A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade

Keman Huang
Renmin University of China, and
MIT
Stuart Madnick and Nazli Choucri
MIT
Fang Zhang
Tsinghua University, and
Harvard University

Research Article

Abstract

Governing cybersecurity risks from digital trade is a growing responsibility for governments and corporations. This study develops a systematic framework to delineate and analyze the strategies that governments and corporations take to address cybersecurity risks from digital trade. It maps out the current landscape based on a collection of 75 cases where governments and corporations interact to govern transnational cybersecurity risks. This study reveals that: first, governing cybersecurity risks from digital trade is a global issue whereby most governments implement policies with concerning that the cybersecurity risks embedded within purchasing transnational digital products can influence their domestic political and societal systems. Second, governments dominates the governance interactions by implementing trade policies whereas corporations simply comply. Corporations do, however, have chances to take more active roles in constructing the governance system. Third, supply chain cybersecurity risks have more significant impacts on governance mode between governments and corporations whereas concerns on different national cybersecurity risks do not. Fourth, the interactions between governments and corporations reveal the exisitence of loops that can amplify or reduce cybersecurity risks. This provides policy implications on transnational cybersecurity governance for policy makers and business leaders to consider their potential options and understand the global digital trade environment when cybersecurity and digital trade overlap.

Policy Implication

- The governance of cybersecurity risks from digital trade is genuinely a global governance issue. Understanding cybersecurity within digital trade is no longer just an option, but a must, for policy makers and business leaders.
- Governments mostly take actions as buyers regarding cybersecurity risks from digital trade, with a primary focus on their domestic political and societal system, while they can be lacking the capability to mitigate such risks. Facilitating the cybersecurity capability building is an essential task that the international community should promote.
- The governance practices are diverse, with a mainstream pattern where governments implement import-related trade policies and corporations take reactive actions. However, corporations have opportunities to shape the cybersecurity governance mode. Therefore, developing platforms effectively engaging both governments and corporations should be the operational bias for the global cybersecurity governance schema construction.
- Different national cybersecurity risks do not significantly impact digital trade governance for cybersecurity, while the supply chain cybersecurity risks do. Hence, when considering the global cybersecurity governance, the community should pay more attention to the supply chain cybersecurity risk management perspective.
- The interactions between governments and corporations can amplify or reduce the cybersecurity risks from digital trade, with the cyber trade norms development platform and corporate responsibility commitment mechanisms playing critical gateway roles to shape the direction. Hence, it is valuable to distinguish adopted, negotiable, or conflicting cyber trade norms to guide the cyber trade norm development, and investigate how corporations design their strategies and take a more active role to depoliticize the transnational cybersecurity risks.

1. Introduction: the challenging transnational governance for cybersecurity risks from digital trade

Digital trade, defined as transactions of products and services which are digitally ordered, enabled or delivered (OECD-IMF, 2018), has become a driving engine of global economic growth. In essence, almost any product or service that contains or uses information technologies constitutes digital trade. Concomitantly, the cybersecurity weaknesses rising from digital technology (Hua and Bapna, 2013) pose a growing risk for any digital trade. This risks become especially challenging when trades occur across national boundaries (Madnick et al., 2019). Managing such cybersecurity risks is becoming a strategic task for governments and corporations (Choucri and Clark, 2019; Jalali et al., 2019).

However, global norms are absent in addressing cybersecurity risks. Cybersecurity policies are inconsistent or conflict across countries, hindering efforts to mitigate growing global cyber risks (Azmeh et al., 2019). Meanwhile, big countries expand their jurisdiction and enforce their influences on other countries in cyberspace (Lambach, 2020). This results into the abuse of the 'national security exceptions' principle (Voon, 2019), which can dismantle the international trade system.

