Interactions Between Cybersecurity and International Trade: A Systematic Framework

Keman Huang, Stuart Madnick, and Simon Johnson

Working Paper CISL# 2018-13

November 2018

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

Working Paper – November 2018

Interactions Between Cybersecurity and International Trade: A Systematic Framework

Keman Huang, Stuart Madnick, Simon Johnson

Abstract

Issues of international trade policy have gained increased attention while cybersecurity has not been a key issue for trade policy until recently. Cybersecurity concerns have presented significant challenges, and cybersecurity-related allegations have become a major source of growing commercial disputes. The future of cybersecurity in international trade will shape not only cyberspace for the countries directly, but also the broader globalized society. However, it is still not clear how cybersecurity and international trade can impact each other, whether the current implemented policies can sufficiently resolve problems, and what can be done to retune the negative impacts of cybersecurity concerns on international trade. To investigate these influences, this paper uses real-world case study, in-depth domain subject expert interviews and workshop practices to develop a systematic framework to understand the relations between cybersecurity concern and international trade. We focus on the different types of cybersecurity concerns, national and organizational actions for cybersecurity concerns and global supply chain management. From these we identify three scenarios (regulation compliance scenario, supply chain strategy scenario and geopolitical scenario) and three mechanisms (the gap between national cybersecurity concerns, public-private cybersecurity management and supply chain risk management) which represent the interaction between cybersecurity concern and international trade. This study reveals that cybersecurity concerns in international trade are not just a regulation compliance issue but should be considered a business strategy issue and geopolitical issue. More importantly, to retune the current "tit for tat" circle, businesses should not only passively react to cybersecurity concerns in international trade context, but need to actively involve themselves in cybersecurity concerns mitigation and policy implementation procedures. In this way, cybersecurity concern pressure can even be used to improve the global supply chain and create competitive advantage.

1 Introduction

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 on which military

security, economic security and culture security rely heavily. 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; N Kshetri 2016; Mata 2015)[1].

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

From the defensive perspective, what should countries do to prevent cyber intrusions? Since it is impractical to examine the millions of lines of software or firmware in all products[4], how can governments and organizations prevent trade from introducing 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 strategy 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, 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. 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. Memories of the 2017 Equifax Data Breach are still fresh; personal information of 143 million consumers was exposed in the incident. Hence, we can predict data localization policies, which restrict the transfer of data across borders around the world (Burri 2017; Mitchell and Hepburn 2016; Selby 2017), becoming a topical issue during the negotiation of trade

---

[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; N 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.

[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.

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, like various barriers to international trade and investing. These policies will shape not only cyberspace for the countries themselves, but the broader globalized society (Friedman 2013; James Lockett 2015). Although we have witnessed many international trade restrictions due to cybersecurity concerns, such as Kaspersky's ban in the U.S., LinkedIn's restriction in Russia, the restriction of data flow to India from the E.U., the restriction of VPN in China etc., there exists no systematic framework to understand how cybersecurity concerns evolve in the international trade context. We investigate how cybersecurity concerns impact international trade, how international trade can impact cybersecurity concerns, whether the implemented policies really solve those concerns, and what can be done to mitigate the negative impacts from them. Of particular concern, recently the international community has become trapped in a "tit for tat" circle, which may eventually result in a "cyber cold war." Without a clear understanding of larger impacts, governmental agencies are implementing policies that may result in cyber conflicts, while businesses struggle to adapt to evolving cybersecurity concerns and restrictions.

In this paper, we intend to develop a systematic framework to understand the connections between cybersecurity concern and international trade. Considering cybersecurity's importance in both the public and private sector, we split the cybersecurity concerns into national cybersecurity concern and supply chain concern. Raising national cybersecurity concerns incites nations to implement cybersecurity related policies which can reshape the international trade environment. Geopolitical relations can impact these policies, and conversely, the policies can retune the geopolitical relations. Business involving in the global supply chain must react to institutional pressure from policies, which affects their international trade behaviors. On the other hand, cybersecurity concern through the international supply chain makes organizations rethink their global supply chain, not only the physical, but also the digital supply chain, to protect organizational assets. Concerns, national and organizational actions and the international trade environment combine into an evolving system through which national cybersecurity policy and organization supply chain management is implemented. This system inspires us to create a systematic framework that will decompose the interactions among cybersecurity concern and international trade. 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 through which to study these cybersecurity related actions and advocate for creating standards for international trade in cyberspace.

To dig into this evolving system, we collect 33 real-world cases covering 149 events related to cybersecurity concern and international trade over the last few decades. We use these cases to verify and retune the presented framework. From these cases we see that cybersecurity concern in the international trade environment becomes a worldwide phenomenon even at the earliest stages. Furthermore, we conducted a domain expert interview and a workshop discussion based on the

[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.

developed framework. This research revealed that cybersecurity concerns in international trade should not be considered as only a regulation compliance issue, but also as a supply chain risk and geopolitical issue. We observed significant gaps between the understanding of cybersecurity concerns among different nations, between public and private sector and along supply chain management. We conclude that companies should not passively react to cybersecurity regulations in international trade environment, but need to involve themselves in cybersecurity concern mitigation and policy implementation procedures. This will not only drag the system out from the "tit-for-tat" circle, but also further improve cybersecurity within the international trade environment and promote the development of the global digital economy.

This paper contributes to our understanding of trade both theoretically and practically. From the theoretical perspective, this paper develops a systematic framework to understand the relation between cybersecurity concern and international trade. The framework encapsulates current understanding about cybersecurity concern, supply chain risk management, geopolitical relation, international trade, public-private relation and organizational institutional pressure theory, Three mutual influence scenarios, including regulation compliance scenario, supply chain strategy scenario and geopolitical scenario, and three impact mechanisms, including the gap between national cybersecurity concerns, public-private cybersecurity management and supply chain risk management, are further identified. The framework enables further research on the dynamic evaluation of cybersecurity-related policy. From the practical perspective, our research suggests that businesses should not passively struggle in the increasingly intensive international trade environment due to cybersecurity concern. Businesses should actively involve themselves in the global supply chain cyber risk management and policy implementation procedure, which may be able to "turn the ship" to avoid a "cyber cold war" in the global digital economy.

The rest of this paper is organized as follows: Section 2 discusses related concepts. Section 3 develops the framework to decompose the relations among cybersecurity concern and international trade environment. Section 4 digs deeper into the real-world cases to verify the presented taxonomy. Based on the further interview and workshop discussion, section 5 discusses the three scenarios and mechanisms to understand the impact of cybersecurity concerns on international trade. Section 6 concludes this paper.

2 Key Concepts

Before we detail our framework for understanding the relations between international trade and cybersecurity concern, in this section we will discuss the key concepts related to this topic.

2.1 National Cyber Security

Since cyberspace was officially labeled as the fifth operational domain (after air, land, sea and space) (Welch 2011), cybersecurity has become an important aspect of national security (Mata 2015). The NATO CCD COE identified the five main perspectives of national cyber security as (Klimburg 2012):

1) **Military Cyber**. Nowadays many governments are building skills to wage cyber war (Liff 2012)

and developing military cyber capability. This military cyber capability can be used as an option for military activities, including "*enabling protection of their own defense networks, enabling network centric warfare capabilities, battlefield or tactical cyber warfare and strategic cyber warfare*" (Klimburg 2012). Military cyber involves both cyber offense and defense capability[7].

2) **Counter Cyber Crime**. Cybercrime activities include not only attacks that impact individual citizens and corporations, but also those that support military cyber activities and cyber terrorism[8].

3) **Intelligence and Counter-Intelligence**. Cyber espionage can be perpetrated by a state, a criminal group operating on behalf of a state or a criminal group operating on its own and stealing intellectual property or government secrets. A government requires the capabilities to detect, combat and respond to such activities.

4) **Critical Infrastructure Protection and National Crisis Management**. The majority of critical infrastructures are increasingly connected to cyberspace. Critical Infrastructure Protection (CIP) requires that infrastructure providers, in both the public and private sector,[9] be a part of the national security framework. National crisis management "*must be extended by an additional cyber component*" (Klimburg 2012).

5) **Internet Governance**. Cyberspace has become an important space for people's daily life. How the state and non-state actors interact to manage cyberspace and maintain its stability is considered a main aspect of national security[10].

Alternately, the "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization (SCO) on Cooperation in the Field of International Information Security" consider the following to be the main threats in the field of ensuing international information security: "*development and use information weapons, preparation for and waging information war; information terrorism; information crime; use of dominant position in information space to the detriment and interests and security of other states; dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural sphere of other states; natural and/or man made threats to safe and stable operation of global and national information infrastructures*"[11]. Furthermore, the International Code of Conduct for Information Security, was submitted to the General Assembly of the United Nations in January 2015 by the six founding member states of the SCO

---

[7] According to the joint statement by US Director of National Security, James Clapper, the Undersecretary of Defense for Intelligence, Marcel Lettre, and NSA and US Cyber Command Director, Admiral Mike Rogers, at a hearing on foreign cyber threats by the Senate Armed Services Committee, more than 30 countries are developing offensive cyber attack capabilities and "protecting critical infrastructure crucial energy, financial, manufacturing, transportation, communication, and health systems, will become an increasingly complex national security challenge". Please refer to (Ranger 2017) and (Clapper, Lettre, and Rogers 2017) for more details. Currently, there are five counties that are believed to have the most highly developed cyber warfare capabilities: the United States, China, Russia, Israel and the United Kingdom. We can also see that many cyber conflicts involve these countries. Iran and North Korea are also considered notable players in this domain. Please refer to (Breene 2016) for details.

[8] The definition of cyber terrorism is still not very clear. The most well-known and respected definition is from Dorothy Denning: "…[H]ighly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction or disruption against digital property."(Denning 2007)

[9] In the US, most service providers, including those who provide public utilities, finance or telecommunications services, are in the private sector, requiring collaboration between the private and public sectors to involve the cybersecurity domain.

[10] In this paper, we are not going to argue for or against cyber diplomacy or internet governance, but to understand the concerns about national cyber security and how such concerns impact international trade.

[11] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). "Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security [unofficial translation]." https://ccdcoe.org/sco.html https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

intending to promote the appropriate norms of state behavior in cyberspace (Gechlik 2017), listing 13 codes "*to identify the rights and responsibilities of States in the information space, promote constructive and responsible behaviour on their part and enhance their cooperation in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open and founded on cooperation, and to ensure that the use of information and communications technologies and information and communications networks facilitates the comprehensive economic and social development and well-being of peoples, and does not run counter to the objective of ensuring international peace and security*" (UN 2015).

It has proved difficult to create cybernorms, as different nations and organizations have different ideologies and practices as well as enormous interests at stake. From a cyber-threat perspective, Nir Kshetri (Nir Kshetri 2016) defined national cyber security threats from four distinct perspectives:

1) Military Security Threats. The military's capability to protect from forceful coercion and to fight wars could be impacted by cyberspace operations[12].

2) Political Security Threats. Cyberspace can be used to launch attacks which can impact a government's political authority, governing capacity and the capability of being recognized[13].

3) Economic Security Threats. Economic security includes trade, production and finance. IP theft and other problems associated with economic espionage is one of the main concerns for the U.S. Much cybercrime, especially organized cybercrime, has been financially motivated.

4) Societal, Socio-Cultural or Cultural Security Threats. Societal, socio-cultural or cultural security involves the sustainability of collective identities and value.

Note that 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. has 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[14], there is no doubt that national cyber security is a multi-dimensional concept and all the different perspectives should be considered. The concerns from these different cyber threat perspectives motivate different policies and regulations in different countries, and are proposed by governments or independent industry organizations.

---

[12] An example is offered in (Nir Kshetri 2016) P14: speaking at a military conference in August 2012, a former ground commander in Afghanistan acknowledged that he used cyber-attacks against an adversary in 2010: "I was able to use my cyber operations against my adversary with great impact. I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations".

[13] The hacker group "Anonymous" is a very famous group that has attacked government websites, using the Internet to express political or social protest. Another example is the use of social networks during the Arab Spring. Note that we are not for or against any specific policies on how to use and govern the Internet, as Internet governance is still a topic that is open to debate.

[14] 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 U.S. 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.

2.2 National Security Exception for Cybersecurity

How can these national cyber security concerns impact international trade? To answer this question, we look to the important "*National Security Exception*" principle in the international trade context. The "*Security Exception*" under WTO and many region trade agreements (RTAs)[15] allows governments to take action when necessary in cases of "*essential security interest*". For example, Article XXI of the GATT, "Security Exceptions", stipulates that:

"*Nothing in this Agreement shall be construed:*

(a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests;

or (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;

or (c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security (emphasis added)."

Article XXIII of the GPA, "Exceptions to the Agreement" stipulates that:

"*1. Nothing in this Agreement shall be construed to prevent any Party from taking any action or not disclosing any information which it considers necessary for the protection of its essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes.*

2. Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail or a disguised restriction on international trade, nothing in this Agreement shall be construed to prevent any Party from imposing or enforcing measures: necessary to protect public morals, order or safety, human, animal or plant life or health or intellectual property; or relating to the products or services of handicapped persons, of philanthropic institutions or of prison labour."

In other words, a member will not be prevented from taking any action which it considers necessary in order to protect their essential security interests. Generally speaking, the security exception embraces five categories: (1) national security information; (2) fissionable materials; (3) military goods and services; (4) war or international emergencies; and (5) UN obligations.

[15] 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 U.S. 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.

In the cybersecurity context, we can see that Article XXI(a), (b)(ii)(iii) of the GATT and Article XXIII:1 of the GPA are the most relevant portions of the exceptions. For example, the government procurement policies of many countries will require that data related to national security and the defense sector should be stored in domestic servers (Mitchell and Hepburn 2016), which can be considered as related to the Article XXI(a) of the GATT and covered in Article XXIII:1 of the GPA. Furthermore, for the US-EU "Safe Harbor" framework, the national security exception allows firms to deviate from the data protection principles in the agreement if they receive a request from law enforcement or intelligence authorities for personal data.

However, this security exception is considered self-defining, or so-called "self-judging" or "self-interpretation"[16] and it is expected to remain unclear in the near future. This raises many cybersecurity conflicts, and it has proven difficult to argue against measures or actions by one country on the grounds of national security.

2.3 Non-tariff barriers/measures to trade

Non-tariff barriers (NTBs), also known as Non-tariff measures (NTMs) are generally defined as "*policy measures other than ordinary customs tariffs that can potentially have an economic effect on international trade in goods, changing quantities traded, or prices or both*". Under this broad definition, NTBs include any policy measures other than tariffs that can impact trade flows (Organization for Economic Co-operation and Development 2005; Staiger 2012). The Trade Analysis and Information System (TRAINs) dataset includes more than 100 different types of NTBs. Basically, the NTBs can be divided into three categories (Staiger 2012):

1) **Imports**. This category refers to the NTBs imposed on imports, including import quotas, import prohibitions, import licensing, customs procedures, and their administration fees.

2) **Exports**. This category refers to the NTBs imposed on exports, including export taxes, export subsidies, export quotas, export prohibitions, and voluntary export restraints.

3) **Behind-the-Border Barriers**. Unlike the other two categories, this category refers to barriers imposed internally in the domestic economy, including domestic legislation covering health/technical/product/labor/environmental standards, internal taxes or charges, and domestic subsidies.

Beside the tariff measures, the United States Trade Representative (USTR) sorts foreign trade barriers (USTR 2017) into ten different categories including:

1) Import policies, including quantitative restrictions, import licensing, customs barriers, and other market access barriers;

2) Sanitary and phytosanitary measures and technical barriers to trade;

3) Government procurement (e.g., "buy national" policies and closed bidding);

4) Export subsidies (e.g., export financing on preferential terms and agricultural export subsidies that displace U.S. exports in third country markets);

5) Lack of intellectual property protection (e.g., inadequate patent, copyright, and trademark

[16] For the security exceptions, "considers it necessary" for the protection of its essential security interests, some argued that it is up to the member to decide while some argued that security exceptions are not wholly self-judging (Peng 2015). This debate is out of scope in this paper. But the unclear legal setting raises many cybersecurity issues.

regimes and enforcement of intellectual property rights);

6) Services barriers (e.g., limits on the range of financial services offered by foreign financial institutions, restrictions on the use of foreign data processing, and barriers to the provision of services by foreign professionals);

7) Investment barriers (e.g., 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);

8) Government-tolerated anticompetitive conduct of state-owned or private firms that restricts the sale or purchase of U.S. goods or services in the foreign country's markets;

9) Digital trade barriers (e.g., restrictions and other discriminatory practices affecting cross-border data flows, digital products, Internet-enabled services, and other restrictive technology requirements); and

10) Other barriers (barriers that encompass more than one category, e.g., bribery and corruption, or barriers that affect a single sector).

To effectively understand and access the non-tariff measures, the United Nations Conference on Trade and Development (UNCTAD) developed a tree-structure taxonomy to organize all non-tariff measures based on their scope and/or design (UNCTAD 2012):

1) Sanitary and phytosanitary measures, known as SBS, refers to measures such as restrictions for substances and ensuring food safety, and those for preventing dissemination of disease or pests.

2) Technical measures, known as TBT, refers to measures such as labeling, standards on technical specifications and quality requirements, and other measures protecting the environment.

3) Pre-shipment inspections and other customs formalities, refers to the measures like Pre-shipment inspection, Direct consignment requirement, Requirement to pass through specified port of customs, and Import-monitoring and -surveillance requirements and other automatic licensing measures.

4) Contingent measures, refers to measures implemented to counteract particular adverse effects of imports in the market of the importing country, including antidumping, countervailing and safeguard measures.

5) Non-automatic Licensing, Quotas, Prohibitions and Quantity-control Measures other than for SPS or TBT reasons and Price-control measures to control or affect the prices of imported goods, including additional taxes and charges.

6) Finance measures, refers to the measures to regulate access to and cost of foreign exchange for imports and define the terms of payment.

7) Competition-related measures, refers to the measures to grant exclusive or special preferences or privileges to one or more limited group of economic operators

8) Distribution Restrictions, refers to the distribution limitation which can be controlled through additional license or certification requirements.

9) Post-sales services Restrictions, refers to the requirements that restrict producers of exported goods to provide post-sales services in the importing country.

10) Import Subsidies, refers to the financial contribution by a government or public body, or via government entrustment or direction of a private body or income or price support, which confers a

benefit and is specific.

11) Government Procurement Restrictions, refers to the measures controlling the purchase of goods by government agencies, generally by preferring national providers.

12) Intellectual Property, refers to the measures related to intellectual property rights in trade: Intellectual property legislation covers patents, trademarks, industrial designs, layout designs of integrated circuits, copyright, geographical indications and trade secrets.

13) Rules of Origin, covers laws, regulations and administrative determinations of general application applied by government of importing countries to determine the origin country of goods.

14) Export-Related Measures, refers to the measures applied by the government of the exporting country on exported goods, including Export-license, -quota, -prohibition and other quantitative restrictions, Export technical measures like certification required by the exporting country, and Export subsidies.

In the cybersecurity context, intuitively, the measures belonging to the TBT, government procurement restrictions, intellectual property, post-sales services restrictions, finance measures and export-related measures can impact and reshape the cyberspace. In the following sections, we will further discuss the specific measures related to cybersecurity which can impact international trade.

2.4 Cyber Impact to Physical/Digital Supply Chain

Nowadays, most organizations, not only in the private sector but also governmental agencies, are becoming increasingly reliant on global supply chains. 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, and Harrington 2012). This globalization raises the critical requirement of supply chain security, "*the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent, the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain*" (Gansler, Lucyshyn, and Harrington 2012). From a cybersecurity perspective, supply chain security can be further defined as "*a program that focuses on the potential risks associated with an organization's suppliers of goods and services*" (Shackleford 2015). Suppliers may have extensive access to resources and assets within the enterprise environment, including the products, the organizations' customer environments or even critical intellectual property like source codes. This access increases the supply chain cyber risk for the organizations. The organizational cyber boundary has been extended to the supply chains. Examples of cyber-attacks through the supply chain include the Stuxnet attack (Nourian and Madnick 2015) and the TJX data breach incident (Salim and Madnick 2016).

To help the industrial sectors secure the supply chain, the National Institute of Standards and Technology (NIST) further identified six 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. Looking specifically at the IT supply chain, the following threats could

create serious cybersecurity risks for organizations, including public sector organizations (GAO 2012): (1) Installation of hardware or software containing malicious logic (2) Installation of counterfeit hardware or software (3) Failure or disruption in the production or distribution of critical products (4) Reliance on a malicious or unqualified service provider for the performance of technical services (5) Installation of hardware or software that contains unintentional vulnerabilities. Some examples of supply chain vulnerabilities which can be exploited to introduce these threats include "*acquisition of information technology products or parts from independent distributors, brokers, or the gray market", "lack of adequate testing for software updates and patches", "incomplete information on IT suppliers" and "Use of supply chain delivery and storage mechanism[s] that are not secure"* (GAO 2012).

On the other hand, with the booming of the global B2B e-commerce industry and social platforms, more and more organizations are adopting modern ICT technologies, like cloud-based platforms, digital payments, mobile technology, IoT technology and advanced data analytics, to reconstruct their global supply chains. These cross-border trades on digital services and goods now have the ability to reach customers globally without the need for extensive physical presence (OECD 2015). The trading relies on open digital channels and differences in policy measures across markets pose significant challenges for digital supply chain management (Schmidtlein et al. 2017). In this digital supply chain context (Palmisano 2016)[17], the business architecture and the organizational boundaries have changed. Threats can come from both within and outside of an organization. Vendors, customers and partners are connected with each other in the digital supply chain. In addition to economic and social opportunities, the global digital network also creates new risks from online fraud, abuse, crime, and security threats. These risks demand that individuals, organizations and nations protect themselves in cyberspace (Donilon et al. 2016). For example, assets such as trade secrets and other intellectual property must be protected from cyber-attacks like unauthorized access, viruses or other malicious code, and phishing attempts (CREATE.org 2016).

2.5 Organizational Strategic Response to Institutional Pressures

According to Oliver's suggestions (Oliver 1991), organizational actors' strategic responses to institutional pressures vary from "passivity to increasing active resistance: acquiescence, compromise, avoidance, defiance and manipulation":

1) **Acquiesce:** refers to organizational assent to institutional pressures, commonly in three forms: Habit, Imitation, and Compliance. Habit refers to "unconscious or blind adherence to preconscious or taken-for-granted rules or values"; Imitation refers to "either conscious or unconscious mimicry of institutional models, including, for example, the imitation of successful organizations and the acceptance of advice from consulting firms or professional associations"; Compliance, by comparison, is defined here as "conscious obedience to or incorporation of values, norms, or institutional requirements".

