano, 2016) between nations over time.

From the defensive perspective, since it is unlikely to examine the millions of lines of software or firmware in these products[4], what should countries do to prevent cyber intrusions when these products can introduce additional attack vectors? Governments around the word have begun to develop strategies to protect themselves against cyber threats. More than 50 countries have published a cybersecurity strategy to define the security of a nation's online environment (Klimburg, 2012; OECD, 2012). There is no doubt that a national cybersecurity strategy is helpful to "protect the society as a whole" (OECD, 2012). However, different policies are implemented to fulfill these strategic goals. One typical example, that has been informally suggested, is that potentially dangerous products coming from questionable countries should be excluded from import. But this raises many policy issues, such as (1) what is a questionable country considering the globalized supply chains for almost every product, (2) what products are of most concern,

[1] Much research suggested that national security issues can significantly impact international trade and foreign direct investment policy. Please refer to the following literature for more details: (Friedman, 2013; Kshetri, 2016; Mata, 2015)

[2] Many military officers, policymakers, and scholars hold this perspective while only a few scholars disagree. Recently, some began to discuss the balance between cyber offense and defense, focusing on the costs and benefits of a cyber offensive operation. Please refer to (Slayton, 2017) for details.

[3] For example, German journalists uncovered a world-wide Jason Bourne-style U.S. spy-program. http://www.spiegel.de/netzwelt/netzpolitik/bnd-skandal-netbotz-baut-offenbar-hintertueren-in-seine-kameras-a-1114252.html. Another recent example: Israeli intelligence hacked into Kaspersky's network and then warned their U.S. counterparts of the Russian intrusion. Please see this for detail: https://www.reuters.com/article/us-usa-security-kaspersky/israeli-spies-found-russians-using-kaspersky-software-for-hacks-media-idUSKBN1CG05P.

[4] Many automatic vulnerability discovery tools are developed over years. However, it still requires much effort to identify false-positive alerts when source codes are considered very important intellectual property that the suppliers will not offer intentionally.

and (3) assuming such restrictions quickly become worldwide policies with retaliations, what might be the impact on international trade and the economy? Furthermore, from the digital supply chain perspective, data is considered a critical asset that supports digital service industries while some countries like Russia, Vietnam, and Indonesia even emphasize data sovereignty[5]. What's worse are the privacy concerns raised by the increasing data breach incidents (Verizon, 2017) over the years. One fresh and big memory for this is that in 2017, personal information of 143 million consumers were exposed in the Equifax Data Breach instance. Hence, we can see the issue of data localization policies which restrict the transfer of data across borders around the world (Burri, 2017; Mitchell & Hepburn, 2016; Selby, 2017) becoming a topical issue during the negotiation of trade agreements in the name of "data protection".

It is a consensus that cybersecurity concerns have presented significant national security challenges. Cybersecurity concerns have become a major source of allegations and growing commercial disputes as different cybersecurity policies are implemented, including various barriers to international trade and investing. These policies will shape not only cyberspace for the countries themselves, but also the broader globalized society (Friedman, 2013; James Lockett, 2015). However, thought we witnessed many international trade restrictions due to cybersecurity concern over these years, like Kaspersky's ban in U.S., LinkedIn's restriction in Russia, restriction of data flow to India from E.U., restriction of VPN in China etc., there exist no systematic framework to understand how cybersecurity concern evolve in the international trade context: how cybersecurity concern ends up into impacting the international trade, whether the implemented policies really solve those concerns, and what can be done to mitigate the negative impacts from them. Without a clear understanding, governmental agencies are implementing different policies and may result into cyber conflicts with each other while businesses are struggling for the evolving cybersecurity concerns and restrictions.

Methodology

The goal of this project is to develop a framework to understand how cybersecurity concerns influent the international trade and what businesses can do in such context. Note that in this paper, we are not going to argue for or against any specific cybersecurity regulation, policy, or operation[6]. Instead, we intend to offer a systematic framework to study these cybersecurity related actions and advocate for creating standards for international trade in cyberspace.

To understand the impact from cybersecurity concern on the international trade, the research team at Cybersecurity at MIT Sloan collected 33 different cases within international trade original from cybersecurity concerns until December 2017[7]. Digging into the detail, especially the timeline, related actors, actions and impacts for each case, a framework is further developed to systematically organize these cases to get an overview of how cybersecurity become a significant issue for international trade. During December 2017 to April 2018, we did an in-depth interview with more than 10 domain experts to understand how cybersecurity

[5] Russian Federal Law on Amendments to Certain Legislative Acts of the Russian Federation to Clarify the Procedure of Personal Data Processing in Information and Telecommunication Networks (Russia) Federal Law No. 242-FZ, signed 21 July 2014, entered into force on 1 September 2016, art 15.5. Decree on the Management, Provision and Use of Internet Services and Online Information (Vietnam), Decree No 72/2013/ND-CP, 15 July 2013, art 4.4, art 5. Undang-Undang Tentang Pelayanan Publik (Indonesia) Law No 25/2009, 18 July 2009. See also Anupam Chander and Uyen P Le, 'Breaking the Web: Data Localization vs the Global Internet' (UC Davis Legal Studies Research Paper No 378, 2014) 19-20.

[6] There are some discussions about whether the specific policies or regulations violate trade agreements. For example, there are some debates about whether China's banking IT security regulation violates the WTO TBT agreement. Please refer to (Sun, 2016) for more details. However, such discussions are out of scope of this paper.

[7] These 33 cases can be provided if required, including the detail timeline and the sources.

impact the international trade in different industrial sectors. On April 2018, a workshop discussion with more than 30 senior executives, managers and researchers focusing on cybersecurity from Fortune 500 companies, key cybersecurity solution providers and governments, who are members of the Cybersecurity at MIT Sloan, provides insightful thought about the framework.

The key takeaways from these discussions, together with the understanding of the cases and framework, direct us to a conceptual model to understand the relations among cybersecurity concern and international trades. Using this framework, we are able to identify three different contexts, including the regulation compliance context, supply chain management context and geopolitical context. More interesting, these three contexts are not independent but can be transformed among each other. Different reactions in different contexts will end up into different results. Therefore, when thinking about cybersecurity on international trade, it is not just a compliance issue, but also can be a business or geopolitical issue.