2) **Compromise**: If "confronted with conflicting institutional demands or with inconsistencies between institutional expectations and internal organizational objectives related to efficiency or

[17] A Digital Supply Chain (DSC) is a customer-centric platform model that captures and maximizes utilization of real-time data coming from a variety of sources. More and more data, including the high value confidential business information, are collected, stored and shared with third-party companies, increasing the importance of cybersecurity measures for digital supply chain management.

autonomy… organizations may attempt to balance, pacify, or bargain with external constituents". Balancing tactics refers to the accommodation of multiple constituent demands in response to institutional pressures and expectations. Pacifying tactics also constitute partial conformity with the expectations of one or more constituents. Bargaining tactics involve the effort of the organization to exact some concessions from an external constituent in its demands or expectations.

3) **Avoid**: refers to the organizational attempt to preclude the necessity of conformity. It includes concealing nonconformity, buffering from institutional pressures, or escaping from institutional rules or expectations. Concealment tactics involve disguising nonconformity behind a façade of acquiescence. Buffering refers to an organization's attempt to reduce the extent to which it is externally inspected, scrutinized, or evaluated by partially detaching or decoupling its technical activities from external contact. Escape is when an organization may exit the domain within which pressure is exerted or significantly alter its own goals, activities, or domain to avoid the necessity of conformity altogether.

4) **Defy**: is a more active form of resistance, including dismissal, challenge and attack. Dismissing, or ignoring institutional rules and values, is a strategic option that organizations are more likely to exercise when the potential for external enforcement of institutional rules is perceived to be low or when internal objectives diverge or conflict very dramatically with institutional values or requirements. Challenge is a more active departure from rules, norms, or expectations than dismissal. Organizations that challenge institutional pressures go on the offensive in defiance of these pressures and may indeed make a virtue of their insurrection. Attack is distinguishable from challenge as a tactic of defiance by the intensity and aggressiveness of the organization's active departure from institutional pressures and expectations.

5) **Manipulate**: refers to the most active response to these pressures. It is intended to actively change or exert power over the content of the expectations themselves or the sources that seek to express or enforce them. Manipulation can be defined as the purposeful and opportunistic attempt to co-opt, influence or control institutional pressures and evaluations. Co-opting refers to importing influential constituents to neutralize institutional opposition and enhance legitimacy. Influence is more generally directed toward institutionalized values and beliefs or definitions and criteria of acceptable practices or performance. Control means dominating institutional constituents and processes when institutional expectations are incipient, localized or weakly promoted.

Although normally organizations are less powerful and must accede to governmental policies or regulations, they can also have the ability to influence policies (Binderkrantz, Christiansen, and Pedersen 2014; Boddewyn and Brewer 1994), especially in consultations regarding business regulations.

3 Relations between International Trade and Cybersecurity Concern

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

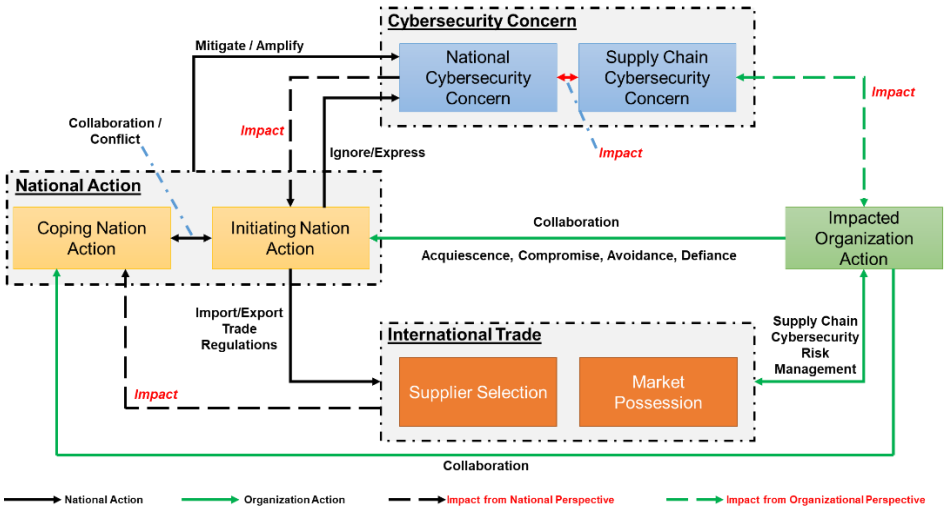


Fig 1: The concept model for the impact between cybersecurity concern and international trade

1) **Cybersecurity concern is rising**: With the wide adoption of information and communications technologies (ICTs) in digital society, (including critical infrastructures that are crucial for military security, economic security and cultural security) cybersecurity has increasingly been invoked as an aspect of "national security." Governments now focus on how to "protect the society as a whole" (OECD 2012) from cyber threat. On 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. The cyber risk from digital and physical supply chains, including increasing cyber attack vectors and data breaches, further deepens 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, and Harrington 2012). The widely accepted public-private partnership arrangements where "*private organizations deliver long-term infrastructure projects and then operate and manage them following an output specification from the public sector purchaser*"(Hodge 2007; Zheng, Roehrich, and Lewis 2008) further blur the boundary between the public and private supply chain. Cybersecurity concerns about the supply chain for critical public infrastructure will increase national cybersecurity concern. Conversely, concern about national cybersecurity impacts perception about supply chain risk, especially supply chain cybersecurity.

2) **Nations[18] take actions for national cybersecurity concern**. To protect nations, organizations and individuals from potential cyber attacks, countries can intervene in cyberspace through cybersecurity policies and regulations that 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. The "National Security Exception" principle in the international trade context allows governments to take action when necessary in cases of "essential

[18] 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.

security interest." This important principle allows for policies which influence international trade, including the import and export of IT goods and services. As we focus on the impact of cybersecurity on international trade, we only consider the nation's actions which will shape international trade relations. In other words, only the actions which can impact global supply chains, including the physical and digital supply chains, will be considered here. These actions include 1) ignoring or expressing concerns without policy implementation, 2) developing import/export trade barriers which directly shape the international trade environment, and 3) collaborating with other nations to mitigate cybersecurity concern or conflict with others which amplifies the concerns. We will discuss more details in the following section.

Note that these actions can arise from an initiating nation, stemming from national cybersecurity concerns, or be enacted by a coping nation as a reaction to the initiating nation's action.

3) **Organizations take 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 executive's agenda. To secure the physical and digital supply chain, organizations need to manage key cyber supply chain risks (NIST 2015). To enhance the cybersecurity for the global supply chain, some organizations may try to ***collaborate*** with their governments to initiate policies to impact international trade. On the other hand, 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. This acceptance is referred to as "***acquiescence,***" especially when these policies are related to national security concerns. For some specific cases, an organization will negotiate with the initiating nation for the cybersecurity regulations, tying to exact some concessions for both sides. This is named "***compromise.***" Sometimes, an 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. This company is engaging in "***avoidance.***" Bundled with avoidance, if an organization challenges or attacks the cybersecurity regulations from the initiating nations, they are acting in "***defiance.***" 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. This is named "***collaboration***"[19].

4) **The international trade environment is reshaped**: National actions, both the initiating and coping actions, together with the organizational actions, reshape the international trade environment. These actions will change the risk and cost for the organization's global supply chain. Consequently, these actions will also impact the organization's decision about supplier selection, where to purchase the goods and services, and market possession, where to sell the products and services. On the other hand, the international trade environment will impact the international relations among different nations, which can influence the national actions when facing national cybersecurity concern. In addition, the strategic importance of the supplier and market within an organizational global supply chain will impact organizational decisions about supply chain cyber risk management, even when facing the institutional

19 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.

pressures from nations. For example, an organization may have a higher potential to choose the "avoidance" action 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.

Using this conceptual model to understand the relations between cybersecurity concern and international trade, we can observe that: *cybersecurity concern will impact national and organizational action, both through policy implementation and supply chain cyber risk management, which consequently reshape the international trade environment. Conversely, the international trade environment will impact national actions and organizational decisions when these entities consider cybersecurity concern*. To dig deep into this framework, in the following section, we will unfold each component and develop a taxonomy to provide in-depth understand about these mechanisms using real-world cases.

3.1 Cybersecurity Concerns

We can understand the cybersecurity concerns which impact international trade from two different perspectives: national cybersecurity concerns and supply chain cybersecurity concern.

3.1.1 National Cyber Security Concern

For the national cyber security perspective, we use the four categories from [Kshetri 2016] as they are most clearly defined. As shown in Table 1, we further detail each category to include different perspectives and then list some examples to clarify:

Table 1: The taxonomy for national cyber security concerns

Cybersecurity Concern			Definition	Example
National Cyber Security	**Military Security**	**Defensive Capability**	Concerns about the potential to increase the cyber attack vectors and harm the cyber defensive capability	In 2017, the U.S. army halts use of Chinese Made Drones from DJI due to the cyber vulnerabilities in the products
		Offensive Capability	Concerns about the potential to impact the cyber offensive capability	In 2014, the U.S. BIS announced that the Wind River Systems Inc. would pay a civil penalty for exporting operating software without licenses.
		Cyber Terrorism	Concerns about the terrorists using cyberspace for attack	In 2015, the U.S. government charged a hacker with stealing data on military and other government personnel and passing them to ISIS.
	Political Security	**Political Espionage**	Concerns about using of cyberspace to obtain political and military information	In 2017, the U.S. General Services Administration (GSA) removed Kaspersky Labs from its list of approved vendors over fears the Russian-owned cybersecurity company represents an undue risk to U.S. interests.

		Political Stability	Concerns about using of cyberspace to impact the government's political authority and governing capability	In 2010, protesters used social media to organize demonstrations, both pro- and anti-governmental, during the Arab Spring
	Economic Security	**Economic Espionage**	Concerns about using of cyberspace to steal economic related information which will impact the trade, production and finance.	In 2017, U.S. President Donald Trump directed the U.S. trade representative (USTR) to examine China's so-called intellectual property practices, despite worries about potential harms to China-US trade ties
		Economic Stability	Concerns about using of cyberspace to impact the economic stability in a country	In 2015, a Russian trading system was attacked by the Trojan Corkow, resulting in trades of more than $400 million in 14 minutes and a high volatility in exchange rate of Dollar/Ruble
	Culture Security	**Public Morals**	Concerns about using cyberspace to impact the sustainability of collective identities and value	In 2017, Google and Facebook admitted that Russians paid tens of thousands of dollars to run online advertisements before the 2016 U.S. election and called for banning foreign governments from posting election advertisements due to the growing fears that the Russian government spread “fake news” aimed at misleading voters

1) **Military security concerns** refers to the concern that cyberspace will impact the military’s cyber capability, not only the defensive but also the offensive capability.

- **Defensive Capability**: The possibility of introducing a larger cyber attack vector to the military system will bring concern about defensive capabilities. The typical example here is, a U.S. Army memo from August 2017 that required service members to "*cease all use, uninstall all DJI applications, remove all batteries/storage media and secure equipment for follow-on direction*"[20] because of the concerns about the potential vulnerabilities in the DJI drone products which can put the military’s operation in risk. In addition, control over the improvement of an opponent's cyber offensive capability is also important for national military security. For example, the Chinese acquisitions of the German semiconductor company Aixtron was blocked in 2016 because Aixtron had a subsidiary in the United States and its technology had potential “military applications,” which included the super computer and smart phones.
- **Offensive Capability**: From a different perspective, countries work to improve their military cyber offensive capability as well as restrict the opponent’s defensive capability. One way to improve the offensive capability is to introduce cyber attack vectors into the targets’ cyberspace. State actors can work with private sector companies in their respective countries to incorporate various forms of vulnerabilities, like built-in backdoors or spyware in computer-based products that are then exported around the world. Furthermore, controlling the export of advanced cyber defensive technology like strong encryption is considered a manifestation of this concern. In 2014, the Intel subsidiary Wind River

[20] Please refer to this link for details: https://www.reuters.com/article/usa-army-drones-idUSL1N1KQ1KC

Systems Inc. was fined a civil penalty of $750,000 for exporting approximately $3 million worth of software containing encryption to government end-users in China, Hong Kong, Russia, Israel, South Africa and South Korea, and to Entity List end-users in China without obtaining the export licenses[21]. Another interesting example is when Stanford University required that "*Stanford researchers MUST email the University Export Control Officer (ECO) with the internet location or URL of the EAR-controlled strong encryption software before making the software publicly available regardless of medium. Only after receiving an email confirmation from the ECO may the researcher upload the code onto a publicly available website*"[22].

- **Cyber Terrorism:** Besides the state-actor in cyberspace, there is also some concern about cyber terrorism[23] defined by the FBI (Singer, P.w, Friedman 2014) as a "*premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents*." In October 2015 the U.S. reached a milestone for fighting cyberterrorism. For the first time, the government charged a hacker with stealing the data, including names, e-mail addresses, passwords, locations and phone numbers, of 1,351 U.S. military and other government personnel and passing it to members of ISIS with the intent to support them in arranging attacks against Western targets[24]. It is also believed that ISIS used social media such as Twitter, Facebook and YouTube to recruit new members through images and the streaming of violent online viral videos (Awan 2017).

2) The **political security** concern refers to the concern that cyberspace can be used to launch attacks to steal a government's secret information or to impact the government's political authority, governing capability and the capability of being recognized.

- **Political Espionage**: The typical manifestation of this is in concern about political espionage, referring to the practice of spying or of using spies, typically by governments, through cyberspace, to obtain political and military information. For example, during June and September, 2017, the U.S. Department of Defense (DoD) suspected that Kaspersky Lab products were suspected being used by the Russian government to carry out espionage practices[25]. Hence, the DoD removed Kaspersky Lab products from the next year's budget in July, and General Services Administration (GSA) removed Kaspersky Labs from its list of approved vendors in July. Following that, in August 2017, the U.S. FBI briefed the companies in the private sector on intelligence that Kaspersky Lab products are unacceptable threats to national security. Finally, in September 2017, the U.S. Senate voted to ban Kaspersky Lab software from government networks which would bar the use of Kaspersky Lab in civilian and military agencies that use government networks. This is reminiscent of Huawei's ban story from 2012 and 2013[26].
- **Political Stability:** Another manifestation of this is in concerns that cyberspace can be used

---

[21] https://www.law360.com/articles/596140/wind-river-case-may-signal-change-for-encryption-exports

[22] http://web.stanford.edu/group/export/encrypt_ear.html. Here we just use Stanford University as an example.

[23] Unique definitions of cyberterrorism don't exist, and different nations will emphasize different aspects of it. In this paper, we place it in the military category as the first cyberterrorism conviction is related to the military goal. However, it is intuitive that cyberterrorism will also impact political security and societal, socio-cultural or cultural security.

[24] http://resources.infosecinstitute.com/the-ferizi-case-the-first-man-charged-with-cyber-terrorism/#gref

[25] https://www.cyberscoop.com/kaspersky-banned-us-dod-ndaa-russian-influence/
https://www.scmagazine.com/gsa-removes-kaspersky-labs-from-its-approved-vendors-list/article/675052/
https://www.cyberscoop.com/fbi-kaspersky-private-sector-briefings-yarovaya-laws/
http://www.rawstory.com/2017/09/us-senate-votes-to-ban-kaspersky-lab-software-from-government-networks/

[26] We are going to discuss more detail about Huawei's ban story in Section 5.

to spread hate speech, fake news (Hine et al. 2016)[27], "terrorism, separatism and extremism"[28] or other information or misinformation, which will threaten political stability (Gechlik 2017). For example, social media played a significant role during the Arab Spring and protesters used social media to organize demonstrations (both pro- and anti-governmental), disseminate information about their activities, and raise local and global awareness of ongoing events[29]. Anonymous[30], a famous hacktivism group, attacked the governments of several countries including the US, U.K., Australia, the Netherlands, Spain, India and Turkey to express their political or social protests. On June 17, 2015, Anonymous claimed responsibility for Denial of Service attacks against Canadian government websites in protest of the passage of bill C-51—an anti-terror legislation that grants additional powers to Canadian intelligence agencies. One big story in 2016 and 2017 has been the subversion of the U.S. presidential election[31], from the self-confessed "mistake" Secretary Clinton made in setting up a private email server, to the hacking of the Democratic National Committee's servers and the leaking of Democratic campaign chair John Podesta's emails to WikiLeaks. Google and Facebook admitted that Russians paid for tens of thousands of dollars to run adverts online before the election and Google intended to extend the ban on proxies for foreign governments handing out election material to the online posts[32]. Since then, election hacking has become a global new normal, with evidence of its occurrence in Germany, Montenegro, France, the Netherlands, Russia and elsewhere. The Freedom House reported that the elections in at least 18 countries in 2016 were impacted by online manipulation and disinformation tactics (Kelly et al. 2017). Another example is that in March 2018, multiple media outlets broke news of Cambridge Analytica's business practices of collecting Facebook data and using "*prostitutes, bribery sting operations, and honey traps to discredit politicians on whom it conducted opposition research*"[33].

3) The **economic security concern** deals with trade, production and finance (Albert and Buzan 2011).

- **Economic Espionage:** The U.S. has repeatedly emphasized its interest in controlling and punishing cyber-attacks that involve economic espionage, especially when related to intellectual property theft. The U.S. Intellectual Property Enforcement Coordinator Danny Marti emphasized that "*Advancements in technology, increased mobility, rapid globalization, and the anonymous nature of the Internet create growing challenges in protecting trade secrets*"[34]. The Commission on the Theft of American Intellectual Property reports that the annual price from intellectual property theft is between $250 billion and $600 billion[35]. In September 2015, President Barack Obama met Chinese President Xi

[27] https://www.nature.com/news/shining-a-light-on-the-dark-corners-of-the-web-1.22128

[28] http://eurasiangroup.org/files/documents/conventions_eng/The_20Shanghai_20Convention.pdf

[29] How to govern the Internet is out of scope in this paper. However, the impact of the Arab Spring is still an arguable issue. For example, Some argues that "[Arab] spring has given way to a winter of economic stagnation and political violence that has plunged Syria, Libya and Yemen into bloody civil war, has led to widespread unrest in Egypt, Iraq and Bahrain, and threatens to destabilize Arab governments from Morocco to Saudi Arabia" (https://www.huffingtonpost.com/joseph-v-micallef/the-arab-spring-six-years_b_14461896.html) while some argues that "at least now that the "old" justifications to differentiate between people do not suffice anymore" (Doomen 2013).

[30] https://en.wikipedia.org/wiki/Anonymous_(group)

[31] The State and Local Election Cybersecurity Playbook, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2018, https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook#election

[32] http://www.telegraph.co.uk/news/2017/11/16/google-ban-foreign-governments-posting-online-election-adverts/

[33] https://en.wikipedia.org/wiki/Cambridge_Analytica

[34] https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html#endnote-9

[35] https://lunarline.com/blog/2017/03/the-cost-of-hacking-intellectual-property-theft/

Jinping and signed an agreement on cyber espionage, pledging to cease state-backed hacking of private-sector firms in each other's country. A similar agreement was reached between China and the U.K. in October. In November, the G20 nations agreed to a set of cybersecurity norms that include a prohibition of commercial espionage[36]. Though it is reported that intellectual property related cyber attacks were significantly reduced after that, in August 2017, U.S. President Trump again instructed the office of the United States Trade Representative to consider an investigation into China's sustained and widespread attacks on America's intellectual property, which indicates that intellectual property theft remains an important concern in cyberspace.

- **Economic Stability:** From another perspective, developing countries have different viewpoints regarding cyber economic security threats. Their main concern centers on economic stability (Nir Kshetri 2016). The Draft to the UN General Assembly[37] on the International Code of Conduct for Information Security was submitted by six founded members of the SCO in January 2015 and emphasized "*Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability*;" and "*To endeavour to ensure the supply chain security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and communications networks to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security*". Naturally, financial stability is an important aspect of economic security. Cybersecurity incidents can threaten financial stability due to the lack of substitutability, loss of confidence and loss of data integrity (OFR 2017). For example, in 2015, a Russian trading system was attacked by the Trojan Corkow, resulting in trades of more than $400 million in 14 minutes with a high volatility in exchange rate of Dollar/Ruble (Kopp, Kaffenberger, and Wilson 2017). Furthermore, a cyber incident which creates large shocks to one financial system can propagate shocks through connected banks, making the highly interconnected financial networks even more fragile (Acemoglu, Ozdaglar, and Tahbaz-Salehi 2015). The CPMI-IOSCO Working Group on Cyber Resilience (WGCR) outlines five primary risk management categories and three overarching components that should be factored in across financial market infrastructures to guarantee financial stability (OICU-IOSCO 2016).

4) The **cultural security concern** involves the sustainability of collective identities and value, or so-called "public order" and "public morals," which is especially emphasized by many developing nations. For example, China's stated goal of creating a healthy cyberspace, which is defined as "porn-free" and "crime-free," reflects an emphasis on cultural security. The "Great Firewall" in China is to ensure that all online content that is circulated within China is in line with important public values, particularly pertaining to maintaining public order and protecting the nation's public morals. "*Countries including Singapore, Lebanon and Turkey ban adult entertainment websites, while Germany bans the*

[36] http://www.washingtonexaminer.com/g20-leaders-get-tough-on-cyber-espionage/article/2576605

[37] https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

sale of Nazi memorabilia on e-commerce websites. Countries such as Iran, Vietnam, and China impose restrictions on political information that is circulated online for the purposes of maintaining public order" (Mitchell and Hepburn 2016). In 2017, China and Russia moved to block virtual private network (VPN) services, intending to further restrict cyberspace.

3.1.2 Supply Chain Cybersecurity Concern

Supply chain risk management (SCRM) is a critical organizational function for both private sector and public-sector organizations, beginning with the sourcing of products and services and extending to the end user. Each organization can both be the "buyer," which is the "*downstream people or organization that consume a given product or service from an organization*", and the "supplier" which is the "*upstream product and service providers that are used for an organization's internal purposes or integrated into the products or services provided to the Buyer.*"(NIST 2018) Hence, from the buyer and supplier perspective, the supply chain cybersecurity concern can be separated into two parts:

Table 2: The cybersecurity concerns from the physical and digital supply chain perspectives

Cybersecurity Concern		Definition	Example
Supply Chain Cyber Security	Supply Chain Cyber Attack Surface Concern	Supply chain can become a vector for attackers to introduce cyber threat into the organization	For the Stuxnet attack to Iran nuclear facility, the U.S. identified NEDA as Iran's leading expert in Siemens Step7 software used throughout Iran's nuclear program and then targeted industrial control systems equipment that NEDA had ordered from suppliers overseas
	Supply Chain Digital Asset Protection Concern	Concern about how to protect the organizational digital assets across the supply chain	The European Union restricts the flow of sophisticated outsourcing business to India by designating it as NOT a data secure country.

1) The **Supply Chain Cyber Attack Surface Concern** refers to the concern that the supply chain can become a vector for attackers to introduce cyber threat into the organization, using supply chain management vulnerability. According the NIST Cybersecurity Framework, the cyber SCRM is to "*identify, assess, and mitigate products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain*"[38]. One famous example of attackers exploiting supply chain vulnerability is the Stuxnet attack to the Iran nuclear facility. As early as 2004, U.S. intelligence agencies identified an Iranian company, NEDA industrial Group, as Iran's leading expert in Siemens Step7 software used throughout Iran's nuclear program. In 2008, the U.S. targeted industrial control systems equipment that NEDA had ordered from suppliers overseas. Malware including Stuxnet was installed on this equipment and then

[38] NIST Cybersecurity Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, https://doi.org/10.6028/NIST.SP.800-161

shipped to Iran, resulting in the destruction of some centrifuges for Iran's nuclear facility[39].

2) The **Supply Chain Digital Asset Protection Concern** refers to the concern about how to protect organizational digital assets across the supply chain. It is especially focused on the protection of critical data like trade secrets or intellectual property. In a digital society, data plays a critical role in many perspectives like reducing transaction costs and enhancing real time resource management. Digital data adds value not only to the service and e-commerce industries but also to manufacturing (J. Meltzer 2014). Actually, 75% of the data driven added value goes to the traditional manufacturing sectors while the internet data flows contribute at least 10% to the global GDP (Manyika et al. 2016). However, data breach incidents are increasing globally over recent years (in both developing and developed countries) (Verizon 2017), which further raises the concern about safeguarding data privacy and security (Kuner 2011)[40] for organizations. For the international supply chain, this is even more critical, as some suppliers and buyers may be in regions where cybersecurity practice is poor. These entities become the "weak link" for the whole supply chain. One interesting case is that the EU requires a "data secure" status for a third country in order to enable personal data transfer from "*the 28 EU countries and three EEA member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary*"[41]. A "data secure" status means that the country "*ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.*"

3.2 National Actions for National Cybersecurity Concern

Considering these concerns, many countries impose policies and regulations with different "specific governmental levers and information assurance principles" (Klimburg 2012). As we focus on the cybersecurity impact on international trade, we only consider actions which will shape international trade relations. In other words, only the actions which can impact global supply chains, including the physical and digital supply chains, will be considered here. In addition, the impacted nations may react to the initiatives from the initiating nations. The actions discussed below are options for the initiating, and the coping nations. Hence, from the governmental lever perspective, we group the national actions into the following categories:

3.2.1 National Action: Ignore or Express Concerns

As shown in Table 2-1, in the case of some specific cyber incidents, governments can choose to ignore the incident and accept the potential risk. For example, in 2004, the German Federal Intelligence Service (BND)[42] discovered that the then-US-based company NetBotz[43] sold security cameras with a built-in backdoor which sent videos to the US-Military's servers. However, the BND hid this information until 2015 when the Attorney-Generals for the German counter-espionage unit's Federal

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

[40] Digital protectionism could also pay a critical role in data cross-border transfer restrictions.

[41] Please refer to the following link to check the 11 countries recognized as data secure. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[42] The BND, Germany's only overseas intelligence service, acts as an early warning system to alert the German government about 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, illegal transfer of technology, organized crime, weapons and drug trafficking, money laundering, illegal migration and information warfare.

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

Office for the Protection of the Constitution (BfV)[44] found out independently. Finally, in 2016, journalists of the German TV-show "Fakt" reported this issue, 12 years later[45].

Unlike ignoring the potential risks, sometimes governments will express concern or offer recommendations but without the mandate to warn citizens about potential cybersecurity threats, or respond to the related policies or regulations from the other nations. It is easy to identify many recent examples: In December 2016, over 18 privacy groups filed complaints with both the U.S. Federal Trade Commission and the European Union alleging that Genesis Toys and its tech partner

Table 2-1: The nation actions due to the cybersecurity concern (part-1).

Category		Definition	Example
Ignore or Express Concerns	Ignore	Ignore and accept the cybersecurity concerns	German Federal Intelligence Service (BND) discovered that the then-US-based company NetBotz sold security cameras with a built-in backdoor that sends the videos to servers of the US-Military in 2004 but hid this information for 12 years
	Express Concerns	Express the concerns about the cybersecurity risk or the related policies and regulations from other nations	In August, 2017, the FBI briefed the private sector companies on intelligence claiming that the Kaspersky Lab products are an unacceptable threat
	Identified as Trade Barrier	Officially identify the related policies and regulations as a barrier to trade	the United States Trade Representative ('USTR') lists the data localization regulation as a trade barrier in the 2017 National Trade Estimate Report on Foreign Trade Barriers

Nuance are violating deceptive practices and privacy laws (including COPPA) through the way that certain toys record kids' voices[46]. In August, 2017, a senior Indian IT ministry official expressed concern about the UC browser from Alibaba: "*There have been complaints against UC Browser that it sends mobile data of its users in India to server in China. There are complaints that even if a user has uninstalled it or cleaned browsing data, the browser retains control of DNS of user's device*"[47]. In 2017, The FBI briefed private sector companies on intelligence which claimed that Kaspersky Lab products are unacceptable threats[48]. There is no doubt that expressing such concerns about the cybersecurity risk of imported products or services could have some impact on international trade. Even without mandates, it can still impact the consumers' cybersecurity adoption behavior (Chen and Zahedi 2016; Riek, Bohme,

[44] The domestic secret service counterparts of the BND in German

[45] https://www.democraticunderground.com/10141582901

[46] https://www.engadget.com/2016/12/06/internet-connected-toys-accused-of-spying-on-kids/

[47] http://www.hindustantimes.com/business-news/alibaba-s-uc-browser-under-govt-scanner-over-mobile-data-leaks-of-indian -users/story-yHWChAGnaX1VKEzBbFDoUM.html

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

and Moore 2016; Venkatesh, Thong, and 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 rising cybersecurity concerns about Kaspersky Lab's products in the U.S.[49] Furthermore, this can impact policy makers' perception, resulting in further actions. For example, for the smart toys, Germany's Federal Network Agency finally forbade illicit radio transmission equipment in toys and prohibited the selling of the smart toy "My Friend Cayla" in February, 2017[50].

Another action here is that some governments will list cybersecurity-related policy as a trade barrier. For example, though there are still many discussions about data localization regulations, the United States Trade Representative ('USTR') lists it as a trade barrier for the U.S. in the 2017 National Trade Estimate Report on Foreign Trade Barriers (USTR 2017). During the WTO Technical Barriers to Trade (TBT) Committee on June 2017[51], members like the European Union, the United States, Japan, Canada and Australia expressed concerns about many of China's policies, including "secure and controllable" requirements for ICT products used in the aviation sector, cyber security guidelines for internet-connected vehicles, encryption requirements for ICT products, etc.

3.2.2 National Action: Trade Regulation

Besides expressing concerns, some nations will take actions to implement trade policies or regulations which will directly impact international trade. Note that these actions can be initiatives for cybersecurity concerns from initiating nations, or used by the coping nations as the response to initiating nations. Following the categories of the non-tariff measures from the United Nations Conference on Trade and Development (UNCTAD) [UNCTAD 2012], we can identify actions which are related to the cybersecurity domain, as shown in Table 2.2 (a) and Table 2.2 (b):

Table 2.2 (a): The nation actions due to the cybersecurity concern (part-2).

Category			Definition	Example
Import-Trade-Barriers	Technical measures	Prohibition, Authorization, or Registration requirement	Imports are prohibited; or the importer should receive authorization, permits or approval; or importers should be registered in order to import certain products.	The Indian government required mobile operators not to import any network equipment manufactured by Chinese vendors such as Huawei and ZTE in 2010
		Conformity assessment requirement	Requirement for product registration, to be tested against a given regulation, certification and inspection	Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, was established in early 2014 on the recommendation of the U.K. National Security Adviser to oversee and ensure the independence, competence and overall effectiveness of HCSEC and to test the

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

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

[51] https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm

				cybersecurity of communication devices provided by Huawei to U.K.
			Requirement for information traceability, like the origin of materials and parts, processing history, and distribution and location of products after delivery	/[52]
	Price-control measures	Additional taxes and charges levied on imports that have or don't have internal equivalents	Additional charges or taxes like Tax on foreign exchange transactions, Import licence fee, Taxes and charges for sensitive product categories	OECD reports the value-added tax (VAT) for cross-boarder business-to-consumer transactions in 2015; Effective 1 January 2017, the new Russian value-added tax (VAT) rules for electronic services (e-services) came into force.
	Finance measures		Regulate the access to and cost of foreign exchange for imports and define the terms of payment, like advance payment, multiple exchange rates, official foreign exchange allocation, terms of payment, etc.	For the Internet-enabled Payment Services, China issued regulations for non-bank suppliers of online payment services in 2010. As of June 2014, only 2 out of over 200 licenses were issued to foreign-invested suppliers with limited services.
	Trade-Related investment measures	Local content measures	Requirements to purchase or use certain minimum levels or types of domestically produced or sourced products, or restrictions on the purchase or use of imported products based on the volume or value of exports of local products	The Argentine Media Law, enacted in 2009 and amended in 2015, requires 50 percent of the news and 30 percent of the music that is broadcast on the radio be of Argentine origin. In the case of private television operators, at least 60 percent of broadcast content must be of Argentine origin. Of that 60 percent, 30 percent must be local news and 10 to 30 percent must be local independent content.

[52] Note that we don't identify an example for the measure "Requirement for information traceability, like the origin of materials and parts, processing history, and distribution and location of products after delivery." However, considering the rising concern about supply chain cybersecurity risk, it is possible that in the near future, we will see some related measures proposed by some governments.

		Foreign Direct Investment Barriers	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	Since 2013, the Committee on Foreign Investment in the United States expanded its review process to apply more oversight to so-called non-notified transactions for the acquisitions related to the "critical technology companies": the Chinese acquisitions of the German semiconductor company Aixtron is blocked in 2016; Huawei voluntarily divested its assets in 3Leaf, a U.S. technology firm in 2011.
	Restrictions on post-sales / digital services		Restricting producers of exported goods to provide post-sales or digital service in the importing country	Data localization regulations by many countries, like Australia, Canada, EU, India, China, Russia, U.S., Vietnam etc.
	Government Procurement Restrictions		Controlling the purchase of goods by government agencies, generally by preferring national providers	The U.S. General Service Administration removed Kaspersky Lab from the list of approved vendors in July 2017.
	Intellectual Property		Requirements related to intellectual property rights in trade	The Chinese government has adopted new regulations requiring companies that sell computer equipment to Chinese banks to turn over secret source code in January 2015.

1) **Import-related Trade Barriers** refer to the measures impacting imports, including technical measures, price-control measures, finance measures, trade-related investment measures, restrictions on post-sales or digital services, government procurement restrictions and intellectual property restrictions. The technical measures are the most common actions related to cybersecurity:

- One typical measure is to set "**prohibition, authorization, or registration requirements**" which could prohibit certain imports, or require the importer to receive authorization, permits or approval, or to register with the government agency. For example, in 2010, the government of India barred mobile operators from importing any network equipment manufactured by Chinese vendors such as Huawei and ZTE, due to concern that the adoption of such equipment could create cybersecurity risk to critical infrastructure[53].
- Another measure might require the product to **go through specific testing, certify the security assertion, or to go through some inspection**. For example, Huawei opened the Cyber Security Evaluation Centre (HCSEC) in the U.K. in 2010, to respond to concerns about the cybersecurity of their products. The HCSEC is considered a key part of Huawei's end-to-end global security assurance system. To respond to the concern raised by the Intelligence and

[53] http://www.newsweek.com/huawei-way-108201

Security Committee (ISC) in 2013, HCSEC further established the HCSEC oversight board with the U.K. National Service Adviser to oversee and ensure "the independence, competence and overall effectiveness of HCSEC"[54]. To improve the cybersecurity situation in critical infrastructure, many governments have established certain cybersecurity standards. For example, in the U.S., the cloud service for the federal government needs to go through a process and certification known as FedRAMP[55] to meet the federal cloud security standards. China proposed the Regulation on Classified Protection of Information Security to define the importance of certain infrastructures and the protections required for different levels[56].

- The third measure is **the requirement for information traceability**. This requirement concerns the origin of materials and parts, processing history, and distribution and location of products after delivery. In other words, the importer needs to offer "log-level" detailed information on the supply chain for the products. Right now, we have not found any examples of such requirements related specifically to cybersecurity. However, considering the rising concern of cybersecurity risk from the supply chain, it is very possible that soon, some governments could propose regulations falling into this category. In fact, we can see similar regulations in other domains. One regulation states, "*before placing imported cosmetic products on the EU market, the person responsible must indicate to the competent authority of the Member State where the products were initially imported, the address of the manufacturer or the address of the importer*" (UNCTAD 2012).

For 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 rapid growth of the digital economy has raised challenges for the current international tax rules. The cross-border trade in goods, services and intangibles also creates challenges for the value-added tax (VAT) system. Following the OECD International VAT/GST guidelines (OECD 2015), the EU, South Korea, Japan, India, the U.K. and Russia introduced the digital service VAT while countries like Australia and New Zealand will introduce foreign e-services VAT charges soon[57]. Note that this foreign e-services VAT is not directly related to cybersecurity concerns, but an action to govern the cross-border trade in cyberspace.

Finance measures refers to the regulations which govern access to and cost of foreign exchange for imports and which define the terms of payment. One of the most-criticized restrictions is the restriction on Internet-enabled payment services in China. As reported by USTR 2017, China issued regulations for non-bank suppliers of online payment services in 2010 while as of June 2014, only 2 out of over 200 licenses were issued to foreign-invested suppliers with requirements to localize data and facilities in China (USTR 2017).

Trade-related investment measures refers to regulations on foreign investment, both direct and indirect scenarios. A typical measure related to cyberspace is the local content requirement. This policy requires foreign providers to purchase or use certain minimum levels or types of domestically produced

---

[54] https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2015

[55] https://www.fedramp.gov/about-us/about/.

[56] Ahrens, Nathaniel. "National Security and China's information security standards" CSIS Hills Program on Governance. (2012). https://csis.org/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf

[57] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-beps-action-1-vat-on- business-to-customers-digital-services-implementation-matrix.pdf

or sourced products. It may also restrict the purchase or use of imported products based on the volume or value of exports of local products. For example, the Argentine Media Law, enacted in 2009 and amended in 2015, requires 50 percent of the news and 30 percent of the music that is broadcast on the radio be of Argentine origin. In the case of private television operators, at least 60 percent of broadcast content must be of Argentine origin. Of that 60 percent, 30 percent must be local news and 10 to 30 percent must be local independent content. Intuitively, these media regulations relate to cyber security culture. China's stated goal of creating a healthy cyberspace, which is defined as "porn-free" and "crime-free," reflects an emphasis on cultural security. The "Great Firewall" in China is to ensure that all online content circulated within China is in line with important public values, particularly pertaining to maintaining public order and protecting the nation's public morals. Another common national cybersecurity measure, is the foreign direct investment (FDI) barrier, which places limitations on foreign equity participation and on access to foreign government-funded research and development programs. It also enacts local content requirements, technology transfer requirements and export performance requirements, and restricts repatriation of earnings, capital, fees and royalties. Since 2013, the Committee on Foreign Investment in the United States has expanded its review process to apply more oversight to so-called non-notified transactions for acquisitions related to "critical technology companies." For example, the Chinese acquisition of the German semiconductor company Aixtron was blocked in 2016 because Aixtron has a subsidiary in the United States and its technology has potential "military applications," including the super computer and smart phone.

Due to the growth of the digital economy, we can observe growing restrictions in cyberspace on post-sales and digital services, preventing producers of exported goods from providing post-sales or digital service in the importing country. The most relevant regulations are data localization regulations, enacted by many countries like Australia, Canada, EU, India, China, Russia, Vietnam etc[58]. For example, Australia proposed the "*Personally Controlled Electronic Health Record Provision*" to restrict the exportation of any personally identifiable health information, while China issued "*Population and Healthcare Information Management Measures*" to prohibit the overseas transfer of health and medical information. Russia proposed the Federal Law 242-FZ requiring all data collected on Russia citizens be stored within Russia. Vietnam and Indonesia view data sovereignty as a matter of national security and protection against foreign surveillance. Even though U.S. agencies list data localization regulation as a foreign trade barrier and question the effectiveness of such restrictions, the "*DoD Interim Rule on Network Penetration Reporting and Contracting for Cloud Services*" also requires that all cloud computing service providers that work for the DoD store DoD data within U.S. Territories.

Government procurement restrictions are the most common and powerful actions from the government. There are several reasons for this. The policies are easier to enact and processes than other kinds of restrictions. Also the large government contracts can help define standards that impact the private sector. Additionally, the political pressure can prorogate to international trade through global supply chains. For example, the U.S. banned the use of Kaspersky Lab products in the government and military systems in 2017. Following this, Best Buy pulled Kaspersky Lab's cybersecurity products from its shelves and websites in September 2017. The FBI considers Kaspersky Lab's products unacceptable

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

for private sector companies participating in intelligence. It is easy to imagine that these private sector companies will remove Kaspersky Lab's products from their environments if they want to get contracts from the FBI. Similarly, 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 Chinese government procurement list[59] in 2015 due to cybersecurity concerns.

The last category of measures related to import trade barriers are those that deal with intellectual property. Often, the initiating nation's specific testing and certification requirements can be considered by the coping nation as a potential violation of intellectual property law. For example, the Chinese government proposed regulation requiring that companies selling computer equipment to Chinese banks turn over their proprietary source code in January 2015. 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 requirement for intellectual property disclosure raises intense disputes among nations. Such provisions are considered import trade barriers, which will definitely impact international trade.

On one hand, intellectual property theft is always a concern for developed countries like the U.S. In August 2017, U.S. President Trump instructed the office of the United States Trade Representative to consider an investigation into China's sustained and widespread attacks on America's intellectual property. 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*."[60]

On the other hand, some developing nations fear a lack of access to intellectual property. The EU, prevents any high-end outsourced business from flowing into India, as India is not considered as a data secure country. Furthermore, because of the lack of data-secure status, India doesn't have access to intellectual property or other sensitive information such as patient records, which will limit the growth of India's outsourcing sector[61].

2.2) Export-related Trade Barriers refers to measures impacting export, including export-license, -quota, -prohibition and other quantitative restrictions, export technical measures, and export subsidies. As shown in Table 2.2 (b), the export trade barriers are basically proposed by the developed nations.

Table 2.2 (b): The nation actions due to the cybersecurity concern (part-2).

Category	Definition	Example

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

[60] As of the time of this draft version in August 28, the details of the agreement aren't fully known. This message is from the U.S. press. Please check more detail here: https://globalnews.ca/news/4415386/nafta-intellectual-property-laws/

[61] http://preemploymentdirectory.com/india-seeks-data-secure-nation-status-more-hi-end-business-from-european- union/#axzz4xynAppPi

Export-Trade-Barrier	**Export-license, -quota, -prohibition, certification, and other quantitative restrictions**	**Export prohibition, quotas limitation, licensing or permit requirements, or registration requirements**	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.
		The technical specification of products and conformity assessment, like inspection or certification requirement	On 2014, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced that Intel subsidiary Wind River Systems Inc. would pay a civil penalty of $750,000 to settle 55 export control violations concerning operating software controlled under ECCN 5D002. Between January 2008 and September 2011, Wind River exported approximately $3 million worth of software to government end-users in China, Hong Kong, Russia, Israel, South Africa and South Korea, and to Entity List end-users in China. Wind River failed to obtain licenses for any of the exports as required by the Export Administration Regulations
	Export subsidies	**Financial contribution by a government or public body, or via government entrustment or direction of a private body, or income or price support**	The then-US-based company NetBotz sold extremely cheap security-cameras to government-departments and to corporations operating with high-tech and military hardware.

Export-license, -quota, -prohibition, -certification and other quantitative restrictions can control export numbers or even prohibit certain exports. The most significant export measures are determined by the Wassenaar Arrangement, a 41-country international forum that seeks consensus among its members on dual-use export controls. The forum adopted new controls on "intrusion software" and "carrier class network surveillance tools" in 2013. The Wassenaar Arrangement is a multilateral export control forum for dual use goods and technology. Its 41 countries must come to a consensus on any proposed export controls. Then, each country implements these controls under their national rules with a significant level of discretion. For example, in 2015, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) published proposed amendments to the Export Administration Regulations (EAR). These amendments sought to implement stricter controls on certain cyber-security related items, including intrusion software and network communications surveillance systems, along with related systems, equipment, software, components, and technology[62]. The proposed rules would further increase the list of controlled items and require a license for the export, re-export, or transfer of these items to all

[62] http://mil-embedded.com/articles/cybersecurity-export-not-now-the-u-s/

destinations except Canada[63]. Due to this regulation, Hewlett-Packard (HP) and its Zero Day Initiative (ZDI) team pulled their sponsorship of the Pwn2Own hacking competition in Japan[64]. The open source vulnerability database "OSVDB" was shut down in 2015. According to Katie Moussouris, a member of the U.S. Wassenaar delegation, "Non-disclosure and decreasing participation among researchers based in Wassenaar countries in international exploitation competitions like Pwn2own has already been observed."[65] It is expected that these controls will impact the international trade related to the security software and technology, including cross-border information sharing.

For the export subsidies measure, the government can support the export of products with built-in backdoors or discovered but non-disclosed vulnerabilities to other countries, which will create the potential for hacking attacks in the future. One interesting example is the one we discussed above: the then-U.S. company Netbotz sold security cameras with a built-in backdoor at extremely cheap prices to government-departments and to corporations operating with high-tech and military hardware.

3.2.3 National Action: Collaboration to Mitigate vs. Conflict to Amplify

1) Collaboration to Mitigate： The World Trade Organization (WTO) is the only global international organization dealing with the rules of trade between nations. Naturally, the impact of cybersecurity on international trade has not always been a consideration of the WTO. When it was originally established, the digital economy was miniscule and cybersecurity was not yet a concern. Trade regulations dealing with cybersecurity concerns can now be discussed in the meeting of the Technical Barriers to Trade (TBT) Committee. As shown in Table 3, based on the "Minutes of the Meeting of 14-15 June 2017, Committee on Technical Barriers to Trade, WTO"[66], we can identify eight concerns about trade regulations that have been implemented by initiating counties. Most of the concerns (seven concerning China's cybersecurity-related regulations and one concerning India's telecommunication-related rules) use unclear definitions of key terms like "secure and controllable", "critical infrastructure" and "IoV Systems." The main concerns are that the "unclear, but broad intended scope" declared in the creation of the security risk assessment could put intellectual property and product security at risk, and that measuring "indigenous" intellectual property with a national standard instead of international testing standards is unnecessary. In addition, these concerns include operational issues. The minutes refer to notifying the TBT committee of measures, offering comment periods and delaying the implementation date etc. However, sometimes it takes a long time to discuss the concerns. For example, the India-New Telecommunications Related Rules have been discussed for about seven years since 2010 and concerns have been raised 20 times. These rules do offer a procedure by which to discuss the related concerns and measures. China, for example, clarified the definition of "secure and controllable" during the TBT meeting. The country has rising concerns related to banking and insurance information technology regulation, which it plans to address by introducing further amendments. However, as the TBT Agreement was not originally implemented for the digital economy, some of the concerns will be

[63] Though due to uniform objections to this regulation by industry groups, nonprofits, and software and technology companies, BIS backed off in 2015. In 2016, the U.S. renegotiated the regulations. Though now the U.S. does not implement these controls, other countries like U.K. already implemented related controls.