Framework to Understand Cybersecurity Concern and International Trade

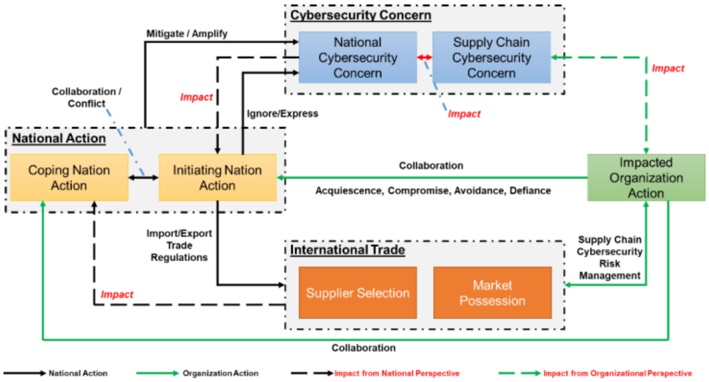

Cybersecurity Concern
National Cybersecurity Concern
Supply Chain Cybersecurity Concern
Mitigate / Amplify
Impact
Impact
Impact
Collaboration / Conflict
Ignore/Express
Impact
National Action
Coping Nation Action
Initiating Nation Action
Collaboration
Acquiescence, Compromise, Avoidance, Defiance
Impacted Organization Action
Import/Export Trade Regulations
Supply Chain Cybersecurity Risk Management
International Trade
Supplier Selection
Market Possession
Impact
Collaboration
National Action
Organization Action
Impact from National Perspective
Impact from Organizational Perspective

Fig 1: The concept model for the impact between cybersecurity concern and international trade

As shown in Figure 1, we have developed a conceptual model to understand the connection between the cybersecurity concerns and international trade:

1) **Cybersecurity concern is rising**: With the wide adoption of information and communications technologies (ICTs) in digital society, including critical infrastructures which military security, economic security and cultural security heavily rely on, cybersecurity has increasingly been invoked as a perspective of "national security". The definitions of national cyber security are not unique to different nations or organizations and different counties will emphasize different perspectives of national cyber security. For example, the U.S. once emphasized the controlling and punishing of cyber-attacks that involve economic espionage, although it is difficult to distinguish non-economic cyber-espionage activities from military attacks. On the other hand, Russia placed a heavy emphasis on military security whereas China emphasized the multi-dimensional aspects of cyber security, including military security, economic security and cultural security. The SCO emphasized the threat from using technologies to disrupt economic, social and political stability (Gechlik, 2017). Though the definition of national cyber security is still up for debate[8], it is no doubt that national cyber security is a multi-dimensional concept and all the different perspectives should be

[8] Sometimes the definition of national cyber security is intentionally vague to achieve some operating space. For example, take the EU-US Safe Harbour Agreement. The US has steadfastly refused to elaborate on the national security exception for data transfer (James Lockett, 2015). Please refer to the following link for details. "Commerce Official Says Safe Harbor Stalemate Continues Over National Security Issues", World Trade Online at Inside U.S. Trade, 12 March 2015, http://insidetrade.com/inside-us-trade/commerce-official-says-safe-harbor- stalemate-continues-over-national-security-issues.

considered, including the military security, political security, economic security and culture security.

From the other hand, most organizations, not only business but also governments, are becoming increasingly reliant on global supply chains, including both digital and physical supply chains. Nowadays, supply chain has become a significant cyber attack vector for many companies. The attackers can exploit the supply chain management vulnerability to introduce cyber threat to an organization. The most famous example using the supply chain vulnerability is the Stuxnet attack to the Iran nuclear facility by planting malwares including Stuxnet to the industrial control system which is then shipped to Iran, resulting in the destruction of some centrifuges for Iran's nuclear facility[9]. Another concern is related to data protection, including critical information like trade secrets or intellectual property. In 2017 alone, there were 541 major, publicly reported data breach incidents in which 1,922,663,085 records were compromised. These cyber risk from digital and physical supply chains, including increasing cyber attack vectors and data breaches, further deepen cybersecurity concerns.

Note that national cybersecurity and supply chain cybersecurity is not isolated. For example, the U.S. Department of Defense (DoD) "*buys products from international commercial and mixed defense and non-defense companies that service many customers, both within and outside of defense markets*" (Gansler, Lucyshyn, & Harrington, 2012). Hence, the cybersecurity from supply chain for the critical infrastructure will raise the concern about the national cybersecurity concern. On the other hand, the concerns of the national cybersecurity will impact the perception about the risks from supply chains and further impact the business' concerns on the supply chain cybersecurity.

2) **Nations[10] takes actions for national cybersecurity concern**: Considering cybersecurity concerns, to protect nations, organizations and individuals from potential cyber attacks, countries can intervene in cyberspace through cybersecurity policies and regulations to increase cyberspace offensive and defensive capability. There is no doubt that these policies and regulations will impact cyberspace, not only for the countries themselves, but the boarder globalized Internet society, resulting in an impact on international trade, including the import and export of IT goods and services. This is because of the important "National Security Exception" principle in the international trade context. The "Security Exception" under WTO and many region trade agreements (RTAs)[11] allow governments to take action when necessary in cases of "essential security interest".

As we focus on the cybersecurity impact on international trade, we only consider the nation's actions which will shape international trade relations. In another word, only the ones which can impact global supply chains, including the physical and digital supply chains will be considered here. Based on the governmental levers, we group the nation's actions as following categories:

[9] https://www.csmonitor.com/World/Security-Watch/2014/0225/Exclusive-New-thesis-on-how-Stuxnet-infiltrated-Iran-nuclear-facility

[10] In this paper, we consider the nation which initiates the actions impacting the international trade due to cybersecurity concern as the initiating nation; for the nation which responses to the actions the initiating nation use, we named them as coping nation.

[11] For example, under WTO, i.e. Article XXI (Security Exceptions) and Article XX (General Exceptions) of the GATT (General Agreement on Tariffs and Trade), Article XIVbis (security exceptions) of the GATS (General Agreement on Trade in Services), Article 73 of the TRIPS (The Agreement on Trade-Related Aspects of Intellectual Property Rights), Article XXIII of the GPA (The Agreement on Government Procurement). The "trans-pacific partnership (TPP)", "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory", with two sectoral exceptions- financial services and for government services and two general exceptions-privacy and essential security. The US and EU have been at odds about whether and to what extent the "Transatlantic Trade and Investment Partnership (TTIP)", should include provisions relating to the free flow of information and prohibitions on data localization. The "Trade in Service Agreement (TISA)" states "No party may prevent the transfer, access, processing or storing of information outside that Party's territory if conducted in connection with a business" except "essential security interests". The ASEAN-based Regional Comprehensive Economic Partnership (RCEP) and The "Free Trade Area of the Asia-Pacific (FTAAP)", are not clear but are unlikely to include data localization restrictions.

- **Ignore or Express Concerns**. For some specific cyber incidents or policies developed by other nations, governments can accept the potential risk and choose to ignore it, like the German Federal Intelligence Service (BND)[12] discovered that the then-US-based company NetBotz[13] sold security cameras with the built-in backdoor which sent videos to the US-Military's servers but hid it until 2015. Unlike just ignoring the potential risks, sometimes governments will express concerns or offer recommendations but without the mandate to warn citizens about potential cybersecurity threats, or response to the related policies or regulations from the other nations like listing those policies or regulations as trade barriers. For example, in 2017, the FBI briefed the private sector companies on intelligence claiming that Kaspersky Lab products are unacceptable threats[14]. There is no doubt that expressing such concerns about the cybersecurity risk with the imported products or services could impact international trade. Even without mandates, it can still impact the consumers' cybersecurity adoption behavior (Chen & Zahedi, 2016; Riek, Bohme, & Moore, 2016; Venkatesh, Thong, & Xu, 2012). According to reports from Reuters, the Best Buy Co pulled Kaspersky Lab's cybersecurity products from its shelves and websites on September 2017, due to the raising cybersecurity concerns about Kaspersky Lab's products in the U.S.[15]
- **Develop Import Trade Barriers**. Some nations will take actions to implement trade policies or regulations which will directly impact the import of international trades. Note that these actions can be initiatives for cybersecurity concerns, or used as the response to the initiatives from initiating nations. Based on the United Nations Conference on Trade and Development (UNCTAD) [UNCTAD 2012], the import-related trade barriers related to cybersecurity domain include: **the technical measures** such as setting the prohibition, authorization, or registration requirements which could prohibit the imports, or require the importer to receive authorization, permits or approval, or should be registered with the government agency; requiring the product to go through specific testing, certify the security assertion, or to go through some inspection; or the requirement for information traceability, like the origin of materials and parts, processing history, and distribution and location of products after delivery. For the **price control measures**, the most typical example is when the government charges additional taxes on imports that have or don't have internal equivalents. The **finance measures** refer to the regulations related to the access to and cost of foreign exchange for imports and define the terms of payment. The **trade-related investment measures** refer to the regulations related to foreign investment, including both direct and indirect scenarios. One typical measure, which is also a very common cybersecurity concern for national security, is the foreign direct investment (FDI) barrier referring the limitations on foreign equity participation and on access to foreign government-funded research and development programs, local content requirements, technology transfer requirements and export performance requirements, and restrictions on repatriation of earnings, capital, fees and royalties. In the cyberspace, due to the growth of the digital economy, we can observe growing **restrictions on post-sales and digital services**, restricting producers of exported goods to provide post-sales or digital service in the importing country. The most arguable regulations here is the **data localization regulations** by many

[12] The BND, Germany's only overseas intelligence service, acts as an early warning system to alert the German government to threats to German interests from abroad. It depends heavily on wiretapping and electronic surveillance of international communications. It collects and evaluates information in a variety of areas such as international non-state terrorism, weapons of mass destruction proliferation and illegal transfer of technology, organized crime, weapons and drug trafficking, money laundering, illegal migration and information warfare.

[13] The company was bought out by a German Company in 2007 and then bought out by the French corporation "Schneider Electric".

[14] https://www.cyberscoop.com/fbi-kaspersky-private-sector-briefings-yarovaya-laws/

[15] https://www.reuters.com/article/us-usa-kasperskylab-best-buy/best-buy-stops-sale-of-russia-based-kaspersky-products-idUSKCN1BJ2M4

countries, like Australia, Canada, EU, India, China, Russia, Vietnam etc[16]. **Government procurement** restrictions are the most common and powerful actions from the government. We can observe many cases related to government procurement over these years, including U.S. banned the use of Kaspersky Lab products in the government and military systems in 2017, the IT equipment from Cisco Systems Inc, Intel Corp's Security Software firm McAfee, and network and server software firm Citrix Systems, have been dropped from the China government procurement list[17] due to cybersecurity concerns. The last measure related to the import trade barriers is the **intellectual property**. Typically, this is allocated with testing and certification. Brazil's National Broadband Plan originally included a provision in the public contract for access to source code, and China's initial Compulsory Certification Program both initially required foreign vendors make their source code available to assure adequate security. Though these proposals were later walked back, the mandatory intellectual property disclosure will definitely impact the international trade, and raise intense disputes among nations[18].

- **Develop Export-related Trade Barriers**. refer to the measure impacting the export, including export-license, -quota, -prohibition and other quantitative restrictions, export technical measures, and export subsidies. For export-license, -quota, -prohibition, -certification and other quantitative restrictions, it will control the export number or even prohibit the export. The most significant measure here is the Wassenaar Arrangement, a 41-country international forum that seeks consensus among its members on dual-use export controls, adopted new controls on "intrusion software" and "carrier class network surveillance tools." in 2013[19]. For the export subsidies measure, the government can support the export of the products with built-in backdoor or discovered but non-disclosure vulnerability to the other countries, which will create the potential for potential hacking attacks in the future. The interesting example for this is the one we discussed above: the then-U.S. company sold the security camera with built-in backdoor extremely cheap to government-departments, to corporations operating with high-tech and military hardware.
- **Collaboration to Mitigate vs. Conflict to Amplify**. The World Trade Organization (WTO) is the only global international organization dealing with the rules of trade between nations. Trade regulations dealing with cybersecurity concerns could have been discussed in the meeting of the Technical Barriers to Trade (TBT) Committee. However, as the TBT Agreement was not originally implemented for the digital economy, some of the concerns will be considered beyond its scope. For example, China argues that "data storage and other similar matters were beyond the scope of the TBT Agreement" while the European Union considers ICT security certification as the "member State competence" so that the related implemented measures "fell outside the scope of the TBT Agreement". Besides the WTO TBT committee, some regional agreements and bilateral-dialogue mechanisms or agreements have been proposed or developed over these years which includes cybersecurity issues. For example, the "trans-pacific partnership (TPP)"[20] states "*No Party shall require a covered person to use or locate computing facilities in that Party's territory as a*

[16] https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures7-29-2016.pdf

[17] http://fortune.com/2015/02/26/why-china-is-making-life-miserable-for-big-u-s-tech/

[18] According to the NIST best practices for supply chain risk management, requiring the provision of source code is considered as a best practice to reduce the cyber risk from supply chain.