[64] https://www.scmagazine.com/wassenaar-arrangement-confusion-cited-as-hp-pulls-pwn2own-sponsorship/article/532500/

[65] https://arstechnica.com/tech-policy/2016/12/us-fails-in-bid-to-renegotiate-arms-trade-restrictions-on-exploit-data-export/

[66] https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm

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, which can be used by nations to discuss cybersecurity-related concerns, Meltzer has proposed an expansion of the General Agreement on Trade in Services (GATS) to cover the scope of online trade (J. P. Meltzer 2015). Some on-going regional agreements also involve cybersecurity issues, especially those concerning data transfer cross-border. For example, the "trans-pacific partnership (TPP)"[67] states "*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 government services and two general exceptions- privacy and essential security. The USA 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/prohibitions on data localization. The "Trade in Service Agreement (TISA)" includes "*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*".

Furthermore, the EU-US Safe Harbor Agreement, which was approved by the EU in 2000, allows data transfer between the EU and the U.S.[68] The "European Commission's Directive on Data Protection" went into effect in October 1998 and prohibited the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. Though the U.S.-EU Safe Harbor Framework was determined to be "invalid" by the European Court of Justice on October 6, 2015, the EU-U.S. Privacy Shield Framework was approved on July 12, 2016. The Shield Framework replaced the U.S.-EU Safe Harbor Framework as a valid legal mechanism to comply with EU requirements when transferring personal data from the European Union to the United States.

Beside these, the Council of Europe Convention on Cybercrime ("CEC") is considered the "most significant, multilateral arrangement that specifically addresses aspects of cyberattacks and exploitation" (Sofaer, Clark, and Diffie 2010). The CEC is a law-enforcement treaty focusing on five types of actions against the integrity of cyber systems. These include illegal access; illegal interception; data interference; system interference; and misuse of devices and the cybercrime-like fraud, forgery, child pornography, and violations of copyright laws. As we discussed above, the Shanghai Cooperation Organization (SCO) also put forth an effort to encourage behavior norms in cyberspace through the submission of the Draft to the UN General Assembly about International Code of Conduct for Information Security in January 2015. The "BRICS Leaders Xiamen Declaration"[69] in September 4, 2017 emphasized the critical role of the UN in "developing universally accepted norms of responsible state behavior in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment." The declaration promotes further collaboration in ensuring security in the use of ICTs according to the "BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICT." Numerous other

[67] The TPP was never put into force as a result of the withdrawal of the U.S. In January 2018, all original TPP signatories except the U.S. concluded 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

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

[69] http://pibphoto.nic.in/documents/rlink/2017/sep/p20179401.pdf

governmental entities are involved in international cybersecurity issues, as evidenced by the ITU World Summit on the Information Society and the cybersecurity working groups in regional bodies like "*the Asia- Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), the European Union (EU), the Group of Eight (G8), the Organization of American States (OAS), and the Organization for Economic Cooperation (OECD)*" (Sofaer, Clark, and Diffie 2010).

In addition, some bilateral-dialogue mechanisms or agreements have been developed over the years to deal with increasing cybersecurity concerns. For example, the first U.S.-China Law Enforcement and Cybersecurity Dialogue (LECD)[70] was held on October 4, 2017, and served as "an important forum for advancing bilateral law enforcement and cyber priorities between [our] two governments"[71]. From the cybercrime and cybersecurity perspectives, "*Both sides will continue their implementation of the consensus reached by the Chinese and American Presidents in 2015 on U.S.-China cybersecurity cooperation, consisting of the five following points: (1) that timely responses should be provided to requests for information and assistance concerning malicious cyber activities; (2) that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors; (3) to make common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community; (4) to maintain a high-level joint dialogue mechanism on fighting cybercrime and related issues; and (5) to enhance law enforcement communication on cyber security incidents and to mutually provide timely responses.*" It offers a positive sign that both governments are working to create behavior norms for cyberspace. In fact, it has been reported that since the original cyber agreement between the U.S and China, "*both public and private sector analysts noted a precipitous drop in economic espionage cyberattacks on U.S. firms originating from Chinese actors*"[72].

2) Conflict to Amplify: The relations between the U.S. and Russia are completely different. To begin, there are substantial suspicions that the Russian government spread "fake news" to mislead voters during the 2016 U.S. election. In July 2017, Rep. Brendan Boyle even introduced the "No Cyber Cooperation with Russia Act," a 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. The proposed act would ban the use of federal funds to create, promote or support a joint cybersecurity program with Russia[73]. Though right now this bill is "in committee" and has not yet come to a vote, it reveals a high level of distrust and, consequently, a tense relationship between these two nations. The cyberspace conflict has even been named "Cold War 2.0."[74] It is believed that escalation will continue, creating huge challenges for cybersecurity cooperation 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 et al. 2017).

---

[70] 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.

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

[72] http://thehill.com/opinion/cybersecurity/356009-the-us-china-cyber-agreement-still-matters-but-its-not-enough

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

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

3.3 Impacted Organization Actions

Similar to Oliver's theory about organizational actors' strategic responses to institutional processes (Oliver 1991), the organization's action to cybersecurity-related regulations can also be divided into five different categories: acquiescence, compromise, avoidance, defiance and influence[75]. This is summarized in Table 3.

1) **Acquiescence**: Normally, organizations must accept the government's cybersecurity-related regulations, especially when the regulations are related to national security concerns. Additionally, for cybersecurity-related standards, local organizations will accede to them since they can improve the organization's cybersecurity which then results in a market advantage. For example, HP announced the world's most secure printers that deliver increased protection against malicious attacks, which can give their printers a competitive advantage[76]. Another scenario involves an organization which intends to enter a new international market. They will try to comply with existing policies and regulations to reduce entrance barriers. We observe many examples of this kind of organizational reaction to cybersecurity regulations. For example, when Russia's regulation of foreign e-service VAT became effective, more than 100 foreign tech giants had already 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[77].

2) **Compromise**: The second type of reaction for an organization is to negotiate with the governments about the cybersecurity regulations, tying to exact some concessions for both sides. Normally the government will offer some window of time for the organizations to communicate the related situations. If the organization can negotiate with the government, they can understand more about the exact cybersecurity concern for the specific case. For example, Microsoft Windows 8 was completely banned from Chinese government procurement in 2014. However, Microsoft chose to work with the Chinese government and built a special government approved version of Windows 10 for China[78]. In another example, the end-to-end encrypted Telegram messaging app, after being threatened with a ban in Russia, finally agreed to register with new Russian Data Protection Laws. However, the app's founder has assured customers that the company will not comply with requirements to share users' confidential data: Telegram will register with the Russian government, but the company will not store citizens' information on the Russian servers[79].

Table 3: The organizational reactions to the cybersecurity related actions from governments

Category	Definition	Example

[75] Here we use "influence" 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

[76] http://www8.hp.com/us/en/solutions/business-solutions/printingsolutions/devicesecurity.html

[77] 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/

[78] https://thenextweb.com/microsoft/2016/03/28/microsoft-windows-10-china

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

Acquiescence	Organization accedes to the cybersecurity related regulations and policies, especially for the local technical standards or when entering an international market	More than 100 foreign tech giants have already registered to accept the foreign e-services VAT structure in Russia, including Google, Apple, Microsoft, LinkedIn, Netflix, Bloomberg and the Financial Times.
Compromise	Organization will negotiate with the governments about the cyber security regulations, trying to exact some concessions from both sides.	Example 1: In the face of the outright ban of Windows 8 for Chinese government procurement, Microsoft built a special government-approved version of Windows 10 for China. Example 2: After being threatened with a ban in Russia, end-to-end encrypted Telegram messaging app has finally agreed to register with new Russian Data Protection Laws, but its founder has assured that the company will not share users' confidential data at any cost: it will register with the Russian government, but not store citizens' information on the Russian servers.
Avoidance	Organization will exit the market or try to disguise nonconformity and pretend to comply	Example 1: Google's complete pull out of Chinese market in 2010. Example 2: Huawei's exit from the U.S. market in 2014 due to the concerns over espionage. Though the company maintains "pretty good growth" without playing the U.S., after comments that businesses and customers in the U.S are getting a bad deal due to Huawei's absence in the market, the company added that it would consider re-entering America if it was welcomed.
Defiance	Organization will dismiss, challenge or attack the cybersecurity regulations. Defiance is normally bundled with avoidance.	Example 1: Russia blocked LinkedIn in 2017, after receiving a letter from the VP of global public policy of LinkedIn stating that LinkedIn will not move Russian user data to Russian territory.
Collaboration	Organization will negotiate with the governments to rescind the cybersecurity requirement, or influent the national governments to negotiate with the source national governments to revise or halt the requirements.	Example 1: After productive discussions, the Government of Pakistan has rescinded the shutdown order of BlackBerry in 2015. Example 2: India tried to negotiate with EU to be assigned a data-secure status. Example 3: Considering the requirement to turn over the source code if selling computer equipment to Chinese banks, the U.S. trade representative took up the issue in formal talks with Chinese regulators. Then-President Obama discussed the matter personally with President Xi Jinping in 2015, and finally China proposed a new regulation in 2016. Example 4: The Wassenaar Agreement cyber security related controls are not implemented due to the uniform objections by the industry groups, nonprofits, and software and technology companies in 2015.

3) **Avoidance**: The third type of reaction is to exit the market, or even try to disguise nonconformity

and pretend that the company already complied with the regulation while actually not having complied. The organization may choose to exit the market when the market is quite small, complying with the regulation is too costly, or if the institutional pressures from the mother-country are too intense. Google's withdrawal from China in 2010 is a typical example. Yahoo and Google faced criticism in the U.S. for helping the Chinese government pursue its cybersecurity goals. Yahoo and its Chinese subsidiary also faced lawsuits in the U.S. for their cybersecurity-related actions in China. Amnesty International accused U.S.-based Internet companies such as Google, Microsoft and Yahoo of violating the Universal Declaration of Human Rights in their agreement with the Chinese government to censor internet use in China. Kai-Fu Lee, the president of Google's Greater China operation, unexpectedly left Google to start a venture fund in September 4, 2009. In a 2009 report, Google noted that it had discovered an attack on its infrastructures that originated in China. In January 2010, Google announced that, in response to a Chinese-originated hacking attack on them and other U.S. tech companies, they were no longer willing to censor searches in China and would pull out of the country completely if necessary. Six months later, Google completely withdraw from the Chinese market. Huawei provides another example, having finally exited the U.S. market in 2014 due to continuous concerns over espionage. Though the company maintained "pretty good growth" without playing the U.S., Huawei commented during an interview that businesses and customers in the U.S are getting a bad deal due to the fact that Huawei is not in the market and added that the company would consider re-entering America if it was welcomed.

4) **Defiance**: Another type of reaction from organization is a dismissal, challenge or attack of cybersecurity regulations. Defiance is normally bundled with avoidance. If the organization is outright banned from the market because of the cybersecurity regulations or policies, they may challenge or attack such regulations. On the other hand, if an organization attacks the regulations, this may result in an outright ban, especially when the government of the initiating nation is powerful. For example, Russia blocked LinkedIn in 2017, after receiving a letter from the VP of global public policy of LinkedIn stating that LinkedIn would not move Russian user data to Russian territory.

5) **Collaboration**: The last type of action is a collaboration with the governments of both the initiating and coping nation, to mitigate the negative impact from the regulations, or even be involved in the regulation making process. We observe many recent cases of collaboration. In 2015, after productive discussions with the Government of Pakistan, the order to shutdown BlackBerry was later rescinded. Considering the requirement to turn over the source code if selling computer equipment to Chinese banks, European and U.S. 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. Another example is the Wassenaar Agreement cyber security related controls, which are not implemented due to uniform objections by industry groups, nonprofits, software and technology companies in 2015. However, not every case results in a happy ending. Though India tried to negotiate with the EU for many years in order to be assigned a data-secure status, the regulation has not changed yet.

From the business perspective, supply chain cybersecurity risk management has become a daily topic in the executives' agenda. This is unsurprising, given the increasing cybersecurity risks associated

with suppliers of goods and services. To secure the physical and digital supply chain, organizations must 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. These concerns shape the organization's decisions on supplier selection and market possession. To enhance cybersecurity for the global supply chain, some organizations will try to ***collaborate*** with their governments to initiate policies which impact international trade. For example, on August 9, 2017, 10 major cybersecurity companies[80] in the U.S. wrote to the U.S. Trade Representative Robert Lighthizer. Their letter encouraged him 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".

4 Evidence from Real-world Cases

As described above, we developed a systematic taxonomy based on a conceptual model to understand different actions related to cybersecurity concern and international trade. To verify our framework, we now look to collected cases related to cybersecurity concern and international trades. Specially, we focus on those cases related to both international trade and cybersecurity concern. Using searching engines like Google as well as publicly available reports and publication, we were able to collect 33 different cases related to our research until December 2017. Note that for each case, we include a series of related events so that we can better understand the dynamics of the case. For example, for the Huawei's restriction case in U.S., we collect the related 14 events between 2008 and 2018, which we will discuss more detail later. Furthermore, for each event, we include the initiating country, coping country, cybersecurity concern, national action, organizational action, timeline and details, resulting in a dataset which includes 149 events.

According to the cases we collected, as shown in Figure 2, the press has heavily focused on trade issues between the U.S., China, and Russia, such as the Kaspersky ban in U.S., LinkedIn's restriction in Russia, and constraints on VPN in China. But the scope of cybersecurity's impact goes far beyond these three countries. Even at this early stage, this is a worldwide phenomenon.

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

Fig 2: Nations that have instituted international trade restrictions due to cybersecurity concerns. Grey color means we collect at least one case related to that nation.

In addition, the impacted products cover most aspects of digital goods and services, not only the VPN, Telecom products, semiconductor, Microsoft office and social media, but also products such as security cameras, banking IT systems, drones, smart phones, smart toys, the online payment service and online content service. This means that cybersecurity's impact on international trade is not limited to specific goods or services. Instead, as we are growing into the digital society, any goods and products related to ICT technology, even toys, can be impacted by cybersecurity concerns.

The different circumstances of each case lead to differing actions and outcomes. Using the framework above, the 33 cases studied are summarized in Figure 3. The 33 cases are horizontal, and the differing circumstances, actions, and outcomes are along the vertical. A check mark and yellow marker are shown whenever the circumstances, actions, and outcomes apply. For purposes of brevity, we do not intend to discuss all these cases in this paper, but the scatter of yellow reveals the great diversity among cases.

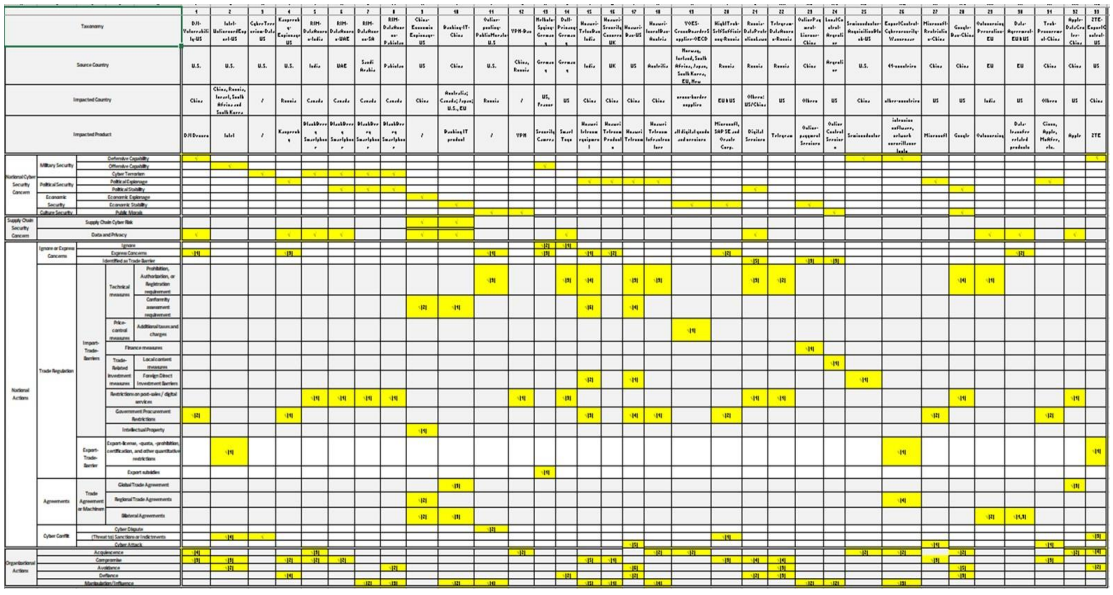
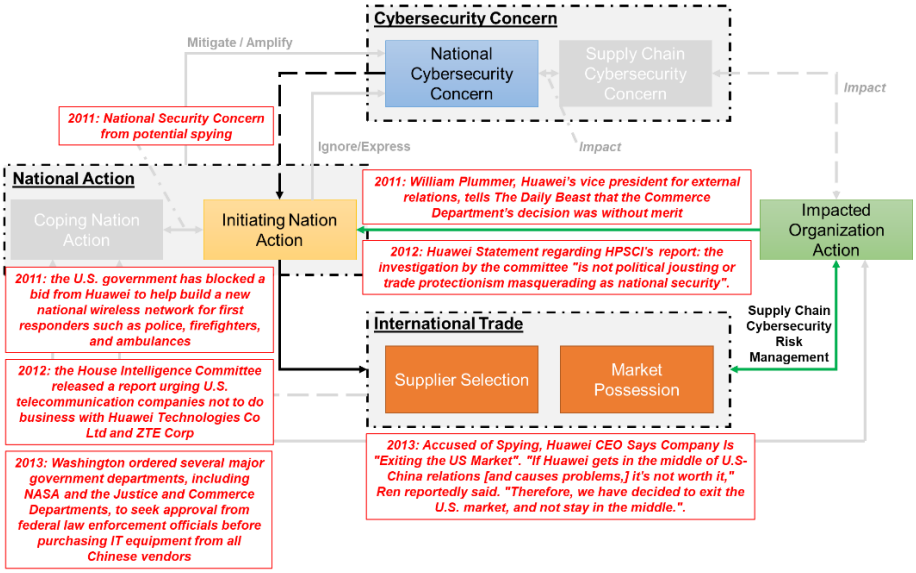


Fig 3: Matrix Listing the Cases Studied and their Differing Circumstances, Actions, Outcomes[81].

4.1 Differing Outcomes of Huawei's case in the U.S. and U.K

We will use Huawei's case in the U.S. and U.K. as an example of differing organizational actions and outcomes. The case is diagrammed in Figure 4.

The sequence of events with the U.S. is shown in Figure 4(a). 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. 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. The report warned that potential Chinese state influence on the companies posed a threat to U.S. security, even though after an 18-month review, a U.S. congressional report concluded that "*there is no evidence of any Huawei involvement with any espionage or other non-commercial activities*"[82]. In 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 Chinese vendors. The new rules required 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. Finally, in 2014, Huawei decided to exit the U.S. telecommunication 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."[83]

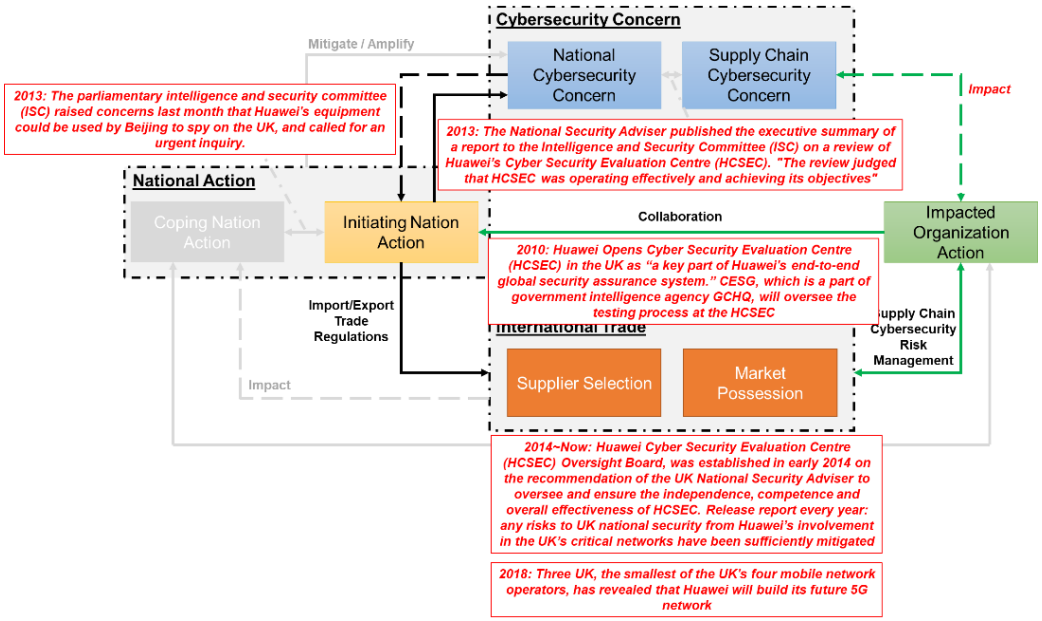


(a) Huawei exits the U.S. market

[81] Note that we don't intend to show the detail of this matrix here. The detail can be available by requested. Here we use this matrix with yellow market to show the diversity of cybersecurity concern and outcome.

[82] https://www.bbc.com/news/technology-19988919

[83] http://gizmodo.com/accused-of-spying-huawei-ceo-says-company-is-exiting-1475628703



(b) Huawei continues business in the U.K

Fig 4: Huawei's Cases in the U.S and the U.K

The other example case, as shown in Figure 4 (b), began when Huawei opened its Cyber Security Evaluation Centre in the U.K. in 2010. "*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 U.K.*" The U.K. government's National Technical Authority for Information Assurance (CESG), which is a part of the Government Communications Headquarters (GCHQ), oversees 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 U.K., 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). The summary concluded that "*The review judged that the HCSEC was operating effectively and achieving its objectives*". In early 2014, the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board was further established on the recommendation of the U.K. National Security Adviser to oversee and ensure the independence, competence and overall effectiveness of HCSEC. Every year it releases a report about any risks to U.K. national security from Huawei's involvement in the U.K.'s critical networks and makes sure that these risks have been sufficiently mitigated.