[19] There is still a lot of debates about what and how to include controls on "intrusion software" and "carrier class network surveillance tools" into the Wassenaar Arrangement

[20] The TPP was never entered into force as a result of the withdrawal of the U.S. In January 2018, all original TPP signatories except the U.S. conclude the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, known as CPTPP or TPP11. Please check this link for more details about CPTPP: https://en.wikipedia.org/wiki/Comprehensive_and_Progressive_Agreement_for_Trans-Pacific_Partnership

condition for conducting business in that territory", with two sectoral exceptions- financial services and government services and two general exceptions- privacy and essential security. The new trade deal reached between the U.S. and Mexico in August 2018 contains rules on copyright and intellectual property, and intends to "establish a notice-and-takedown system for copyright safe harbors for Internet service providers (ISPs) that provides protection for IP and predictability for legitimate technology enterprises who do not directly benefit from the infringement, consistent with United States law."[21] Another example here is the EU-US Safe Harbour Agreement, which was approved by the EU in 2000, and the updated version the EU-U.S. Privacy Shield Framework approved in 2016, regulates the data transfer between the EU and the US[22]. The first U.S.-China Law Enforcement and Cybersecurity Dialogue (LECD)[23] was held on October 4, 2017, and served as "an important forum for advancing bilateral law enforcement and cyber priorities between [our] two governments"[24].

On the other hand, some nations can choose an opposite option when considering the cybersecurity concern. For example, in July 2017, Rep. Brendan Boyle introduced the "No Cyber Cooperation with Russia Act", in response to U.S. President Donald Trump's comments on his meeting with Russian President Vladimir Putin at the G-20 summit about a potential establishment of a joint cybersecurity unit between the two countries, which would ban the use of federal funds to create, promote or support a joint cybersecurity program with Russia[25]. Though right now this bill is "in committee" and has not come to a vote yet, it reveals a high level of distrust and, consequently, a tense relationship between these two nations. In cyberspace, it has even been named "Cold War 2.0."[26] It is believed that escalation will continue, which will create huge challenges for cooperation on cybersecurity on both sides. Furthermore, the threat of sanctions or indictments have been suggested as an "deterrence" option which could create consequences for cyber espionage and coercive actions (Sheldon Whitehouse, McCaul, Evans, & Bhalotra, 2017).

3) **Impacted Organizations Takes actions for Cybersecurity Concern**: Given the increasing cybersecurity risks associated with an organization's suppliers of goods and services, supply chain cybersecurity risk management becomes a daily topic in the business executives' agenda. To secure the physical and digital supply chain, organization need to manage these key cyber supply chain risks (NIST, 2015), including (1) Third party service providers or vendors with physical or virtual access to information systems, software code, or IP; (2) Poor information security practices by lower-tier suppliers; (3) Compromised software or hardware purchased from suppliers; (4) Software security vulnerabilities in supply chain management or supplier systems; (5) Counterfeit hardware or hardware with embedded malware; (6) Third party data storage or data aggregators. This will definitely shape the organization's decision on supplier selection and market possession.

To enhance the cybersecurity for the global supply chain, some organizations will try to ***collaborate*** with their governments to initiate policies to impact the international trade. For example, on August 9, 2017,

[21] The details of the agreement aren't fully known when we drafted this version at August 28. This message is from the U.S. press. Please check more detail here: https://globalnews.ca/news/4415386/nafta-intellectual-property-laws/

[22] https://build.export.gov/main/safeharbor/eu/eg_main_018476

[23] The LECD is one of four dialogues agreed to by President Trump and President Xi during their first meeting in Mar-a-Lago in April 2017.

[24] https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue

[25] http://www.executivegov.com/2017/07/proposed-bill-seeks-to-block-potential-us-russia-cybersecurity-alliance/

[26] https://www.eastwest.ngo/sites/default/files/RIAC-EWI-Russia-US-Cybersecurity-Policybrief11-en.pdf

10 major cybersecurity companies[27] in U.S. wrote to the U.S. Trade Representative Robert Lighthizer to "incorporate cybersecurity trade issues in the upcoming modernization of the North American Free Trade Agreement (NAFTA)", such as "promot[ing] development and alignment of voluntary cyber risk management frameworks, [like the NIST Cybersecurity Framework] among the parties to NAFTA".

From the other hands, as more and more nations are implementing cybersecurity related international trade policies, organizations need to respond to these institutional processes. Normally, organizations will accept the government's cybersecurity-related policies, named "***acquiescence***", especially when these policies are related to national security concerns. We can observe that plenty of examples of the organizational reactions fall into this category. For example, when Russia's regulation of foreign e-service VAT became effective, more than 100 foreign tech giants just registered to accept the foreign e-services VAT structure in Russia, including Google, Apple, Microsoft, LinkedIn, Netflix, Bloomberg and the Financial Times in just a few months[28]. For some specific cases, organization will negotiate with the initiating nation for the cybersecurity regulations, tying to exact some concessions for both sides, named "***compromise***". One typical example here is for the end-to-end encrypted messaging app, Telegram, after being threatened with a ban in Russia, the company finally agreed to register with new Russian Data Protection Laws, but its founder has assured that the company will not comply to share users' confidential data at any cost: just register with the Russian government, but the company wouldn't store citizens' information on the Russian servers[29]. Sometimes, organization will make a totally different decision, to exit the market, or try to disguise nonconformity and pretend that the company already complied with the regulation while actually not having complied, named "***avoidance***". This may happen when the market is quite small, or complying with the regulation is too costly, or the institutional pressures from the mother-country are too intense, which will totally reshape the organization's global supply chain. Two typical examples include Google's withdrawal from China in 2010 due to criticism in the U.S. for helping the Chinese government pursue its cybersecurity goals and Huawei's withdrawal from U.S. in 2014 due to the continuous concerns over espionage. Normally bundled with avoidance, organization will challenge or attack the cybersecurity regulations from the initiating nations, named "***defiance***". For example, the VP of global public policy of LinkedIn challenged the Russian Data Protection Laws and stated that LinkedIn would not move Russian user data to Russian territory, while in 2017 Russia blocked LinkedIn. Finally, organization can also choose to work together with nations, both the initiating and coping nation, to mitigate the negative impact from the regulations, or even be involved in the regulation making process, named "***collaboration***"[30].

Cybersecurity in International Trade: Regulation? Business? Or Geopolitics?

Using the conceptual model to understand cybersecurity's impact on international trade, we have discussed the key components: the cybersecurity concerns include both national cybersecurity concern and supply chain cybersecurity concern, which can impact each other. There exist many different options for nations and organizations to deal with these cybersecurity concerns. Different actions from nations and organizations will end up into totally different results. Based on the national and organizational actions, we

[27] https://www.cyberscoop.com/cyber-ceos-urge-nist-framework-made-part-nafta-talks/

[28] Note that at that time, LinkedIn was still blocked to enter Russia. Please refer to the following links for detail : https://thestack.com/cloud/2017/04/11/facebook-joins-foreign-tech-firms-to-pay-russian-google-tax/

[29] https://thehackernews.com/2017/06/telegram-russia-partnership.html

[30] Here we use "collaboration" instead of "manipulation" from Oliver's theory about organizational actors' strategic responses to institutional processes. This is because in the international trade context, organizations work together with nations to influence the implemented or developing policies, while "manipulation" is too strong to describe these interactions between the public and private relations.

can identify three different loops in the conceptual model, representing the three different contexts for cybersecurity impact in international trade:

1) **Regulation Compliance Context**: in this scenario, as shown in Figure 2 (a), due to the national cybersecurity concern, the initiating nation will implement the import/export cybersecurity related trade policies, which will impact the international trade. Organizations consider these policies as regulations that they need to compliant with, and then use these regulations as the baseline guidance for their global supply chain risk management. In most cases, organizations can only accept these policies. In some other case, organizations can try to negotiate with the initiating nation to mitigate the negative impact, though the results can be totally different case-by-case. Nowadays, we can observe many cases belonging to this context, within which organization proactively react to the global cybersecurity policies. Given the reality that more and more cybersecurity related policies are coming, proactively reacting will create significant compliance cost and uncertainty for the organizational global supply chain.

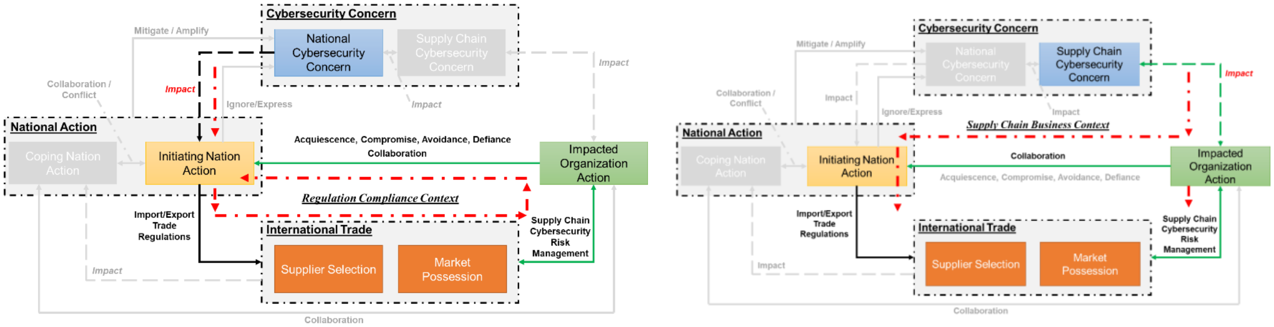


Fig 2 (a) [left]: Cybersecurity impact on International Trade: Regulation Compliance Context

Fig 2 (b) [right]: Cybersecurity impact on International Trade: Supply Chain Business Context

2) **Supply Chain Management Context**: in the supply chain management context, as shown in Figure 2 (b), organizations consider the cybersecurity risk from supply chain as an important business strategy decision and try to implement the supply chain cybersecurity risk management standard. To make this implementation easier, organization may even try to influent the mother-nation to implement some import/export trade regulations to further impact the international trade. These will work together to reshape the global supply chain.

3) **Geopolitics Context:** in this scenario, as shown in Figure 2 (c), the impact on international trade from cybersecurity is considered as the geopolitical topic. Considering the national cybersecurity concern, the initiating nation will use import/export trade regulations to impact the international trade, which will definitely impact the other nations. The coping nation will take different actions to react to these initiated trade regulations. Some global mechanisms like the WTO TBT Agreement and the General Agreement on Trade in Services (GATS) maybe used to discuss or negotiate these international trade disputes in cyberspace. Some recent regional trade agreements and bilateral-dialogue mechanisms or trade agreements have been created or negotiated with the intention to mitigate cybersecurity concerns in a more effective way, while some international organizations also get involved in these issues to promote behavior norms in cyberspace. For example, the U.S. and the EU worked together to develop the Privacy Shield Framework to replace the U.S.-EU Safe Harbor Framework for handling the data cross-border transfer issue. However, we can also observe that tense relationships can result in escalating cyber conflicts and digital trust can deteriorate. This

creates significant negative impacts on trade, and it can even result in a “trade war”. The Russia-U.S. cyber disputes in the past two years is a typical living example for this case.

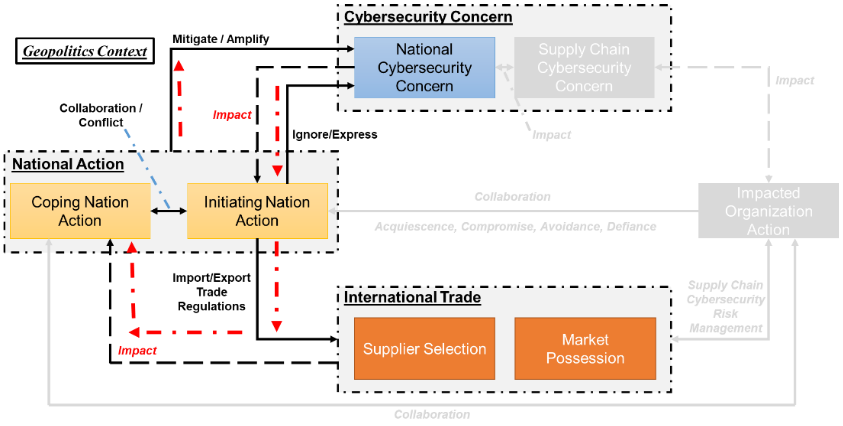


Fig 2 (c): Cybersecurity impact on International Trade: Geopolitics Context

Transformation among Regulation Compliance, Supply Chain Business and Geopolitical Context

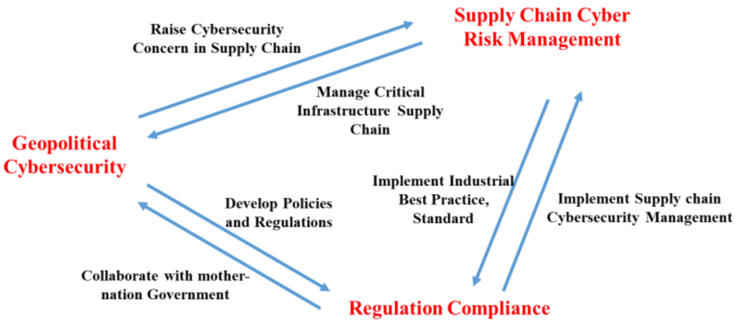

Raise Cybersecurity Concern in Supply Chain
Supply Chain Cyber Risk Management
Manage Critical Infrastructure Supply Chain
Geopolitical Cybersecurity
Implement Industrial Best Practice, Standard
Implement Supply chain Cybersecurity Management
Develop Policies and Regulations
Collaborate with mother-nation Government
Regulation Compliance

Fig 4: Transformation among Different Contexts

As summarized in Figure 4, using the developed framework, it can be seen that these three contexts are not independent but can be transformed among each other.