Hence, although the U.S. and Australia continue to lock Huawei out from their 5G markets, in August 2018, Three U.K., the smallest of the U.K.'s four mobile network operators, revealed that Huawei will build its future 5G network.[84]

[84] https://www.lightreading.com/mobile/5g/nokia-samsung-miss-out-as-three-uk-gives-5g-job-to-

This in-depth case study, about Huawei's business in the 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 the organization to help to reduce the national cybersecurity concern and enhance the global supply chain security. It also shows that if the organization and the countries can work together and systematically implement the best practices, it could reshape international trade and reduce overall cybersecurity risk.

4.2 Interaction between International Relations and Cybersecurity Concern within the International Trade Context

Based on the cases we collected, we can observe the interaction dynamic of organizational and national actions. In addition, the international relations and collaboration mechanisms between the initiating and coping nation have significant impact on the resolution of the cybersecurity concerns. Taking the U.S.-China relationship as an example:

- Before 2015, there was no effective cooperation/dialogue mechanism between the U.S. and China on cybersecurity issues. Huawei was finally banned and left the U.S. market while products from Cisco Systems Inc and Intel McAfee have been removed from China's government procurement list.
- The U.S. and Chine began developing cybersecurity cooperation in 2015 and LECD was held in October 2017. During this time, the U.S. and China have been developing digital trust and promoting cyber behavior norms to deal with their respective cybersecurity concerns. It offers a positive sign that both governments are working to create behavior norms for cyberspace.
- Since 2018, China and the United States have been locked in the on-going China–United States trade war rendering cyberspace communication channels between the U.S. and China ineffective. During this time we have observed an increase in cases of products banned due to cybersecurity concerns: A group of lawmakers wrote a letter to the Federal Communications Commission expressing concerns about Huawei's smartphone sold in the United States, and the AT&T and Verizon Communication Inc. dropped all plans to sell Huawei's smartphone under pressure from the U.S. government. The U.S. government failed to approve a multimillion-dollar merger between MoneyGram and Ant Financial, an affiliate of Alibaba in January 2018. President Trump signed the Defense Authorization Act in 2018 August which largely banned the use of Huawei and ZTE technology by the U.S government and government contractors.

5 Dynamics between International Trade and Cybersecurity Concern

Until now, using the conceptual model and the cases we collected, we have seen that cybersecurity impact on international trade is a worldwide phenomenon and can affect any product or event with an ICT component. In addition, there exist many different options for nations and organizations to deal with these cybersecurity concerns. Different actions from nations and organizations will end up with totally different results; the interaction between international trade and cybersecurity concern is highly diversified.

huawei/d/d-id/745121

5.1 Three Mechanisms Affecting Cybersecurity Concern and International Trade

To get a deeper understanding about the interactions between international trade and cybersecurity concern, during December 2017 to April 2018, we did an in-depth interview with more than 10 domain experts to understand how cybersecurity impacts international trade in different industrial sectors. On April 2018, we organized 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. The workshop discussion provides insightful thought about the framework presented here.

The key takeaways from these discussions and interviews, together with the understanding of the cases and framework, help us identify three different scenarios. These include the regulation compliance scenario, supply chain cyber risk management scenario and geopolitical scenario, which represent the three main dynamic mechanisms between international trade and cybersecurity concern:

- **Regulation Compliance Scenario**: in this scenario, as shown in Figure 5 (a), due to the national cybersecurity concern, the initiating nation will implement import/export cybersecurity related trade policies, which will impact international trade. Organizations consider these policies as regulations with which they need to comply, and then use these regulations as the baseline guidance for their global supply chain risk management. In most cases, organizations' only option is to accept these policies. However, sometimes 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 observe many cases belonging to this scenario, in which organizations proactively react to global cybersecurity policies. Given that more and more cybersecurity related policies are coming into effect, acting in anticipation of these policies will create significant compliance cost and uncertainty for the organizational global supply chain.

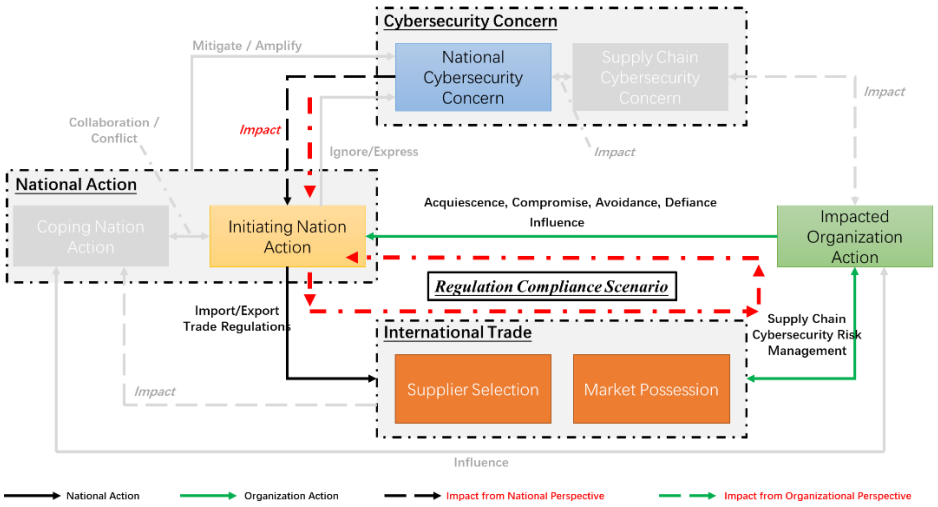


Fig 5 (a): Cybersecurity impact on International Trade: Regulation Compliance Scenario

- **Supply Chain Cyber Risk Management Scenario**: in the supply chain management context, as shown in Figure 5 (b), organizations consider cybersecurity risk from the supply chain as an important influence on business strategy. Businesses try to implement the supply chain cybersecurity risk

management standard. To make this implementation easier, an organization may even try to influence the mother-nation to implement some import/export trade regulations to further impact international trade. These influences will work together to reshape the global supply chain.

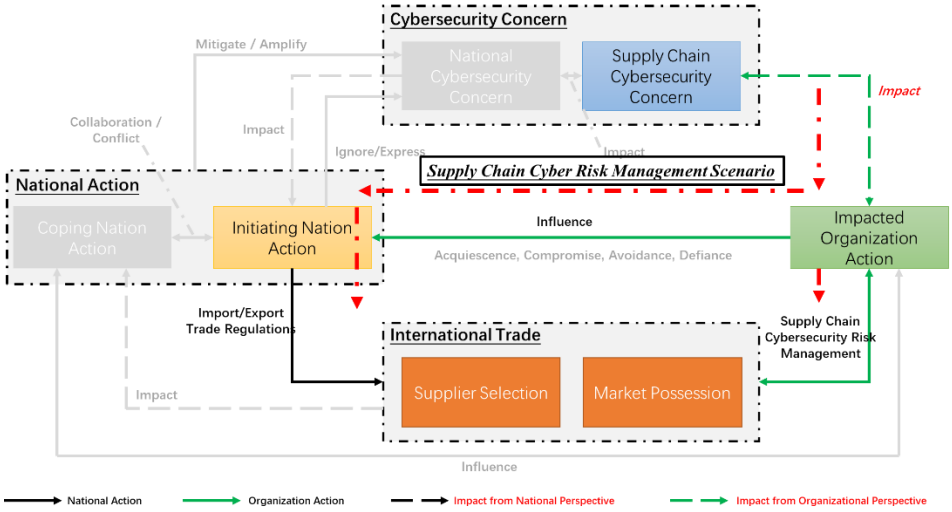


Fig 5 (b): Cybersecurity impact on International Trade: Supply Chain Cyber Risk Management Scenario

- **Geopolitics Cybersecurity Scenario:** in this scenario, as shown in Figure 5 (c), the cybersecurity's impact on international trade from is considered from the geopolitical perspective. Considering national cybersecurity concerns, the initiating nation will use import/export trade regulations to impact international trade, which will impact the other nations. The coping nation will take different actions in reaction to newly initiated trade regulations. Some global mechanisms like the WTO TBT Agreement and the General Agreement on Trade in Services (GATS) may be 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 of mitigating cybersecurity concerns in a more effective way. In addition, 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 serve as a living example of this scenario.

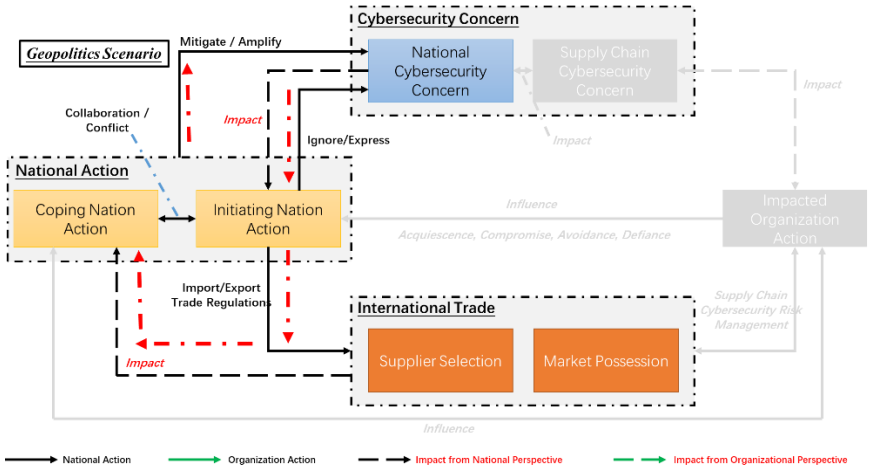


Fig 5 (c): Cybersecurity impact on International Trade: Geopolitics Scenario

5.2 Transformation among Three Scenarios

Using the developed framework, it can be seen that these three scenarios are not independent but can be transformed among each other, as summarized in Figure 6:

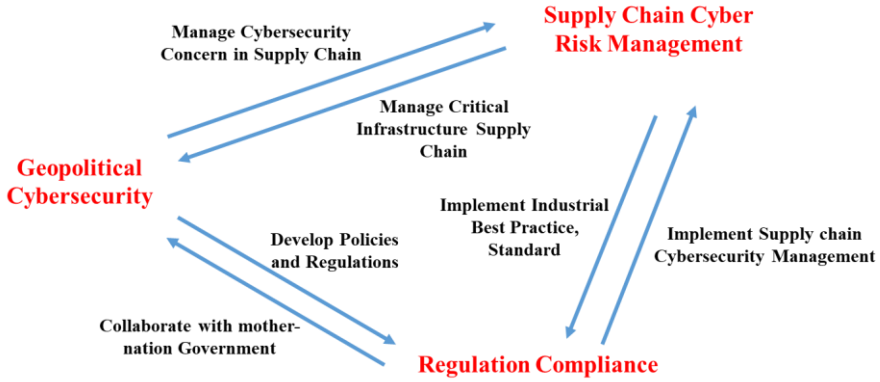


Fig 6: Cybersecurity impact on International Trade: Geopolitics Scenario

- **From Regulation Compliance to Geopolitical Cybersecurity Scenario**: If the organizations impacted by the initiating nation's actions can influence their mother-nations to act, the regulation compliance scenario can be transformed into a geopolitical cybersecurity scenario. Note that this transformation can be a good thing, but can also make a conflict worse. 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. For example, considering China's pending requirement that foreign businesses turn over source code if selling computer equipment to Chinese banks, European and U.S. 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. However, if the initiating nation and coping nation have strained relations, it is easy to amplify the cyber conflict between two nations and trap these

two nations into a "tit for tap" loop.

- **From Regulation Compliance to Supply Chain Cyber Risk Management Scenario**: In this scenario, organizations don't view cybersecurity risk as only a regulation compliance issue. Instead, they use the regulation compliance pressure to push the organization to consider cybersecurity risk from the supply chain management perspective. This can even positively impact international trade and reduce global supply chain cyber risk.
- **From Supply Chain Cyber Risk Management to Regulation Compliance Scenario**: If organizations can systematically consider the cybersecurity risk of the supply chain and try to implement best practices in each industry sector, it will reshape international trade. When an organization develops its global supply chain, its leaders must consider not only supply chain efficiency factors like cost and revenue, but also take into consideration the cybersecurity risk from different vendors. To push the implementation of the best industry practices and standards, organizations can even work together with governments to speed up the adoption of these practices and standards. For example, in 2017, ten major cybersecurity companies in the U.S sought to promote the development and alignment of the NIST cybersecurity framework into NAFTA.
- **From Supply Chain Cyber Risk Management to Geopolitical Cybersecurity Scenario**. This transformation is the case most typically seen case when examining the impact of cybersecurity on international trade. Just as we discussed before, the supply chain risk management of critical infrastructures can impact national security and become an important topic for geopolitical cybersecurity.
- **From Geopolitical Cybersecurity to Regulation Compliance Scenario.** Nations will implement different cybersecurity related regulations and policies, with which organizations must comply. On the other hand, geopolitical pressure can sometimes impact organizational reactions to the initiating nation's cybersecurity policies. Google's withdrawal from China in 2010 was impacted by criticism in the U.S. leveled at the company for helping the Chinese government pursue its cybersecurity goals.
- **From Geopolitical Cybersecurity to Supply Chain Cyber Risk Management Scenario.** When organizations interact with the cybersecurity risk from nations, their actions can impact supply chain cybersecurity concerns in the industry sector. For example, in 2017, the FBI briefed private sector companies on intelligence claiming that Kaspersky Lab products are unacceptable threats[85]. Even without mandates, this information impacted 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 in September 2017, due to cybersecurity concerns about Kaspersky Lab's products in the U.S.[86] Furthermore, this can impact policy makers' perception, resulting in further actions and reactions. In the example of the smart toys, Germany's Federal Network Agency finally forbade illicit radio transmission equipment in toys and prohibited the selling of the smart toy, "My Friend Cayla," in February, 2017[87]. On the other hand, considering the cybersecurity concerns Huawei's telecom products, the U.K. government's National Technical Authority for Information Assurance (CESG) and Huawei Cyber Security

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

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

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

Evaluation Centre (HCSEC) Oversight Board worked together to investigate the potential cyber threat. Taking the supply chain cyber risk management perspective, they were able to build and fully implement an end-to-end global cyber security assurance system to mitigate and manage the global cybersecurity challenge.

6 Conclusion

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

The cybersecurity of global supply chains is becoming an important issue for all nations. Due to the lack of consensus on cyberspace behavior norms and the vague definitions of national cyber security, we observe and expect even more cyber conflicts and negative impact on international trade in the near future. The good news is that recently there have been and continue to be many efforts made to reach consensus on cyberspace, especially with regards to the behaviors of the state. Though the details about national cyber security are still unclear, 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, nations must find common ground and work together to construct cybernorms.

From the organization's perspective, ignoring 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 of cybersecurity on these companies 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 turn into a cybersecurity risk management angle, and even become involved in the regulation process, not only during the comment periods but also during the regulation draft process. Since international trade cybernorms have yet to be developed, 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 relevant specific technical trends and market requirements. Organizations can create industrial best practices by focusing on global supply chain cybersecurity management. Though it would be a voluntary measure at the very beginning, once such standards are widely accepted across the industry sector, it could become the "de facto" cybernorm needed to mitigate the negative impact from cybersecurity concerns. Furthermore, organizational consensus could move cybernorms forward among different nations in cyberspace.

The conceptual model developed in this paper identifies three different scenarios when considering the cybersecurity impact on the international trade: the regulation compliance scenario, within which organizations act in anticipation of national cybersecurity policies; the supply chain cyber risk management scenario, within which organizations consider the supply chain cybersecurity as a strategy issue and try to manage the cyber risks within their physical and digital global supply chains; and the

geopolitical cybersecurity scenario, where nations can either collaborate to mitigate the cybersecurity concern or clash with each other and amplify the dispute. Importantly, these three scenarios are not independent but can be transformed into each other. In reality that there are no established cybernorms, now or in the near future. Therefore, if the whole system becomes looped into the negative geopolitical cybersecurity scenario, the "tit for tat" mire will evenly push the whole international trade into a "cyber trade war." To avoid this situation, the whole society, especially the business community, should work together to implement industrial best practice standards to turn the geopolitical pressures into the supply chain cyber risk management scenario. This will only to improve supply chain cybersecurity management and reduce the cybersecurity concern from global supply chain, but also help to reduce national cybersecurity concerns.

In the future, based on this conceptual model, we will develop a framework to further understand the dynamics of the national and organizational actions which can support the decision making process. We will develop policy suggestions that use cybersecurity concerns to improve international supply chain cyber security risk management.

Acknowledgements

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 would like to thank members from Cybersecurity at MIT Sloan for their valuable comments and input.

Reference

Acemoglu, Daron, Asuman Ozdaglar, and Alireza Tahbaz-Salehi. 2015. "Systemic Risk and Stability in Financial Networks." *American Economic Review* 105(2): 564–608.

Albert, Mathias, and Barry Buzan. 2011. "Securitization, Sectors and Functional Differentiation." *Security Dialogue* 42(4–5): 413–25. http://journals.sagepub.com/doi/10.1177/0967010611418710.

Awan, Imran. 2017. "Cyber-Extremism: Isis and the Power of Social Media." *Society* 54(2): 138–49.

Binderkrantz, Anne Skorkjær, Peter Munk Christiansen, and Helene Helboe Pedersen. 2014. "A Privileged Position? The Influence of Business Interests in Government Consultations." *Journal of Public Administration Research and Theory* 24(4): 879–96.

Boddewyn, Jean J, and Thomas L Brewer. 1994. "International-Business Political Behaviour: New Theoretical Directions." *Academy of Management Review* 19(1): 119–44.

Breene, Keith. 2016. "Who Are the Cyberwar Superpowers?" *WORLD ECONOMIC FORUM*: 1. https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

Burri, Mira. 2017. "The Regulation of Data Flows Through Trade Agreements." *Georgetown Journal of Internatonal Law* 48: 407–48.

Chen, Yan, and Fatemeh Mariam Zahedi. 2016. "Individuals' Internet Security Perceptions and Behaviors Polycontextual Contrasts Between the United States and China." *MIS Quarterly* 40(1): 205–22.

Clapper, James R., Marcel Lettre, and Michael S. Rogers. 2017. "Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States." : 7.

CREATE.org. 2016. *The Importance of Cybersecurity for Trade Secret Protection*.

Denning, De. 2007. “A View of Cyberterrorism Five Years Later.” *Internet Security: Hacking, Counterhacking and Society* (May 2000): 1–18. http://books.google.com/books?hl=en&lr=&id=VKFMTDnapl4C&oi=fnd&pg=PA239&dq=A+view+of+cyberterrorism+five+years+later&ots=jDeGRbWfzb&sig=tarJQVvl1i7RQbFu5TL-yTURkXk.

Donilon, Thomas et al. 2016. *Commission on Enhancing National Cybersecurity*.

Doomen, Jasper. 2013. “Political Stability after the Arab Spring.” *Sociological Forum* 28(2): 399–408.

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

Gansler, Jacques S, William Lucyshyn, and Lisa H Harrington. 2012. “Defense Supply Chain Security: Current State and Opportunities for Improvement.”

GAO. 2012. “IT SUPPLY CHAIN: National Security- Related Agencies Need to Better Address Risks.” *Report to Congressional Requesters* (March): 45.

Gechlik, Mei. 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*, National Security, Technology, and Law Working Group of the Hoover Institution, 1–24.

Hine, Gabriel Emile et al. 2016. “Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan’s Politically Incorrect Forum and Its Effects on the Web.” (Icwsm): 92–101. http://arxiv.org/abs/1610.03452.

Hodge, Graeme A. 2007. “Public-Private Partnerships: An International Performance Review.” *Public Administration Review* 67(3): 545–58.

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

Kelly, Sanja et al. 2017. *Freedom on the Net 2017*. https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf.

Klimburg, Alexander. 2012. NATO CCD COE Publication *National Cyber Security Framework Manual*.

Kopp, Emanuel, Lincoln Kaffenberger, and Christopher Wilson. 2017. *Cyber Risk, Market Failures, and Financial Stability*. http://www.imf.org/~/media/files/publications/wp/2017/wp17185.ashx.

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

Kshetri, Nir. 2016. *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*. Springer. http://books.google.com/books?id=wajCDAAAQBAJ&pg=PP1&dq=intitle:The+Quest+to+Cyber+Superiority+inauthor:kshetri&hl=&cd=1&source=gbs_api%0Apapers3://publication/uuid/77FDCDAE-71AD-4A2B-8D66-2C58D6EA1D7B.

Kuner, Christopher. 2011. *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future.* http://dx.doi.org/10.1787/5kg0s2fk315f-en.

Liff, Adam P. 2012. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies* 35(3): 401–28.

Lynn, William J. 2010. “Defending a New Domain the Pentagon’s Cyber Strategy.” *Foreign Affairs* 89(5): 98. http://www.scribd.com/doc/36500793/Defending-a-New-Domain-the-Pentagon-s-Cyber-Strategy.

Maness, Ryan C., and Brandon Valeriano. 2016. “The Impact of Cyber Conflict on International Interactions.” *Armed Forces & Society* 42(2): 301–23. http://journals.sagepub.com/doi/10.1177/0095327X15572997.

Manyika, James et al. 2016. *Digital Globalization : The New Era of Global Flows*.

Mata, Dan Constantin. 2015. “Cybersecurity Dimensions of National Security.” *Journal of Law and Administrative Sciences*: 132–42.

Meltzer, Joshua. 2014. Global Economy & Development *Supporting the Internet As a Platform for International Trade Opportunities for Small and Medium-Sized Enterprises and Developing Countries*.

Meltzer, Joshua Paul. 2015. “The Internet, Cross-Border Data Flows and International Trade.” *Asia & the Pacific Policy Studies* 2(1): 90–102. http://doi.wiley.com/10.1002/app5.60.

Mitchell, Andrew D, and Jarrod Hepburn. 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*, , 1–3.

———. 2018. *Framework for Improving Critical Infrastructure Cyber Security-Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018.

Nourian, Arash, and Stuart Madnick. 2015. “A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet.” *IEEE Transactions on Dependable and Secure Computing* PP(99): 20.

OECD. 2012. OECD Digital Economy Papers *Cybersecurity Policy Making at a Turning Point*. Paris. http://search.proquest.com.library.capella.edu/docview/1223514107?accountid=27965%5Cnhttp://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ABI/INFORM+Global&rft_val_fmt=info:ofi/f.