First of all, if the organization can collaborate with the mother-nations to take some actions, the regulation compliance context can be easily transformed into the geopolitical context. If the initiating nation and coping nation can work together to solve the raised cybersecurity dispute, it can help to mitigate the potential negative impact to international trade. One typical example here is that: considering the requirement to turn over the source code if selling computer equipment to Chinese banks, European and US companies have asked their authorities for urgent help in stopping the implementation of these new cyber security regulations. The U.S. trade representative has taken up the issue in formal talks with Chinese regulators and President Obama discussed the matter personally with President Xi Jinping in 2015. Finally, China proposed a new regulation in 2016. Secondly, if the organization can further use the regulation compliance pressure as an external factor to push the organization to consider the cybersecurity risk in the supply chain cybersecurity management, it can even create some positive impact for the international trade by reducing the supply chain cyber risk.

On the other hand, geopolitical pressure can sometime impact the organizational reactions to the initiating nation's cybersecurity policies. Google's withdrawal from China in 2010 was impacted by the criticism in the U.S. for helping the Chinese government pursue its cybersecurity goals. In addition, expressing the cybersecurity risk from nations can impact the supply chain cybersecurity concerns in the industry sector. For example, in 2017, The FBI briefed the private sector companies on intelligence claiming that Kaspersky Lab products are unacceptable threats[31]. Even without mandates, it still impacted the consumers' cybersecurity adoption behavior (Chen & Zahedi, 2016; Riek et al., 2016; Venkatesh et al., 2012). According to reports from Reuters, the Best Buy Co pulled Kaspersky Lab's cybersecurity products from its shelves and websites on September 2017, due to the raising cybersecurity concerns about Kaspersky Lab's products in the U.S.[32] Furthermore, this can impact the policy makers' perception and result in further actions. For example, for the smart toys, Germany's Federal Network Agency finally forbid illicit radio transmission equipment in toys and prohibited the selling of smart toy "My Friend Cayla" in February, 2017[33].

Finally, if organization can systematically consider the cybersecurity risk from supply chain and try to implement the best practice in each industry sector, it will definitely reshape the international trade, as when organization developers their global supply chain, they will not only just consider the supply chain efficiency like cost and revenue, but also take the cybersecurity risk from different vendors into consideration. Furthermore, just as we discuss before, critical infrastructures can impact the national security, their supply chain cybersecurity risk management can become an important topic for the geopolitical cybersecurity.

Regulation Compliance v.s. Supply Chain Strategy：Huawei's locked out from U.S. market but Continue in the U.K.

It can be seen that for the regulation context, initiating nation implements the relative policies and organization only proactively react to such policies, while for the supply chain business context, organization will consider the supply chain cybersecurity risk when implementing the global supply chain and influent nations to take some actions to mitigate such cybersecurity concern. This difference makes thing different. Here we can compare the Huawei's cases in the U.S. and U.K. as an example:

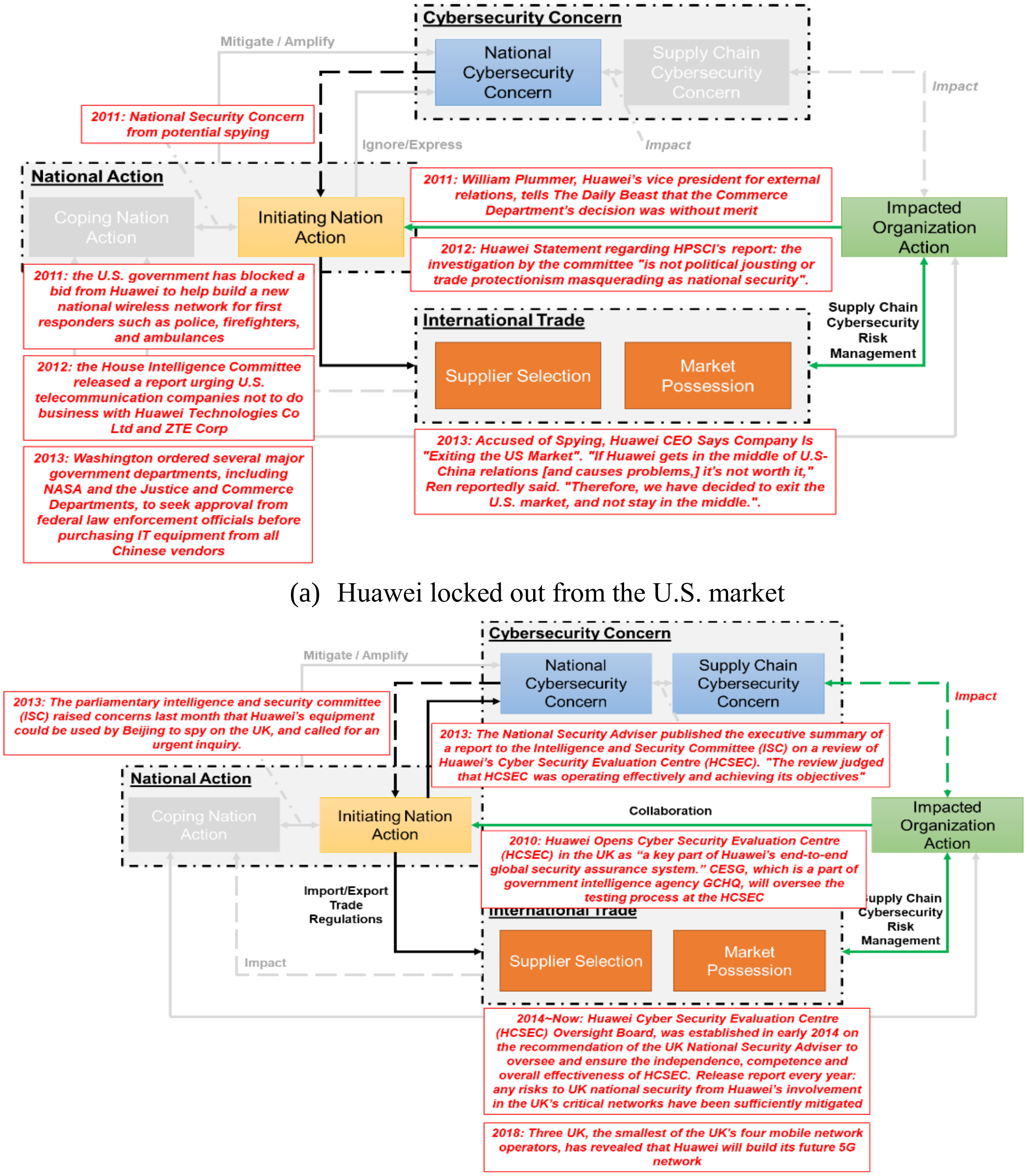
As shown in Figure 3 (a), since when Huawei, in a partnership with Bain Capital, proposed to buy 3Com for $2.2 billion in 2008 but banned by the US Committee on Foreign Investment (CFIUS) due to the "national security concern", Huawei's business in the U.S. become worse and worse over time. In 2011, worried about potential spying, the U.S. government blocked a bid from Huawei to help build a new national wireless network for first responders such as police, firefighters, and ambulances, though "the Commerce Department's decision was without merit" commented by Huawei's vice president for external relations later. In 2012, the U.S. further released a report urging U.S. telecommunication companies not to do business with Huawei Technologies Co Ltd and ZTE Corp because it said potential Chinese state influence on the companies posed a threat to U.S. security. Though the public portion of the report didn't offer actual examples, and Huawei state that "the investigation by the committee 'is not political jousting or trade protectionism masquerading as national security'. Unfortunately, the Committee's report not only ignored our proven track record of network security in the United States and globally, but also paid no attention to the large amount of facts that we have provided.", in 2013, Washington ordered several major government departments, including NASA and the Justice and Commerce Departments, to seek approval from federal law enforcement officials

[31] https://www.cyberscoop.com/fbi-kaspersky-private-sector-briefings-yarovaya-laws/

[32] https://www.reuters.com/article/us-usa-kasperskylab-best-buy/best-buy-stops-sale-of-russia-based-kaspersky-products-idUSKCN1BJ2M4

[33] http://www.npr.org/sections/thetwo-way/2017/02/17/515775874/banned-in-germany-kids-doll-is-labeled-an-espionage-device

before purchasing IT equipment from all Chinese vendors, requiring the agencies to make a formal assessment of “cyber-espionage or sabotage” risk in consultation with law enforcement authorities when considering buying information technology systems. The assessment must include “any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized” by China. Finally, in 2014, Huawei had no choice but was "exiting the US Market". "If Huawei gets in the middle of U.S-China relations [and causes problems,] it's not worth it. Therefore, we have decided to exit the U.S. market, and not stay in the middle."



2011: National Security Concern from potential spying

2011: William Plummer, Huawei’s vice president for external relations, tells The Daily Beast that the Commerce Department’s decision was without merit

2012: Huawei Statement regarding HPSCI's report: the investigation by the committee "is not political jousting or trade protectionism masquerading as national security".

2011: the U.S. government has blocked a bid from Huawei to help build a new national wireless network for first responders such as police, firefighters, and ambulances

2012: the House Intelligence Committee released a report urging U.S. telecommunication companies not to do business with Huawei Technologies Co Ltd and ZTE Corp

2013: Washington ordered several major government departments, including NASA and the Justice and Commerce Departments, to seek approval from federal law enforcement officials before purchasing IT equipment from all Chinese vendors

2013: Accused of Spying, Huawei CEO Says Company Is "Exiting the US Market". "If Huawei gets in the middle of U.S-China relations [and causes problems,] it's not worth it," Ren reportedly said. "Therefore, we have decided to exit the U.S. market, and not stay in the middle.".

(a) Huawei locked out from the U.S. market

2013: The parliamentary intelligence and security committee (ISC) raised concerns last month that Huawei's equipment could be used by Beijing to spy on the UK, and called for an urgent inquiry.

2013: The National Security Adviser published the executive summary of a report to the Intelligence and Security Committee (ISC) on a review of Huawei's Cyber Security Evaluation Centre (HCSEC). "The review judged that HCSEC was operating effectively and achieving its objectives"

2010: Huawei Opens Cyber Security Evaluation Centre (HCSEC) in the UK as “a key part of Huawei’s end-to-end global security assurance system.” CESG, which is a part of government intelligence agency GCHQ, will oversee the testing process at the HCSEC

2014~Now: Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, was established in early 2014 on the recommendation of the UK National Security Adviser to oversee and ensure the independence, competence and overall effectiveness of HCSEC. Release report every year: any risks to UK national security from Huawei’s involvement in the UK’s critical networks have been sufficiently mitigated

2018: Three UK, the smallest of the UK's four mobile network operators, has revealed that Huawei will build its future 5G network

(b) Huawei continues business in the U.K

Fig 3: Huawei’s Cases in the U.S and the U.K

On the other hand, as shown in Figure 3 (b), in 2010, Huawei opened its Cyber Security Evaluation Centre in the UK. "*The new Cyber Security Evaluation Centre is a key part of Huawei's end-to-end global* *security assurance system. This centre is like a glasshouse – transparent, readily accessible, and open to regulators and our customers*," said John Frieslaar, Managing Director, Huawei Cyber Security Evaluation Centre. "*The establishment of this Centre demonstrates our commitment to building mutual trust in the area of cyber security and to continuously delivering high-quality and reliable communications networks to our customers in the UK*."

The UK government's National Technical Authority for Information Assurance (CESG), which is a part of government intelligence agency Government Communications Headquarters (GCHQ), will oversee the testing process at the Cyber Security Evaluation Centre. In 2013, when the parliamentary intelligence and security committee (ISC) raised concerns that Huawei's equipment could be used by Beijing to spy on the UK, and called for an urgent inquiry, the U.K. National Security Adviser then published the executive summary to the ISC on a review of Huawei's Cyber Security Evaluation Centre (HCSEC) concluding that "The review judged that HCSEC was operating effectively and achieving its objectives".

In early 2014, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, was further established on the recommendation of the UK National Security Adviser to oversee and ensure the independence, competence and overall effectiveness of HCSEC. Every year it will release a report about any risks to UK national security from Huawei's involvement in the UK's critical networks and make sure that these risks have been sufficiently mitigated. Hence, though the U.S., and Australia continue to lock Huawei out from their 5G markets, in August 2018, the Three UK, the smallest of the UK's four mobile network operators, revealed that Huawei will build its future 5G network.

This in-depth case study, about Huawei's business in U.S. and U.K., shows that if the organization can consider the cybersecurity risk from the global supply chain perspective, it is possible for organization to help to reduce the national cybersecurity concern and enhance the global supply chain security. More importantly, it reveals a potential to turn the regulation compliance context to supply chain context, instead of resulting into geopolitical cyber conflict.