———. 2015. *Addressing the Tax Challenges of the Digital Economy, Action 1 - 2015 Final Report*. OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris. http://www.oecd-ilibrary.org.ez.urosario.edu.co/docserver/download/2314251e.pdf?expires=1429553838&id=id&accname=guest&checksum=446CDC8269DEAE27FEB0B6D9820B9960.

OFR. 2017. *Cybersecurity and Financial Stability: Risks and Resilience*. https://login.ezproxy.net.ucf.edu/login?auth=shibb&url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=42989261&site=ehost-live%5Cnhttps://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf.

OICU-IOSCO. 2016. “Cyber Security in Securities Markets – An International Perspective Report on IOSCO ’ s Cyber Risk Coordination Efforts.”

Oliver, Christine. 1991. “STRATEGIC RESPONSES TO INSTITUTIONAL PROCESSES.” *Academy of Management Review* 16(1): 145–79. http://amr.aom.org/cgi/doi/10.5465/AMR.1991.4279002.

Organization for Economic Co-operation and Development. 2005. OECD Trade Policy Studies *Looking Beyond Tariffs: The Role of Non-Tariff Barriers in World Trade*. http://www.oecd-ilibrary.org/trade/looking-beyond-tariffs/export-duties_9789264014626-8-en.

Palmisano, Sam. 2016. *Digital Supply Chains : A Frontside Flip*.

Peng, Shin Yi. 2015. “Cybersecurity Threats and the WTO National Security Exceptions.” In *Journal of International Economic Law*, , 449–78.

Ranger, Steve. 2017. “US Intelligence: 30 Countries Building Cyber Attack Capabilities.” *ZDNet*. http://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/.

Riek, Markus, Rainer Bohme, and Tyler Moore. 2016. “Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance.” *IEEE Transactions on Dependable and Secure Computing* 13(2): 261–73.

Salim, Hamid, and Stuart Madnick. 2016. *Cyber Safety : A Systems Theory Approach to Managing Cyber Security Risks-Applied to TJX Cyber Attack*.

Schmidtlein, Rhonda K., David S. Johanson, Irving A. Williamson, and Meredith M. Broadbent. 2017. *Global Digital Trade 1 : Market Opportunities and Key Foreign Trade Restrictions*. https://www.brookings.edu/testimonies/global-digital-trade-1-market-opportunities-and-key-foreign-trade-restrictions/.

Selby, John. 2017. “Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?” *International Journal of Law and Information Technology* 25(3): 213–32. http://academic.oup.com/ijlit/article/25/3/213/3960261/Data-localization-laws-trade-barriers-or.

Shackleford, Dave. 2015. SANS Whitepaper *Combatting Cyber Risks in the Supply Chain*.

Sheldon Whitehouse, Michael T. McCaul, Karen Evans, and Sameer Bhalotra. 2017. *From Awareness to Action: A Cybersecurity Agenda for the 45th President*. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160103_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

Singer, P.w, Friedman, Allan. 2014. “Cybersecurity and Cyberwar.” *Igarss 2014* (1): 1–5.

Slayton, Rebecca. 2017. “What Is the Cyber Offense-Defense Balance?” *International Security* 41(3): 72–109.

Sofaer, A., D. Clark, and W. Diffie. 2010. 8 *Cyber Security and International Agreements*. http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059440.pdf.

Staiger, R.W. 2012. “Non-Tariff Measures and the WTO.” *WTO Working Paper* (January): 45. https://www.wto.org/english/res_e/reser_e/ersd201201_e.pdf.

Sun, Nan-xiang. 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.

UN. 2015. “Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General.” *UN Doc. A/69/723* 00392(January): 6.

UNCTAD. 2012. “Classification of Non-Tariff Measures.” *United Nations Publication UNCTAD/DITC/TAB/2012/2* (February 2012): 52.

USTR. 2017. “NTE Trade Barriers.” *(Online)*. http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/ftrade/#.

Venkatesh, Viswanath, James Y. L. Thong, and Xin Xu. 2012. “CONSUMER ACCEPTANCE AND USE OF INFORMATION TECHNOLOGY: EXTENDING THE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY.” *MIS Quarterly* 36(1): 157–78. http://s3.amazonaws.com/academia.edu.documents/36422124/Venkatesh_utaut2.pdf%3DUnified_theory_of_acceptance_and_use_of.pdf.

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

Welch, Gen. Larry D. 2011. “Cyberspace – the Fifth Operational Domain.” *IDA Research Notes*: 1–7.

Zheng, Jurong, Jens K. Roehrich, and Michael A. Lewis. 2008. “The Dynamics of Contractual and Relational Governance: Evidence from Long-Term Public-Private Procurement Arrangements.” *Journal of Purchasing and Supply Management* 14(1): 43–54.

ID	Key	Abstract	Source Country	Impacted Country	Impacted Products	Concern	Nation Actions	Organization Action	TimeLine	Detail	Source
1	DJI-Vulnerability-US	US army halts use of Chinese Made Drones (DJ) due to the concern of "cyber vulnerabilities" in the products	U.S.	China	DJI Drones	Military-Defensive	Express Concerns	Avoidance	4/1/2016	the FBI has now ordered drone manufacturer DJI to unlock a Phantom 3 drone downed at 2016 presidential candidate Donald Trump's private headquarters in Florida. DJI has refused to unlock the drone for authorities to reveal the aerial footage and flight history.	https://aviationvoice.com/dji-refuses-to-unlock-drone-apple-offers-support-2-201604011108/
							Government Procurement Restrictions		8/2/2017	Army memo posted online and verified by Reuters applies to all DJI drones and systems that uses DJI components or software. It requires service members to "cease all use, uninstall all DJI applications, remove all batteries/storage media and secure equipment for follow-on direction." The memo says DJI drones are the most widely used by the Army among off-the-shelf equipment of that type. A Pentagon spokesman said the Army was considering issuing a statement about the policy. DJI did not immediately respond to requests for comment. The move appears to follow studies conducted by the Army Research Laboratory and the Navy that said there were risks and vulnerabilities in DJI products. The memo cites a classified Army Research Laboratory report and a Navy memo, both from May as references for the order to cease use of DJI drones and related equipment	https://www.reuters.com/article/usa-army-drones-idUSL1N1KQ1KC
								Compromise: Make Statement	8/4/2017	DJI makes civilian drones for peaceful purposes. They are built for personal and professional use, and are not designed for military uses or constructed to military specifications. We do not market our products for military customers, and if military members choose to buy and use our products as the best way to accomplish their tasks, we have no way of knowing who they are or what they do with them. The US Army has not explained why it suddenly banned the use of DJI drones and components, what "cyber vulnerabilities" it is concerned about, or whether it has also excluded drones made by other manufacturers. Around the globe, businesses and governments rely on DJI to provide an aerial perspective on their work to save time, save money and sometimes even save lives. Even in highly sensitive applications involving critical infrastructure, customers use DJI products with confidence that they can accomplish their tasks. DJI has worked hard to earn our reputation as the drone industry's leading innovator, and we will continue to provide solutions that our customers can depend on. If any of our customers have questions or concerns about DJI's technology, we ask them to contact us directly so we can work to address them. Until then, we ask everyone to refrain from undue speculation.	
								Acquiescence	8/15/2017	DJI is working on a "local data mode" for its apps that prevents any data from being sent to or received from the internet. The feature will be welcomed by many, but it's hard not to attribute the timing and urgency of the announcement to the recent ban of DJI gear by the U.S. Army over unspecified "cyber vulnerabilities." "We are creating local data mode to address the needs of our enterprise customers, including public and private organizations that are using DJI technology to perform sensitive operations around the world," said Brendan Schulman, the company's VP of Policy and Legal Affairs, in a press release. The new feature should arrive before the end of September.	https://fstoppers.com/aerial/us-army-ban-dji-what-really-going-190937
2	Intel-UnlicensedExport-US	Wind River unlicensed exports of operating software containing encryption as required by the Export Administration Regulations	U.S.	China, Russia, Israel, South Africa and	Intel	Military-Offensive	Export Control	Avoidance	2008/1~2011/9	Between January 2008 and September 2011, Wind River exported approximately $3 million worth of software to government end-users in China, Hong Kong, Russia, Israel, South Africa and South Korea, and to Entity List end-users in China. Wind River failed to obtain licenses for any of the exports as required by the Export Administration Regulations.	https://www.law360.com/articles/596140/wind-river-case-may-signal-change-for-encryption-exports
								Compromise	10/8/2014	On Oct. 8, 2014, BIS announced that Intel subsidiary Wind River Systems Inc. would pay a civil penalty of $750,000 to settle 55 export control violations concerning operating software controlled under ECCN 5D002.	
3	CyberTerrorism-Data-US	the U.S. government charged a hacker with stealing data bout military and other government personnel and passing them to ISIS	U.S.	/	/	Military-CyberTerrorism			2015/9~2015/10	Ardit Ferizi was arrested in September 2015, according to the US intelligence the man provided the data to the popular IS militant Junaid Hussain, which disclosed it on the web. According to the investigators, Hussain and Ferizi started their collaborations months before, in April 2015. In October 2015, for the first time, the US Government has charged a hacker in Malaysia with stealing the data belonging to the US service members and passing it to the members of the ISIS with the intent to support them in arranging attacks against Western targets,	http://resources.infosecinstitute.com/the-ferizi-case-the-first-man-charged-with-cyber-terrorism/#gref
4	Kaspersky-Espionage-US	Kaspersky Lab Products are banned in the U.S. due to the concerns of using the products for cyber espionage	U.S.	Russia	Kaspersky	Political Espionage	Government Procurement Restrictions		6/28/2017	The Department of Defense's next budget may ban the use of products from Kaspersky, the Moscow-based cybersecurity company accused by U.S. officials of possibly being under Kremlin influence.The newest draft of the National Defense Authorization Act won unanimous approval of the Senate Armed Services Committee on Wednesday.	https://www.cyberscoop.com/kaspersky-banned-us-dod-ndaa-russian-influence/
								Compromise-Negotiate	7/2/2017	founder and CEO Eugene Kaspersky repeated his offer to allow U.S. officials to review the company's source code	https://www.bankinfosecurity.com/russia-threatens-retaliation-if-us-bans-kaspersky-lab-a-10081
							Express Concerns		7/11/2017	Bloomberg magazine published an article, accusing the Moscow-based world leader in cybersecurity of close ties to Russia's security service, the FSB. The report, titled "Kaspersky Lab has been working with Russian Intelligence" alleged that the magazine had got hold of internal communication that explicitly show that Kaspersky Lab "has maintained a much closer working relationship" with FSB "than it has publicly admitted."	https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence
							Government Procurement Restrictions		7/14/2017	The federal agency in charge of purchasing, the General Services Administration, this month removed Moscow-based Kaspersky Lab from its list of approved vendors. The GSA's move on July 12 has left state and local governments to speculate about the risks of sticking with the company or abandoning taxpayer-funded contracts, sometimes at great cost. The General Services Administration (GSA) has removed Kaspersky Labs from its list of approved vendors over fears the Russian-owned cybersecurity company represents an undue risk to U.S. interests. GSA spokesman told Politico the move was made to "ensure the integrity and security of U.S. government systems and networks." Federal agencies can still buy and use Kaspersky products that are not part of a GSA contract and the GSA's move is a leading indicator that the Trump administration is not in favor of using Kaspersky products. This follows a move made by the U.S. Senate Armed Services Committee on June 29 that saw its annual defense spending bill containing a provision prohibiting the Department of Defense from using any products from Moscow-based cybersecurity firm Kaspersky Lab.	https://www.scmagazine.com/gsa-removes-kaspersky-labs-from-its-approved-vendors-list/article/675052/
								Compromise: Make Statement	7/14/2017	statement: Kaspersky Lab has no ties to any government, and the company has never helped, nor will help, any government in the world with its cyberespionage efforts. The company has a 20 year history in the IT security industry of always abiding by the highest ethical business practices and trustworthy development of technologies, and Kaspersky Lab believes it is completely unacceptable that the company is being unjustly accused without any hard evidence to back up these false allegations	
							Express Concerns		8/17/2017	The FBI has been briefing private sector companies on intelligence claiming to show that the Moscow-based cybersecurity company Kaspersky Lab is an unacceptable threat to national security	https://www.cyberscoop.com/fbi-kaspersky-private-sector-briefings-yarovaya-laws/
								Defiance	8/17/2017	In a statement to CyberScoop, a Kaspersky spokesperson blamed those particular accusations on "disgruntled, former company employees, whose accusations are meritless" while FBI officials say, in private and away from public scrutiny, they know the incident took place and was blessed by the company's leadership.	
							Government Procurement Restrictions		9/18/2017	US Senate votes to ban Kaspersky Lab software from government networks. The bill would bar the use of Kaspersky Lab in civilian and military agencies. The directive issued by the Trump administration last week applies only to civilian government agencies and not the Pentagon, but U.S. intelligence leaders said earlier this year that Kaspersky Lab was already generally not allowed on military networks.	http://www.rawstory.com/2017/09/us-senate-votes-to-ban-kaspersky-lab-software-from-government-networks/
5	RIM-DataAccess-India	RIM finally sets up BlackBerry server in Mumbai, providing a mechanism for lawful interception of its messenger services, due to the government's concern that militants could use the BlackBerry's secure network to plot terror attacks without fear of being monitored	India	Canada	BlackBerry Smartphone	Military-CyberTerrorism	Restrictions on post-sales / digital services		8/10/2010	Since the 2008 Mumbai killings, the Indian government has pressured BlackBerry to give it access to users' data -- BlackBerry devices were reported to have been used by the terrorists in the attacks; India backed down in 2008. India has given Research In Motion, the maker of the popular BlackBerry smartphone, until August 31 to comply with a request to gain access to encrypted corporate email and messaging services or those services will be shut	http://www.hollywoodreporter.com/news/india-says-rim-must-meet-26635
								Compromise	8/12/2010	Officials said RIM had proposed tracking emails without sharing encryption details, but that was not enough. The company said in a statement on Thursday that it had tried to be as cooperative as possible with governments. R.I.M. has said that it cannot provide unencrypted messages because its vaunted security system gives control over encryption to corporations and their employees, not to R.I.M. "RIM maintains a consistent global standard for lawful access requirements that does not include special deals for specific countries."	http://www.hollywoodreporter.com/news/india-says-rim-must-meet-26635
								Compromise	11/17/2010	BlackBerry maker Research In Motion (RIM) is ready to allow Indian authorities access to the emails and messages of its most high-profile corporate customers, according to a ministry official in the country. The secure communications of India's 400,000 BlackBerry owners could soon be lawfully accessed by government officials, the unnamed official said, adding that RIM is preparing for "providing live access" to customers' encrypted servers. "They have in principle agreed to provide us recorded data from their servers," India's the Mint business newspaper quoted an unnamed Indian ministry official as saying. RIM allowed Indian authorities access to the Messenger service since 1 September	https://www.theguardian.com/technology/2010/nov/17/india-blackberry-monitored-emails
								Acquiescence	2/20/2012	BlackBerry has finally set up its server in Mumbai following intense pressure from the government to provide a mechanism for lawful interception of its messenger services and Nokia has been asked to follow suit	http://www.gadgetsnow.com/tech-news/RIM-finally-sets-up-BlackBerry-server-in-Mumbai/articleshow/11963492.cms
6	RIM-DataAccess-UAE	BlackBerry escapes blackout but with tightened restrictions in UAE	UAE (United Arab Emirates)	Canada	BlackBerry Smartphone	Military-CyberTerrorism; Political Stability	Restrictions on post-sales / digital services		8/1/2010	UAE said it would block e-mail, instant messaging, and Web browsing on BlackBerry devices starting October 11 if it fails to reach an agreement with RIM to bring BlackBerry services in the region in line with UAE telecommunications regulations	http://www.nytimes.com/2010/08/02/business/global/02berry.html?mcubz=1
								Compromise: Make Statement	8/3/2010	In its statement, the company explained that data on its BlackBerry Enterprise Server network is encrypted so that no one, not even RIM, can access it.	https://www.cnet.com/news/rim-responds-to-blackberry-ban-in-middle-east/
								Compromise	10/8/2010	UAE telecommunications regulator said on Friday that RIM had brought its devices into line with strict local jurisdictions on security and encryption. Although the details of the compromise are unknown, RIM is thought to have granted some access to communications passed between devices to the UAE government, though there is no confirmation of this from either side	https://www.theguardian.com/technology/2010/oct/08/blackberry-uae-ban
							Restrictions on post-sales / digital services		4/18/2011	The UAE is to ban individuals and small businesses from using the most secure BlackBerry settings – for email, web browsing and BlackBerry Messenger – as part of security fears sweeping the Middle East. Only companies with more than 20 BlackBerry accounts will be able to access the encrypted BlackBerry service, which is favoured by corporate users and government agencies. "The UAE [Telecommunications Regulatory Authority] has confirmed to RIM that any potential policy regarding enterprise services in the UAE would be an industry-wide policy (not specific to BlackBerry) applying equally to all enterprise solution providers and with the intent of avoiding any impact on legitimate enterprise customers", the Canadian company said.	https://www.theguardian.com/technology/2011/apr/18/uae-blackberry-emails-secure

7	RIM-DataAccess-SA	BlackBerry ban lifted in Saudi Arabia	Saudi Arabia	Canada	BlackBerry Smartphone	Military-CyberTerrorism; Political Stability	Restrictions on post-sales / digital services		8/6/2010	Saudi Arabia has ordered the country's cell phone service providers to halt all BlackBerry services this week	https://www.cnet.com/news/saudi-arabia-announces-blackberry-ban/
								Influence	8/10/2010	BlackBerry Messenger ban gets temporary reprieve after RIM meets requirements imposed by Saudis	https://www.theguardian.com/technology/2010/aug/10/blackberry-saudi-arabia-ban-lifted
8	RIM-DataAccess-Pakistan	Pakistan allows BlackBerry to continue services	Pakistan	Canada	BlackBerry Smartphone	Military-CyberTerrorism; Political Stability	Restrictions on post-sales / digital services		7/27/2015	Pakistan willl ban BlackBerry's enterprise server and its internet and messaging services "for security reasons" in a crackdown on privacy. Mobile phone operators were told by the Pakistan telecommunication authority on Friday that the BlackBerry services must be shut down by Nov 30	https://www.theguardian.com/technology/2015/jul/27/pakistan-bans-blackberry-messaging-internet-services-privacy-crackdown
								Avoidance	11/30/2015	BlackBerry Chief Operating Officer Marty Beard confirmed in a statement posted to the smartphone makers' website that the company will not operate in Pakistan after Nov 30. the Government of Pakistan has notified BlackBerry that it has extended its shutdown order from November 30 to December 30. BlackBerry will delay its exit from the Pakistan market until ther	
								Influence	12/31/2015	After productive discussions, the Government of Pakistan has rescinded its shutdown order, and BlackBerry has decided to remain in the Pakistan market. "We are grateful to the Pakistan Telecommunication Authority and the Pakistani government for accepting BlackBerry's position that we cannot provide the content of our customers' BES traffic, nor will we provide access to our BES servers."	
9	China-Economic Espionage-US	US concern on the Cyber enabled theft of intellectual property from China	US	China	/	Economic Espionage	Bilateral Agreements		9/2015	The agreement reached by Obama and Xi stated that there should be increased communication and cooperation between the two countries to investigate and prevent cyber crimes emanating from their territory, and that neither the U.S. nor Chinese government would knowingly conduct or support cyber-enabled theft of intellectual property. They also agreed that both sides are committed to identifying, developing, and promoting appropriate norms of state behavior in cyberspace within the international community and establishing a high-level joint dialogue mechanism on fighting cybercrime and related issues.	http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/
							Bilateral Agreements		10/2015	China inked a similar deal with the United Kingdom	https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later
							Regional Agreements		11/2015	China, Brazil, Russia, the United States, and other members of the Group of Twenty accepted the norm against conducting cyber-enabled theft of intellectual property	
							Bilateral Agreements		6/2016	The United States and China have also held two round of cyber talks between the U.S. Department of Homeland Security (DHS) and Chinese Ministry of Public Security (MPS), the first in December 2015, the second in June 2016	
							Bilateral Agreements		8/2016	the Ministry of Public Security reported that the hotline between DHS and MPS was up and running	
							Conformity assessment requirement		8/2017	US President Donald Trump directed the US trade representative (USTR) to examine the so-called China's intellectual property practices, despite worries about potential harms to China-US trade ties	http://www.chinadaily.com.cn/world/2017-08/15/content_30625943.h
							Bilateral Agreements		10/4/2017	The first U.S.-China Law Enforcement and Cybersecurity Dialogue (LECD) was held on October 4, 2017, and served as "an important forum for advancing bilateral law enforcement and cyber priorities between two governments"	https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue
10	Banking-IT-China	To strengthen the security of the information network and operations management in the banking system to improve the stability of the financial systems	China	Australia; Canada; Japan; United States of America; European Union	Banking IT product	Economic Stability	Conformity assessment requirement; Intellectual Property		1/28/2015	The Chinese government has adopted new regulations requiring companies that sell computer equipment to Chinese banks to turn over secret source code, submit to invasive audits and build so-called back doors into hardware and software, according to a copy of the rules obtained by foreign technology companies that do billions of dollars' worth of business in China.	https://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html
								Influence	2/26/2015	European and US companies have asked their authorities for urgent help in stopping the implementation of new Chinese cyber security regulations, which are expected to force local and foreign banks to use information technology equipment deemed "secure and controllable" by Beijing.	https://www.ft.com/content/12a7a126-bd67-11e4-9902-00144feab7de
							Bilateral Negotiate		3/19/2015	The U.S. trade representative has taken up the issue in formal talks with Chinese regulators and President Obama indicates that he discussed the matter pe	http://www.chinalawblog.com/2015/03/china-bank-technology-rules-not-the-same-old-thing.html
								Influence	4/17/2015	China has suspended a policy that would have effectively pushed foreign technology companies out of the country's banking sector, according to a note sent by Chinese regulators to banks.	https://www.nytimes.com/2015/04/17/business/international/china-suspends-rules-on-tech-companies-serving-banks.html?_r=0
								Influence	10/30/2015	August 20, officials from the banking regulator told representatives of several Western tech firms that they would seek opinions on a new version of the bank procurement rules; October 30, the CIRC extended its comment period on the draft rules by two weeks until November 15, a move which critics of the regulations said could be significant. the China Insurance Regulatory Commission (CIRC) in October, state that insurance companies, along with their holding companies and asset managers, should prioritize the purchase of "secure and controllable" products, including domestic encryption technologies and local hardware and software.	
							Global Trade Agreement		14/6/2017	June 2017, during the WTO TBT commette meeting, the china representive responsed that the Guideline for Promoting the Application of Secure and Controllable Information Technology in Banking Sector (2014-2015) had expired	
11	Online-posting-PublicMorals-U.S	Russia is suspected to impact the 2016 U.S. election	U.S.	Russia	/	Public Morals	Express Concerns		Dec-16	In December 2016, two senior intelligence officials told U.S. news media that they were highly confident that Vladimir Putin personally directed the operation to interfere in the 2016 presidential election. Russian officials have strongly denied the allegations every time they resurfaced. when ABC News reported that U.S. intelligence officials told the news agency that Putin was directly involved in the covert operation,[28] Russian Foreign Minister Sergey Lavrov said he was "astonished" by this "nonsense"	http://abcnews.go.com/International/officials-master-spy-vladimir-putin-now-directly-linked/story?id=44210901
							Dispute		Jan-17	In January 2017, the Office of the Director of National Intelligence, representing the work of the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA) and the National Security Agency (NSA), published the following assessment: "President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments."	https://web.archive.org/web/20170413224426/https://www.dni.gov/index.php/newsroom/press-releases/224-press-releases-2017/1466-odni-statement-on-declassified-intelligence-community-assessment-of-russian-activities-and-intentions-in-recent-u-s-elections
							Restrictions on post-sales / digital services		May-17	one half of all news on Twitter directed at Michigan prior to the election was junk or fake. Facebook, until May 2017 when it announced plans to hire 3,000 content reviewers, thought that the problem could be solved by engineering	https://www.barrons.com/articles/facebook-tesla-realize-technology-cant-solve-everything-1494018925
							Dispute		Jun-17	In June 2017, Putin told journalists that "patriotically minded" Russian hackers may have been responsible for the cyberattacks against the U.S. during the election campaign. Putin continued to deny any government involvement, stating, "We're not doing this on the state level."	https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html
							Dispute		7/12/2017	Three House Democrats introduced a bill, No Cyber Cooperation with Russia Act, Wednesday prohibiting the U.S. from forming a collaborative cybersecurity initiative with Russia.	http://thehill.com/policy/cybersecurity/341689-dem-reps-introduce-bill-to-block-cybersecurity-team-up-with-russia
							Restrictions on post-sales / digital services		Sep-17	In September 2017, Facebook told congressional investigators it had discovered that hundreds of fake accounts linked to a Russian troll farm had bought $100,000 in advertisements targeting the 2016 U.S. election audience.	https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html
							Restrictions on post-sales / digital services	Influence	Nov-17	In November 2017, Google has called for America to ban foreign governments from posting election adverts after a backlash over Russian "fake news"	http://www.telegraph.co.uk/news/2017/11/16/google-ban-foreign-governments-posting-online-election-adverts/
12	VPN-Ban-China and Russia	China and Russia move to block virtual private network services, bar people from using VPNs, services that skirt censorship restrictions by routing web traffic abroad	China, Russia	/	VPN	Public Morals	Restrictions on post-sales / digital services		7/12/2017	China asked telecom companies to start blocking user access to VPNs that didn't pass government muster by next February	https://www.wired.com/story/china-russia-vpn-crackdown/
							Restrictions on post-sales / digital services		7/31/2017	Russia follows China in tightening internet restrictions, raising fresh censorship concerns. President Vladimir Putin signed the bill prohibiting virtual private networks (VPNs) and other technologies that anonymize users, according to the government's website on Sunday.	https://www.cnbc.com/2017/07/31/russia-follows-china-in-vpn-clampdown-raising-censorship-concerns.html
								Acquiescence	8/4/2017	Apple complied with a Chinese government order to remove VPNs from its Chinese iOS AppStore, "We would obviously rather not remove the apps, but like we do in other countries we follow the law wherever we do business," company CEO Tim Cook said in an earnings call on Tuesday. "We strongly believe participating in markets and bringing benefits to customers is in the best interest of the folks there and in other countries as well."; Amazon's cloud services in China this week said it would no longer support VPN use	https://www.wired.com/story/china-russia-vpn-crackdown/
13	Netbotz-Spying-Germany	Massive US-spying. Security-cameras all over the planet transmit directly to US-military with built-in	Germany	US, France	Security Camera	Military-Offensive	Export subsidies		2004	The US-based company NetBotz is selling security-cameras. These cameras are being used in high-security-areas all over the world, from Korea and Thailand to Germany, in government-installations as well in corporate installations at an unusually low price	https://www.democraticunderground.com/10141582901
							Ignore		2005	The german intelligence-service BND actively decided against reporting it to their superiors because they "feared the political implications". In 2005, the BND noticed that NetBotz is aggressively selling its cameras extremely cheap to government-departments, to corporations operating with high-tech and military hardware. And they still didn't tell anybody.	

		backdoor						Express Concerns	2016	German attorney-generals for the german counter-espionage unit BfV to find out what the BND should have reported to them in an official manner in 2015 and journalists of the german TV-show "Fakt" got their hands on documents of the BfV who mentioned this massive espionage	
14	Doll-Privacy-Germany	Banned In Germany: Kids' Doll Is Labeled An Espionage Device	Germany	US	Smart Toys	Privacy and Data	Express Concerns		12/6/2016	Complaints to regulators say that some toys collect the voices of children without permission. Over 18 privacy groups are filing complaints with both the US' Federal Trade Commission and the European Union alleging that Genesis Toys and its tech partner Nuance are violating deceptive practices and privacy laws (including COPPA) through the way certain toys record kids' voices	https://www.engadget.com/2016/12/06/internet-connected-toys-accused-of-spying-on-kids/
								Defiance	12/6/2016	Nuance, the U.S. company in question, has said in response to similar criticisms that it "does not share voice data collected from or on behalf of any of our customers with any of our other customers."	http://whatsnext.nuance.com/connected-living/speech-recognition-data-privacy/
							Restrictions on post-sales / digital services		2/17/2017	Germany's Federal Network Agency, or Bundesnetzagentur, said on Friday it was prohibiting retailers from selling My Friend Cayla, which garnered controversy last year over built-in technology that experts said allowed it to effectively spy on children. The government forbids illicit radio transmission equipment in toys.	http://www.npr.org/sections/thetwo-way/2017/02/17/515775874/banned-in-germany-kids-doll-is-labeled-an-espionage-device
15	Huawei-TelcoBan-India	Investment barriers, and blocked sales between Indian mobile phone operators and Chinese equipment firms, faced by Huawei in India, due to the concerns that foreign telecom equipment vendors, especially Chinese, may install spyware and malware that could monitor voice and data traffic and bring down networks	India	China	Huawei telecom equipment	Political Espionage	Foreign Direct Investment Barriers		2006	While Huawei already has an R&D operation in India, for instance, the Foreign Investment Promotion Board has been sitting on its application for a $60 million expansion in Bangalore to develop software for its equipment for months. At the same time, Huawei has applied for a license to bid as an equipment supplier for large-scale Indian telecom projects run by state-owned service providers MTNL and BSNL. But the Telecom Ministry, likewise, has blocked that application. According to press reports, India's Intelligence Bureau suspects that Huawei has ties to China's intelligence apparatus and military, and even performs the debugging sweeps for the Chinese Embassy in India.	
							Government Procurement Restrictions		2009	In May 2009, Bharat Sanchar Nigam Limited (BSNL), the public sector telecommunication giant, was advised by the Ministry of Defense 'not to award equipment contracts to Huawei and Zhong Xing Telecommunication Equipment Company Limited (ZTE) in the interest of national security' (Indian Express, November 1, 2009). Indian security concerns arise from the fact that the Chinese company is owned by Ren Zhengfei, a former PLA officer who is alleged to have close links with the Chinese Communist Party (CCP). Similarly, Intelligence Bureau (IB), the premiere Indian internal intelligence agency, was also concerned about Huawei and had noted "BSNL should not award contracts to Chinese companies, as these companies are known to have links with the Chinese state and security apparatus and, therefore, their presence in this critical sector has national security implications in a variety of ways'	http://www.newsweek.com/huawei-way-108201 https://jamestown.org/program/chinese-infrastructure-projects-trouble-india/
							Prohibition, Authorization, or Registration requirement		4/30/2010	the government has told mobile operators not to import any network equipment manufactured by Chinese vendors such as Huawei and ZTE. Indian officials say the ban was prompted by concerns Chinese telecom equipment could have spyware or malicious software embedded in it which could give Chinese intelligence agencies access to telecom networks in India. The ban and other regulations come less than a week after media reports that Chinese hackers had broken into the computer networks of India's security, defence and diplomatic establishment. Indian telecom companies will have to get "security clearance" from India's Home Ministry before projects are approved	
								Compromise and Influence	5/4/2010	Chinese telecoms maker Huawei Technologies is planning to meeting senior Indian officials to persuade them its equipment poses no security threat, a report said Tuesday, The move comes after New Delhi last week blocked sales between Indian mobile phone operators and Chinese equipment firms, As part of efforts to convince India it poses no security threat, Huawei has told the government it is restructuring its Indian operations so that the chairman and board of directors of the local arm will all be Indian residents. In a letter to the prime minister's office, Huawei wrote it is "not just a Chinese company" as 85% of its staff — and nearly all of its research and development workforce — in the country are Indians. "Huawei is willing to give additional information that the Indian government agencies require. This is our commitment."	http://www.livemint.com/Companies/XU5G9jsURlxXE5LmmaQExI/Huawei-seeks-India-meeting-over-telcom-ban.html
							Conformity assessment requirement	Compromise and Influence	8/2010	The Indian Government lifted its ban in 2010 after a few months of negotiation but ordered that all Chinese equipment pass extensive security checks before certification, saying vendors must allow inspection of their equipment and share design and source codes in escrow accounts. India has approved imports of Chinese telecom equipment by Indian mobile operators, Reliance Communications and Tata Teleservices. Got the approval after the Chinese firms accepted all the conditions set by India.	https://www.globaltelecomsbusiness.com/article/b11vzbjrbqn0c6/india-lifts-chinese-telecom-import-ban
16	Huawei-SecurityConcern-UK	Huawei Cyber Security Evaluation Centre to mitigaate the UK's critical networks cybersecurity concerns	UK	China	Huawei Telecom Products	Political Espionage		Compromise and Influence	11/24/2010	Huawei Opens 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." CESG, which is a part of government intelligence agency GCHQ, will oversee the testing process at the Cyber Security Evaluation Centre	http://pr.huawei.com/en/news/hw-093468-ukcenter-security.htm#.Wam82siGNt8
							Express Concerns		6/18/2013	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. Britain's national security adviser, Sir Kim Darroch, will review operations at the company's cyber-security evaluation centre – known as the Cell – in Banbury, Oxfordshire.	http://www.telegraph.co.uk/technology/news/10190026/UK-government-to-scrutinise-Huawei-cybersecurity-centre.html
								Compromise and Influence	12/17/2013	The National Security Adviser has today 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"	https://www.gov.uk/government/publications/huawei-cyber-security-review
								Compromise and Influence	2014~2017	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 mitigatec	https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2015
17	Huawei-Ban-US	Investment barriers and Ban faced by Huawei in the U.S.	US	China	Huawei Telecom	Political Espionage	Foreign Direct Investment Barriers		2/20/2008	When Huawei, in a partnership with Bain Capital, proposed to buy 3Com for $2.2 billion in 2008, the US Committee on Foreign Investment (CFIUS) raised security concerns and put the deal on hold. Huawei's stake in 3Com, which markets intrusion detection systems, would "gravely compromise" U.S. national security. The U.S. Department of Defense uses 3Com intrusion detection products	http://www.csoonline.com/article/2122321/build-ci-sdlc/security-concerns-scuttle-bain-huawei-bid-for-3com.html
							Foreign Direct Investment Barriers		10/11/2011	Worried about potential spying, the U.S. government has blocked a bid from China's telecommunications giant Huawei to help build a new national wireless network for first responders such as police, firefighters, and ambulances.	http://www.thedailybeast.com/us-blocks-china-telecom-bid-to-build-wireless-network-over-spying-concerns
								Defiance	10/11/2011	William Plummer, Huawei's vice president for external relations, tells The Daily Beast that the Commerce Department's decision was without merit.	http://www.thedailybeast.com/us-blocks-china-telecom-bid-to-build-wireless-network-over-spying-concerns
							Prohibition, Authorization, or Registration requirement		10/7/2012	the House Intelligence Committee released a report urging U.S. telecommunication companies not to do business with Huawei Technologies Co Ltd and ZTE Corp because it said potential Chinese state influence on the companies posed a threat to U.S. security. The public portion of the report didn't offer actual examples, but observers believed a major concern was the potential for future meddling by Beijing in the companies' products due to the close relationships between major Chinese firms and the government.	http://www.reuters.com/article/us-usa-china-huawei-zte/u-s-lawmakers-seek-to-block-china-huawei-zte-u-s-inroads-idUSBRE8960NH20121008
								Defiance	10/8/2012	Huawei Statement regarding HPSCI's report: 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. Even before the investigation began, the Chairman of the committee advocated to media that "I stand by my caution to the American business community about engaging Huawei technology until we can fully determine their motives'	http://pr.huawei.com/en/news/hw-194454-hpsci.htm#.WanQfMiGNt8
									10/18/2012	A US government security review has found no evidence telecoms equipment firm Huawei Technology spies for China. security vulnerabilities posed a greater threat than any links between the firm and the Chinese government	http://www.bbc.com/news/technology-19988919
							Conformity assessment requirement; Government Procurement Restrictions		3/27/2013	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. requires 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.	http://www.reuters.com/article/us-usa-cybersecurity-espionage/u-s-law-to-restrict-government-purchases-of-chinese-it-equipment-idUSBRE92Q18O20130327
								Avoidance	12/3/2013	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." Plummer told FP that "Huawei has adjusted our priority focus to markets that welcome competition and investment, like Europe," and suggested that Ren was just "making a comment on the current market environment" in the interview.	http://gizmodo.com/accused-of-spying-huawei-ceo-says-company-is-exiting-1475628703
							Attack		3/22/2014	NSA pried way into the servers in Huawei's sealed headquarters and exploit huawei's technology so that when the company sold equipement to other countries, the NSA could roam through their system to conduct surveillance	https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html
							Government Procurement Restrictions	Avoidance	10/16/2014	The Chinese firm is banned from bidding for US government contracts because of concerns over espionage. Guo Ping, the company's chief executive, said that businesses and customers in the U.S are getting a bad deal due to the fact Huawei are not in the market but added that the company would consider re-entering America if it was welcomed. Ping added that the company maintains "pretty good growth" without playing the U.S.	http://www.bbc.com/news/business-29620442
							Express Concerns		1/9/2018	AT&T walked away from a deal to sell the Huawei smartphone, the Mate 10, to customers in the United States. A group of lawmakers wrote a letter to the Federal Communications Commission expressing misgivings about a potential deal between Huawei and an unnamed American telecommunications company to sell its consumer products in the United States. It cited longstanding concerns among some lawmakers about what they said were Huawei's ties to the Chinese government. Huawei has previously released phones in the U.S. but these have been sold online rather than through carriers.	https://www.nytimes.com/2018/01/09/business/att-huawei-mate-smartphone.html?_ga=2.67962449.1726646242.1537886218-1748405356.1537886218 https://finance.yahoo.com/news/t-walks-away-deal-sell-huawei-smartphones-wsj-004358588--finance.html
								Defiance	1/10/2018	Speaking at a CES event earlier this month, Richard Yu, Huawei's consumer products chief, defended his company's record. "We serve 170 countries, and for 30 years we've proven our quality and we've proven our privacy and security protection," Yu said.	https://www.bloomberg.com/news/articles/2018-01-30/verizon-is-said-to-drop-plans-to-sell-phones-from-china-s-huawei
							Supplier Choose		1/30/2018	Verizon Communications Inc. has dropped all plans to sell phones by Chinese manufacturer Huawei Technologies Co., including the new Mate 10 Pro, under pressure from the U.S. government, according to people familiar with the matter	https://www.bloomberg.com/news/articles/2018-01-30/verizon-is-said-to-drop-plans-to-sell-phones-from-china-s-huawei

							Government Procurement Restrictions	Avoidance	8/13/2018	Huawei and ZTE technology will largely be banned from use by the US government and government contractors. The ban was signed into placed by President Trump today as a component of the much larger Defense Authorization Act	https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump
18	Huawei-InvestBan-Austria	Huawei banned from Australia broadband project, due to the concern of capability for future spying or sabotage thought no past malicious activity had been discovered	Austrilia	China	Huawei Telecom Infrastructure	Political Espionage	Government Procurement Restrictions		3/24/2012	Australia has blocked China's Huawei Technologies Co Ltd HWT.UL from tendering for contracts in the country's $38 billion National Broadband Network (NBN) due to cyber security concerns	
								Compromise and Influence	10/24/2012	Chinese technology giant Huawei has offered to provide unrestricted access to its software code as it seeks to counter negative public perceptions that it poses a security risk. Offered to set up a national cyber security centre, based on a similar concept in the United Kingdom, that would independently evaluate all overseas-made technology products. Accepted and Moved on.	
									7/5/2013	The Australian Security Intelligence Organisation has refused to say why it allowed Chinese telecommunications provider ZTE to tender for the NBN but recommended banning Beijing-based rival Huawei	https://www.itnews.com.au/news/asio-wont-be-drawn-on-ztes-nbn-tender-348999
							Prohibition, Authorization, or Registration requirement		11/1/2013	Some senior officials in the new Liberal-led Coalition government, including Communications Minister Malcolm Turnbull, had supported a review of the ban, raising expectations it would be scrapped. But Australia's new and conservative prime minister Tony Abbott has reportedly confirmed the nation's decision to ban Huawei from providing any kit to the country's national broadband network	https://www.theregister.co.uk/2013/11/01/australian_confirms_huawei_ban/
								Influence	4/28/2015	Huawei Enterprise Solutions Architect Paul Cooney said Huawei and its Australian clients had moved on to forge positive business relationships. This had seen Huawei build key national 4G infrastructure for Optus and Vodafone. At the consumer level it was providing branded handsets to all three major Australian telcos and it was actively pursuing new-age technology projects in regional Australia including using its proprietary 4G eLTE technology "regional Australia, which has suffered from expensive and older technology, was an obvious target"	http://www.theaustralian.com.au/business/technology/huawei-upbeat-about-its-growth-in-australia/news-story/3295509c5f013dd663f61a22a4e4e7d2
									11/6/2016	Fairfax Media has confirmed that NBN contractor, France's Alcatel-Lucent, used its Shanghai-based subsidiary to make fibre optical and copper components used to link homes and businesses to the network.	http://www.smh.com.au/national/revealed-chinas-communist-party-link-to-nbn-20161105-gsipc1.html
								Influence	6/5/2017	Huawei Australia appoints former NBN security head as cybersecurity officer	http://www.zdnet.com/article/huawei-australia-appoints-former-nbn-security-head-as-cybersecurity-officer/
									6/9/2017	The NBN: how a national infrastructure dream fell short. Eight years into the National Broadband Network (NBN) project, Australia has an internet speed that lags well behind many advanced economy countries – 50th in the global rankings. the NBN rollout was politically motivated and socioeconomically biased from the beginning	http://sydney.edu.au/news-opinion/news/2017/06/09/the-nbn--how-a-national-infrastructure-dream-fell-short.html
									8/1/2017	The Turnbull government has commissioned the Australia Communications and Media Authority to investigate and end the blame game between the National Broadband Network and internet service providers about who is at fault for a rising tide of customer complaints	http://www.afr.com/technology/web/nbn/government-commissions-acma-study-in-bid-to-end-nbn-blame-game-20170801-gxmr8c
							Government Procurement Restrictions		6/18/2017	Chinese firm Huawei banned from NBN supplying phones to Australia Defence	http://www.smh.com.au/federal-politics/political-news/chinese-firm-huawei-banned-from-nbn-supplying-phones-to-australia-defence-20170616-gwsne4.html
19	VOES-CrossBoarderSupplier-OECD	the Organisation for Economic Co-Operation and Development (OECD) approved the digital goods and services tax as the preferred method of taxing the growing digital economy	Norway, Iceland, South Africa, Japan, South Korea, EU, New Zealand, Russia	cross-border supplies	all digital goods and services	Economic Stability	Price-control measures		10/5/2015	It notes that because the digital economy is increasingly becoming the economy itself, it would not be feasible to ring-fence the digital economy from the rest of the economy for tax purposes. The report notes, however, that certain business models and key features of the digital economy may exacerbate BEPS risks, and shows the expected impact of measures developed across the BEPS Project on these risks. The report also describes rules and implementation mechanisms to enable efficient collection of value-added tax (VAT) in the country of the consumer in cross-border business-to-consumer transactions, which will help level the playing field between foreign and domestic suppliers. The report also discusses and analyses options to deal with the broader tax challenges raised by the digital economy, noting the need for monitoring developments in the digital economy over time.	http://www.oecd.org/tax/addressing-the-tax-challenges-of-the-digital-economy-action-1-2015-final-report-9789264241046-en.htm https://quaderno.io/blog/digital-taxes-around-world-know-new-tax-rules/
							Price-control measures		6/3/2016	President Putin signed into law VAT bill No. 244 (the "Law" or "VAT Bill"), which introduces the concept of "services provided through the Internet" or electronically supplied services ("ESS" or "electronic services") and amends the Russian place-of-supply rules for value-added tax purposes accordingly. The Law comes into effect on 1 January 2017, and completely reshapes the economics for electronic services provided by nonresident companies to Russian customers in the business- to-business ("B2B") and business-to-consumer ("B2C") segments, both with and without involvement of foreign intermediaries, such as aggregators and payment agents	https://www.lexology.com/library/detail.aspx?g=0508c5a0-db0d-4e82-9684-26f98b2ccea7
								Acquiescence	1/13/2017	The move has caused some drivers to quit Uber said Stanislav Shvagerus, head of lobby group Taxi 2018. Losing drivers is bad news for Uber, which has struggled to catch Yandex.Taxi, the market leader. Uber denies that a significant number of drivers are quitting the company. All the companies, including LinkedIn which is banned in Russia at that time registered to the VAT Bill.	https://www.bloomberg.com/news/articles/2017-01-13/uber-russian-drivers-quit-after-putin-s-tax-on-u-s-tech-giants
20	HightTech-SelfSufficiency-Russia	Russia wants to develop Self-Sufficiency due to concerns of national security after the EU and US enacted sanctions for Crimea	Russia	EU & US	Microsoft, SAP SE and Oracle Corp.	Political Espionage; Economic Stability	Sanctions/Indictments Express Concerns; Government Procurement Restrictions		9/27/2016	Russia's capital is ditching Microsoft's technology after president Vladimir Putin urged state officials and local companies to reduce their reliance on foreign technology. As a result, it is replacing Microsoft Exchange and Outlook on 6,000 computers with email systems developed by state-run carrier Rostelecom PJSC, reports Bloomberg. It may also consider installing software developed by Russia's New Cloud Technologies to replace Microsoft Windows and Office on nearly 600,000 devices. Klimenko has described Google as a "potential threat to our national security" as the company has the ability to track "everything" and won't respond to requests for information from Russian law enforcement agencies. He has also said that he wants the Russian government to switch from Windows to a Linux-based open-source OS. Putin is going after Microsoft because it is the biggest American name in information technology and because it's easy to convince Russians that the company works with the U.S. intelligence community; Moscow's government has already switched Cisco Systems Inc. technology for city surveillance cameras to local software, Yermolaev said. State media company Rossiya Segodnya and Moscow's regional government switched from Oracle database systems to open-code PostgreSQL software supported by local programmers, according to Digital Russia.	https://qz.com/793258/russias-vladimir-putin-is-replacing-microsofts-msft-products-and-servers-with-local-alternatives/
								Compromise	11/1/2016	"We don't spy on anyone. We don't work with any government to spy on others, and we never would," said Dominic Carr, Microsoft's general manager for public affairs. "We make sure governments can review our software to confirm for themselves that our products are secure. And we've worked hard to increase privacy protections for customers including by suing the US government four times.'	https://www.nbcnews.com/news/us-news/putin-wants-push-microsoft-out-russia-battle-us-n674781
21	Russia-DataProtectionLaws	Data and privacy protection	Russia	Others: US/China	Digital Services	Political Stability Privacy and Data	Restrictions on post-sales / digital services			Russian Data Protection Laws: all foreign tech companies have been required to store the past six months' of the personal data of its citizens and encryption keys within the country; which the company has to share with the authorities on demand	
								Defiance	11/11/2016	Russia's communications regulator Roskomnadzor has started to enforce a proposed block of LinkedIn in the country, after the social network failed to transfer Russian user data to servers located in the country, violating a law instituted in Russia requiring all online sites to store personal data on national servers	https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/
							Prohibition, Authorization, or Registration requirement		3/7/2017	Russia's internet regulator today confirmed that access to social networking site LinkedIn — which has been blocked in Russia since November 2016 — is not returning to Russia anytime soon, after it received a letter from the social network's VP of global public policy stating that LinkedIn will not move Russian user data to Russian territory. LinkedIn, which is now owned by Microsoft and has 6 million users in the country, told TechCrunch that it is still working on lifting the ban.	https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/
							Prohibition, Authorization, or Registration requirement		5/8/2017	Russia has blocked access to Chinese social media app WeChat, developed by Tencent Holdings, for failing to give its contact details to the Russian communications watchdog.	http://www.reuters.com/article/us-tecnent-wechat-russia/russia-blocks-chinese-social-media-app-wechat-idUSKBN18204J
								Compromise	5/11/2017	Russia unblocks China social media app WeChat. Telecoms authority announces reversal after company provided 'relevant information' for registration. Tencent said in a brief statement it was sorry about Moscow's decision and was communicating with Russian authorities over the matter. Russia requires internet service providers to register with related government bodies, but Tencent said it "had a different understanding" on this issue.	http://www.scmp.com/news/china/diplomacy-defence/article/2094004/russia-unblocks-china-social-media-app-wechat
							Identified as Trade Barrier		10/1/2017	the United States Trade Representative ('USTR') lists the data localization regulation as trade barrier in the 2017 National Trade Estimate Report on Foreign Trade Barriers	
22	Telegram-DataAccess-Russia	Telegram Agrees to Register With Russia to Avoid Ban as terrorists allegedly used the Telegram's app to communicate and plot attacks	Russia	US	Telegram	Military-CyberTerrorism	Prohibition, Authorization, or Registration requirement		6/23/2017	Russia threatens to ban Telegram if it doesn't hand over data. Russian authorities say the app supports terrorist activity.	https://www.engadget.com/2017/06/26/russia-ban-telegram-hand-over-data/
								Defiance / Avoidance	6/26/2017	Pavel Durov, the founder of Telegram, said the app was not blocked in any other countries, adding that if the app is banned in Russia then the government officials will entrust their communications to other countries' messengers	https://thehackernews.com/2017/06/russia-telegram-data-law.html
								Compromise	6/28/2017	After being threatened with a ban in Russia, end-to-end encrypted Telegram messaging app has 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. Expanding on his comments, Mr Durov told the Financial Times newspaper: "We didn't want to give the authorities a chance to block Telegram under a pretext of not providing nonsense data like the name of our company. "If they're going to block us, they'll have to do it for a serious reason.'	https://thehackernews.com/2017/06/telegram-russia-partnership.html http://www.bbc.com/news/technology-40443599