Conclusion

With the development of the digital economy, cyberspace plays an increasingly critical role in international trade. Cybersecurity concerns, including the national and supply chain cybersecurity concern, motivate nations and organizations to take actions intending to protect cyberspace and reduce potential cybersecurity risks. The various implemented policies and regulations are reshaping international trade relations while some mechanisms and agreements have been proposed or developed to solve cyber conflicts and mitigate the negative impact on international trade.

Cybersecurity is becoming an important issue for all nations involving global supply chains. Due to the lack of consensus on cyberspace behavior norms and the vague definitions of national cyber security, we can observe and expect even more cyber conflicts and its negative impact on international trade in the near future. The good news is that recently there have been and there continue to be many efforts made to reach some consensus on cyberspace, especially with regards to the behaviors of the state. Though the details about national cyber security are still not clear, it is widely accepted that national cybersecurity includes many different perspectives and different nations emphasize different views. However, instead of each nation proposing its own set of norms that will inevitably be at odds with one other, finding common ground and working together to construct cybernorms is an arduous but necessary task.

From the organization's perspective, "cybersecurity is no longer an option". This is especially true for the companies that rely heavily on Internet technology or global, physical, and digital supply chains. The impact on these companies from cybersecurity will become more and more significant in the future. Instead of only considering cybersecurity a regulation issue and trying to comply with the emerging policies and regulations, organizations should become involved in the regulation processes, not only during the comment periods but also during the regulation draft process. Since right now there are still no cybernorms in international trade, there is still a long way to go. Different industrial sectors will have specific characters in cyberspace, so one good option is for organizations to work together to build best practices or guiding rules following the relevant specific technical trends and market requirements, creating industrial best practices focusing on the global supply chain cybersecurity management. Though it would be a voluntary measure at the very beginning, once it is widely accepted across the industry sector, it could become the "de facto" cybernorm needed to mitigate the negative impact from cybersecurity concerns. Further, it could move cybernorms forward among different nations in cyberspace.

The developed conceptual model identifies three different contexts when considering the cybersecurity impact on the international trade: the regulation compliance context within which organizations proactively react to the national cybersecurity policies; the supply chain management context within which organizations consider the supply chain cybersecurity as a strategy issue and try to reduce the cyber risks from global supply chain; and the geopolitical context where nations can collaborate to mitigate the cybersecurity impact or conflict with each other to amplify the dispute. More importantly, these three contexts are not independent but can be transformed to each other. Given the reality that there is no cybernorms, or difficult to achieve a cybernorm in cybespace in the near future, if the whole system was looped into the geopolitical context, it can even result into "cyber trade war". To avoid this situation, the whole society, especially the business community, should work together some industrial best practice to guide the issue out from the "tit for tat" mire, not only to improve the supply chain cybersecurity management and reduce the cybersecurity concern from global supply chain, but also help to reduce the national cybersecurity concerns.

In the future, based on this conceptual model, we are going to develop a framework to further understand the dynamics of the national and organizational actions which can support the decision making process.

Acknowledgement

This work is partially supported by the MIT Internet Policy Research Initiative, and Cybersecurity at MIT Sloan (the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, MIT-(IC)^3). The authors thank members from the Cybersecurity at MIT Sloan for their valuable comments and inputs.

References

Burri, M. (2017). The Regulation of Data Flows Through Trade Agreements. *Georgetown Journal of Internato nal Law*, *48*, 407–448.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors Polycontextual Contrasts Between the united states and china. *MIS Quarterly*, *40*(1), 205–222.

Clapper, J. R., Lettre, M., & Rogers, M. S. (2017). Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States.

Friedman, A. A. (2013). Cybersecurity and Trade: National Policies, Global and Local Consequences. *Brookings Institution Center for Technology Innovation*, (September), 1–18.

Gansler, J. S., Lucyshyn, W., & Harrington, L. H. (2012). Defense Supply Chain Security: Current State and Opportunities for Improvement.

Gechlik, M. (2017). Appropriate Norms of State Behavior in Cyberspace : Governance in China and Opportunities for US Businesses. In *Conference on US-China Relations: Cyber and Technology* (pp. 1–24). National Security, Technology, and Law Working Group of the Hoover Institution.

James Lockett. (2015). Where High and Low Politics Meet: National Security and Cybersecurity. *WORLD ECONOMIC FORUM*, (August), 18–21.

Klimburg, A. (2012). *National Cyber Security Framework Manual*. *NATO CCD COE Publication*. https://doi.org/10.1017/CBO9781107415324.004

Kshetri, N. (2016). *Cybersecurity-Related Barriers to International Trade and Investment*. *The Quest to Cyber Superiority*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2809819

Lynn, W. J. (2010). Defending a New Domain the Pentagon's Cyber Strategy. *Foreign Affairs*, *89*(5), 98. Retrieved from http://www.scribd.com/doc/36500793/Defending-a-New-Domain-the-Pentagon-s-Cyber-Strategy

Maness, R. C., & Valeriano, B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society*, *42*(2), 301–323. https://doi.org/10.1177/0095327X15572997

Mata, D. C. (2015). Cybersecurity Dimensions of National Security. *Journal of Law and Administrative Sciences*, 132–142.

Mitchell, A. D., & Hepburn, J. (2016). Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. *The Yale Journal of Law and Technology*, (October 2016), 1–35.

NIST. (2015). Cyber Supply Chain Best Practices. In *Best Practices in Cyber Supply Chain Risk Management* (pp. 1–3).

OECD. (2012). *Cybersecurity Policy Making at a Turning Point*. *OECD Digital Economy Papers*. Paris. https://doi.org/http://dx.doi.org/10.1787/5k8zq92vdgtl-en

Ranger, S. (2017). US intelligence: 30 countries building cyber attack capabilities. Retrieved from http://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. https://doi.org/10.1109/TDSC.2015.2410795

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. https://doi.org/10.1093/ijlit/eax010

Sheldon Whitehouse, McCaul, M. T., Evans, K., & Bhalotra, S. (2017). *From Awareness to Action: A Cybersecurity Agenda for the 45th President*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160103_Lewis_CyberRecommendationsNextAdministration_Web.pdf

Slayton, R. (2017). What Is the Cyber Offense-Defense Balance? *International Security*, *41*(3), 72–109. https://doi.org/10.1162/ISEC

Sun, N. (2016). Piercing the Veil of National Security: Does China's Banking IT Security Regulation Violate the TBT Agreement. *Asian Journal of Wto & International Health Law and Policy*, *11*(2), 395–436.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). CONSUMER ACCEPTANCE AND USE OF INFORMATION TECHNOLOGY: EXTENDING THE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.1111/j.1540-4560.1981.tb02627.x

Verizon. (2017). *2017 Data Breach Investigations Report*.