							Prohibition, Authorization, or Registration requirement		4/13/2018	Moscow court bans the Telegram messaging app over its failure to give Russian security services the ability to read users' encrypted data. The court took 18 minutes to approve the ban, and the ban was immediately taken into effect. This ruling came a month after Telegram lost a lawsuit it brought against the Federal Security Service (F.S.B.) which had demaned access to messages.	https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html
23	OnlinePayment-Licence-China	Issued licences for non-bank suppliers of online payment services to govern the increasing digital economic	China	Others	Online-pagyment Services	Economic Stability	Finance measures		2010	China issued regulations for non-bank suppliers of online payment services in 2010	
							Identified as Trade Barrier		2017	the United States Trade Representative ('USTR') lists the the licences as trade barrier in the 2017 National Trade Estimate Report on Foreign Trade Barriers arguing that as of June 2014, only 2 out of over 200 licenses were issued to foreign-invested suppliers with limited services.	
24	LocalContent-Argentine	Argentine Media Law requires the local content for the broadcast on the radio and television	Argentine	US	Online Content Services	Public Morals	Local content measures		2015	The Argentine Media Law, enacted in 2009 and amended in 2015, requires 50 percent of the news and 30 percent of the music that is broadcast on the radio be of Argentine origin. In the case of private television operators, at least 60 percent of broadcast content must be of Argentine origin. Of that 60 percent, 30 percent must be local news and 10 to 30 percent must be local independent content.	
							Identified as Trade Barrier		2017	the United States Trade Representative ('USTR') lists the the licences as trade barrier in the 2017 National Trade Estimate Report on Foreign Trade Barriers arguing that as of June 2014, only 2 out of over 200 licenses were issued to foreign-invested suppliers with limited services.	
25	Semiconductor-AcquisitionBlock-US	US blocked the Chinese acquisitions of semiconductor company Aixtron, Lattice due to the concern that product can be used for military	U.S.	China	Semiconductor	Military-Defensive	Foreign Direct Investment Barriers	Acquiescence	Oct-16	the Chinese acquisitions of the German semiconductor company Aixtron is blocked in 2016 because Aixtron has a subsidiary in the United States and its technology has the potential "military applications", including the super computer and smart phones.	https://www.nytimes.com/2016/12/02/business/dealbook/china-aixtron-obama-cfius.html
							Foreign Direct Investment Barriers	Acquiescence	9/13/2017	President Trump issued an Executive Order blocking the $1.3 billion acquisition of a U.S. semiconductor manufacturer, Lattice Semiconductor Corporation ("Lattice"), by a Chinese government-backed private equity fund, Canyon Bridge Capital Partners ("Canyon Bridge")	https://corpgov.law.harvard.edu/2017/09/24/president-trump-blocks-chinese-acquisition-of-lattice-semiconductor-corporation/
26	ExportControl-Cybersecurity-Wassenaar	debates new export controls for cyber security and surveillance tools protecting human rights activists and political dissidents from surveillance by authoritarian governments	41-countries	other-countries	"intrusion software" and "carrier class network surveillance tools."	Military-Defensive	Export-license, -quota, -prohibition, certification, and other quantitative restrictions		12/2013	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." The Wassenaar Arrangement is a multilateral export control forum for dual use goods and technology where 41 countries must come to a consensus on proposed export controls. Then, each country implements these controls under their national rules with a significant level of discretion	https://www.lexology.com/library/detail.aspx?g=fce3911a-a9c0-4dbb-87f9-601c4e594aaa
								Influence	5/20/2015	the U.S. Department of Commerce's Bureau of Industry and Security (BIS) published proposed amendments to the Export Administration Regulations (EAR) to implement stricter controls on certain cyber-security related items. The proposed rule would create new restrictions and requirements for the export of hardware, software, and technology related to "intrusion software" (but not "intrusion software" itself), requiring a license for export to all destinations except Canada. It implements the 2013 Wassenaar Arrangement control on intrusion and surveillance technologies	
								Influence	6/3/2015	the State Department's Directorate of Defense Trade Controls (DDTC) and BIS proposed revisions to U.S. export control regulations that would permit cross-border electronic transfers of export-controlled data and software without a specific export authorization, provided certain conditions are met, including securing the data or software with end-to-end encryption and ensuring that foreign persons are not given the means to decrypt such data or software.	https://www.lexology.com/library/detail.aspx?g=fce3911a-a9c0-4dbb-87f9-601c4e594aaa
								Acquiescence	9/4/2015	Hewlett-Packard (HP) and its Zero Day Initiative (ZDI) team pulled their sponsorship of the Pwn2Own hacking competition in Japan	https://www.scmagazine.com/wassenaar-arrangement-confusion-cited-as-hp-pulls-pwn2own-sponsorship/article/532500/
							Regional Agreements		3/2/2016	US officials have announced that they plan to re-negotiate regulations on the trade of tools related to "intrusion software." The rules were negotiated through the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, an agreement governing the trade of weapons and technology that could be used for military purposes.	https://arstechnica.com/tech-policy/2016/03/us-to-renegotiate-rules-on-exporting-intrusion-software-under-wassenaar-arrangement/
							Regional Agreements		12/21/2016	Wassenaar weapons pact talks collapse leaving software exploit exports in limbo. The countries did agree that command and control software for botnets should be included in the export ban.	https://www.theregister.co.uk/2016/12/21/wassenar_negotiations_fail/
							Regional Agreements		2/15/2017	Cybersecurity and the Wassenaar Arrangement — What Needs to Be Done in 2017: fashion a workable standard that strengthens cybersecurity while protecting human rights and political dissent. It is critical that those concerned about these controls step up to the plate and offer constructive solutions before the window to do so closes	http://www.steptoecyberblog.com/2017/02/15/cybersecurity-and-the-wassenaar-arrangement-what-needs-to-be-done-in-2017/
27	Microsoft-Restriction-China	Chinese Concern about Microsoft Product for provided the U.S. government back-door access	China	US	Microsoft	Political Espionage			9/4/1999	NSA Built Back Door In All Windows Software by 1999. Microsoft built in a "key" for the nation's most powerful intelligence agency to the cryptographic standard used in Microsoft Windows 95, Windows 98, Windows NT4 and Windows2000. Microsoft denied that the key belongs to the NSA, saying instead that the " NSAKEY" label simply means the cryptography architecture meets the NSA's standards for export	http://www.cnn.com/TECH/computing/9909/03/windows.nsa.02/ http://www.washingtonsblog.com/2013/06/microsoft-programmed-in-nsa-backdoor-in-windows-by-1999.html
								Acquiescence	3/25/2010	Microsoft rejected Brin's critique, saying it would continue to obey local laws on censorship in China.	https://www.theguardian.com/technology/2010/mar/25/china-microsoft-free-speech-google
							Attack		6/21/2013	Snowden divulged the NSA programs in mid-2013; Microsoft has collaborated closely with US intelligence services to allow users' communications to be intercepted, including helping the National Security Agency to circumvent the company's own encryption, according to top-secret documents obtained by the Guardian.	https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
							Government Procurement Restrictions		5/20/2014	China bans Microsoft Windows 8 on government computers. Tuesday's announcement said desktop, laptop and tablet personal computers bought for government use must use a different operating system. The brief statement gave no explanation. Microsoft wants customers to switch to Windows 8 after support for its 13-year-old Windows XP operating system ended in April. Some customers have avoided that, citing expense and inconvenience. "We aim to build products that deliver the features, security and reliability customers expect, and we're happy to answer the government's questions," Ms. Li said in an email.	https://phys.org/news/2014-05-china-windows.html https://www.nytimes.com/2014/07/29/business/microsoft-offices-in-china-are-targets-of-authorities-visits.html?mcubz=1
								Compromise	5/20/2014	Microsoft said Tuesday it would maintain efforts to gain approval in China for its Windows 8 operating system after a ban announced by Beijing."We were surprised to learn about the reference to Windows 8 in this notice," the company said in a statement, referring to a Chinese government official notice.	https://phys.org/news/2014-05-microsoft-china-windows.html
								Compromise	3/28/2016	Microsoft built a special government-approved version of Windows 10 for China. Partnering with a state-run technology and defense company, CETC, Microsoft created its specialized version of Windows, officially called Zhuangongban, to comply with governmental standards. It doesn't have all the same consumer apps and services that come with Windows 10 elsewhere and that it's equipped with additional device management and security controls.	https://thenextweb.com/microsoft/2016/03/28/microsoft-windows-10-china/#.tnw_BRlgGwuH
28	Google-Ban-China	Google left China due to the concern about China's censorship on internet content	China	US	Google	Public Morals		Compromise	2006	Google created a Chinese version of its search engine, at Google.cn, to be in a better position to profit from China's booming economy. To gain the toehold, Google complied with the Chinese government's demands for censorship of Internet search results about political dissent and other hot-button issues	http://www.nbcnews.com/id/34860435/ns/business-world_business/t/googles-threat-china-traces-back-founders/#.Wa1slsiGOUk https://www.theguardian.com/technology/2010/mar/24/google-china-sergey-brin-censorship
									9/4/2009	Kai-Fu Lee unexpectedly left to start a venture fund	
								Defiance	1/2010	Google announced that, in response to a Chinese-originated hacking attack on them and other US tech companies, they were no longer willing to censor searches in China and would pull out of the country completely if necessary	
								Defiance	3/23/2010	Google co-founder Sergey Brin has called on Washington to take a stand against China's censorship of the internet, urging the US to make the issue a "high priority". Brin, talking to the Guardian about Google's decision yesterday to lift censorship from its Chinese internet search engine, called on government and businesses to act in order to put pressure on Beijing.	
							Restrictions on post-sales / digital services		3/30/2010	searching via all Google search sites in all languages was banned in mainland China. ther Google services such as Google Mail and Google Maps appeared to be unaffected. The ban was lifted the next day.	
							Prohibition, Authorization, or Registration requirement	Avoidance	6/30/2010	Google ended the automatic redirect of Google China to Google Hong Kong, and instead placed a link to Google Hong Kong to avoid their Internet Content Provider (ICP) license being revoked	
29	Outsourcing-Prevention-EU	Indian's outsourcing preventions due to EU data restrictions	EU	India	Outsourcing	Data and Privacy Protection	Prohibition, Authorization, or Registration requirement		Oct-98	Under the E.U. Data Protection Directive, personal data cannot be transferred from an E.U. member state to a country not in the E.U. unless that nation's laws are adequate: Switzerland, Israel, Canada, Argentina, Guernsey, the Isle of Man and the U.S. Uruguay	
							Bilateral Agreements		9/13/2012	India has demanded that the E.U. award it data-secure status similar to the U.S. safe harbor agreement. European Union's decision to examine if it's "data secure" before committing to bilateral free trade agreement aimed at boosting outsourcing flow between region and India	http://www.pcworld.com/article/262278/india_pushes_eu_for_datasecure_status.html
							Bilateral Agreements		4/4/2016	New Delhi has demanded that the European Union lift restrictions on flow of sophisticated outsourcing business to India by designating it as a data secure country. This however does not seem imminent. "The evaluation that we made of the Indian proposal was that, yes, it would be difficult to accommodate the way it was expressed," Mr. Rosario said. India has also been keen to obtain 'data secure' nation status from the EU, a classification that is crucial for the development of its IT and ITES sectors in Europe. This is one of the topics where we would be willing to narrow down the gaps between the sides, when things move ahead, when things move ahead and our representatives are able to sit down together," Mr. Rosario said.	http://www.thehindu.com/business/Industry/eu-had-offered-india-gradual-asymmetric-elimination-of-tariffs/article8524692.ece

30	Data-Agreement-EU & US	EU-U.S. data flows and data protection	EU	US	Data-transfer related products	Data and Privacy Protection	Bilateral Agreements Conformity assessment requirement		2000	the EU-US Safe Harbour Agreement, which was approved by the EU in 2000, allows data transfer between the EU and the US	
									1/8/2013	Europeans were previously alarmed by the fact that the PATRIOT Act could be used to obtain data on citizens outside the United States. But this time the focus is a different law—the Foreign Intelligence and Surveillance Amendments Act—which poses a "much graver risk to EU data sovereignty than other laws hitherto considered by EU policy-makers, EU citizens and businesses are warned against using the cloud over the risk that U.S. law enforcement and intelligence agencies can obtain your personal records. Here's how the U.S. can acquire your data, even if you're based in the EU. In January 2013, Gus Hosein, head of the UK-based NGO Privacy International, declared that US surveillance and spying agencies' possible access to EU citizens' data stored in US companies' clouds is "an irreversible loss of data sovereignty."	http://www.slate.com/blogs/future_tense/2013/01/08/fisa_renewal_report_suggests_spy_law_allows_mass_surveillance_of_european.html https://www.cbsnews.com/news/patriot-act-can-obtain-data-in-europe-researchers-say/
							Express Concerns		6/14/2013	Brussels has declared the FISAA a 'grave risk' to data protection and citizens' rights	https://www.bestvpn.com/if-europeans-think-their-data-is-safe-from-the-nsa-they-should-think-again/
							Bilateral Agreements		7/2016	The Umbrella Agreement, which came into force on 1 February this year, is a big improvement compared to the past situation when our information exchanges were subject to fragmented and often weak protections which caused legal uncertainty and exposed them to legal challenges. The Privacy Shield – like the Umbrella Agreement in the law enforcement area – shows that it is possible to bridge those differences. I am pleased to see that a growing number of US companies have endorsed this framework. Almost 2,000 of them have already signed up to the Privacy Shield	http://europa.eu/rapid/press-release_SPEECH-17-826_en.htm
							Bilateral Agreements		6/12/2016	the U.S.-EU Safe Harbor Framework was sentenced as "invalid" on October 6, 2015, the EU-U.S. Privacy Shield Framework was approved on July 12, 2016	http://www.silicon.co.uk/e-regulation/surveillance/privacy-shield-legal-challenge-199649?inf_by=59a9e3f0681db8ea648b47e2
									2017	Turning back to the protection of personal data, our revised General Data Protection Regulation will come into force in 2018.	http://europa.eu/rapid/press-release_SPEECH-17-826_en.htm
31	Tech-Procurement-China	The number of approved foreign tech brands on China's purchase list fell by a third due to the concerns about national cyber security	China	Others	Cisco, Apple, McAfee, etc.	Political Espionage	Cyber Attack		5/15/2014	the NSA intercepted Cisco routers to install surveillance equipment without the company's knowledge, which Cisco CEO John Chambers later complained about to President Obama.	https://www.infoworld.com/article/2608141/internet-privacy/snowden--the-nsa-planted-backdoors-in-cisco-products.html
							Government Procurement Restrictions		2/26/2015	Cisco said afterwards [Snowden] its China business had slowed to a crawl, in part because its IT-equipment was associated with spying. Cisco Systems Inc, had none left by late 2014, Smartphone and PC maker Apple Inc has also been dropped over the period, along with Intel Corp's security software firm McAfee and network and server software firm Citrix Systems, The number of approved foreign tech brands fell by a third, while less than half of those with security-related products survived the cull.	http://www.reuters.com/article/us-china-tech-exclusive/china-drops-leading-tech-brands-for-certain-state-purchases-idUSKBN0LV08720150227 http://fortune.com/2015/02/26/why-china-is-making-life-miserable-for-big-u-s-tech/
32	Apple-DataCenter-China	Apple sets up China data center to meet new cyber-security rules	China	US	Apple	Data and Privacy Protection	Restrictions on post-sales / digital services		4/11/2017	The Cyberspace Administration of China (CAC) issued draft measures for implementing the data localisation provisions under the Cybersecurity Law of China (Cybersecurity Law) and the National Security Law of China on 11 April 2017. "Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data Overseas"	http://www.dataprotectionreport.com/2017/05/cross-border-data-transfers-china-issues-new-measures-to-strengthen-data-localisation/
								Acquiescence	6/12/2017	The U.S. technology company said it will build the center in the southern province of Guizhou with data management firm Guizhou-Cloud Big Data Industry Co Ltd. Apple is the first foreign firm to announce amendments to its data storage for China following the implementation of a new cyber-security law on June 1 that requires foreign firms to store data within the country. Other foreign firms that oversee cloud businesses, including Amazon.com Inc and Microsoft Corp, already have data centers in China.	https://www.reuters.com/article/us-myanmar-rohingya/explosions-rock-myanmar-area-near-bangladesh-border-amid-rohingya-exodus-idUSKCN1BF0FJ
							Global Trade Agreement		6/14/2017	The U.S., Japan, EU, Australia, Canada expressed the specific trade concerns on the WTO TBT Committee. China representive responed that data storage and other similar matters were beyond the scope of the TBT Agreement	
33	ZTE-ExportControl-US	ZTE Corp alleged violations of U.S. export controls on Iran	US	China	ZTE	Military-Defensive	Export-license, -quota, -prohibition, certification, and other quantitative restrictions	Avoidance-Pretend to comply	2012	Reports by Reuters in 2012 that the company had signed contracts to ship millions of dollars worth of hardware and software from some of America's best-known technology companies to Iran's largest telecoms carrier, Telecommunication Co of Iran (TCI), and a unit of the consortium that controls it	https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending
							Sanctions		3/6/2016	The U.S. Commerce Department is set to place export restrictions on Chinese telecoms equipment maker ZTE Corp (000063.SZ) for alleged violations of U.S. export controls on Iran. The restrictions will make it difficult for the company to acquire U.S. products by requiring ZTE's suppliers to apply for an export license before shipping any American-made equipment or parts to ZTE	http://www.reuters.com/article/us-zte-usa-china/u-s-commerce-department-to-place-restrictions-on-chinas-zte-idUSKCN0W80AV
								Acquiescence	3/7/2017	ZTE Corporation Agrees to Plead Guilty and Pay Over $430.4 Million for Violating U.S. Sanctions by Sending U.S.-Origin Items to Iran	https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending
34	ba-MoneyGran	Ant Financial was blocked from buying MoneyGram	US	China	MoneyGram				1/2/2018	MoneyGram plunges after US denies a proposed merger with Alibaba financial services affiliate	https://www.cnbc.com/2018/01/02/ant-financial-moneygram-deal-off-mgi-stock-falls.html