Most governments lack sufficient cybersecurity capability (Manjikian, 2010), and private sectors have stronger control over the cyberinfrastructures (Carr, 2016). Therefore, public–private partnerships is considered as the operational basis for cybersecurity governance (Abbott et al., 2016; Boeke, 2018; Carr, 2016; Christensen and Petersen, 2017; Naseemullah and Staniland, 2016; Weiss and Jankauskas, 2019). For transnational digital trade, cybersecurity governance is challenged by the overlap of cyber territories whereby home and host governments both attempt to influence; the inconsistent interests among home and host governments, corporations, and international organizations (Christensen and Petersen, 2017; Eduardsen and Marinova, 2020; John and Lawton, 2018; Lambach, 2020); and the uneven cybersecurity capability among different vendors (ITU, 2019), resulting into much more diverse and complex governance practices.

This study aims to develop a systematic framework to delineate and analyze *how governments and corporations interact to address cybersecurity risks embedded in digital products/services from digital trade*. Specifically, this study explores the following three key questions:

- **RQ1**: What are the cybersecurity risks from digital trade, and who raises the concerns?
- **RQ2**: What strategies do governments and corporations use to manage these risks, and what governance modes emerge through their strategic interactions?
- **RQ3**: How do different cybersecurity risks from digital trade and governance modes influence each other?

To answer these questions, this study first develops a systematic framework based on a thorough literarature review. Then we use it to analyze the modes of governments and corporations in addressing cybersecurity risks by developing a unique collection of 75 cases with 228 events crossing 31 different nations. The results reveal that governancing cybersecurity risks from digital trade invovles global and diverse efforts, clarifying the misperception that it is only an issue among the US, China and Russia. Governments mostly implement trade policies from the views of digital product/service buyers. They are concerned that cybersecurity risks in digital trade may influence their domestic political and societal systems. Though cyberspace's complexity gives much power to corporations (Eriksson and Giacomello, 2006), governments dominate the interaction by implementing trade policies with which corporations comply most of the time. The supply chain cybersecurity risks can significantly shape the transnational cybersecurity governance mode while national cybersecurity risks have little impacts. Corporations can have a more active role when cybersecurity risk is raised by governments where the digital products are from. Importantly, the dynamics of interactions between governments and corporations demonstrate a reinforcement loop of strategies that amplify cybersecurity risks and a balancing loop that reduces them.

This study provides two contributions to the existing literature on transnational cybersecurity governance. First, this article offers the first systematic framework for transnational cybersecurity governance based on various strategies and the interaction patterns between governments and corporations. Second, we build up a collection of cases to map out the interactions between governments and corporations, providing a panoramic view of the transnational cybersecurity governance practices. Third, we reveal how the context, the cybersecurity risks from digital trade, and different governance modes impact each other. These conceptual and empirical insights identify the critical gaps that policy makers and business leaders need to bridge to construct a more effective and sustainable governance schema for the digital trade system.

2. Theoretical background

2.1. Interactions between cybersecurity and digital trade

Cybersecurity is the ability of an actor (either a government and corporation) to protect itself and its institutions against cyber risks (Choucri and Clark, 2019; Helfat and Peteraf, 2003). Effective cybersecurity governance goes beyond cyber securing an institution's internal system, to protecting its global supply chain as a whole (Madnick, 2019).

Digital products and services now rely heavily on global supply chains (Boyson, 2014). Nations are beginning to territorialize cyberspace as national cyber territory, thereby expanding their jurisdiction into cyberspace (Lambach, 2020). Some governments, like the US and EU, are extending their influences to third countries through laws and regulations over cyberspace to gain extraterritorial jurisdiction (Daskal, 2018). One example is the EU General Data Protection Regulation (EU GDPR), which applies to any data controllers and processors involving data subjects within the European Economic

Area (EEA), regardless of whether the processing takes place within EEA or not (Bendiek and Römer, 2019). Governments increasingly delegate the enforcement of laws to corporations domestically but achieve states' extraterritorial oversight goals through the corporations' global reach. For example, the US Clarifying Lawful Overseas Use of Data Act (US CLOUD Act) required all US-based technology companies to provide requested data stored on their servers regardless of where the data are stored, to comply with the CLOUD Act. States' assertions of their cyber territory transnationally using international corporations as the intermediary can create dispute and distrust between nations. Due to difficulty in identifying all potential vulnerabilities, lack of trust among governments amplifies the perceived national cybersecurity risks from digital trade.

Therefore, cybersecurity risks from digital trade includes cybersecurity risks from the global digital supply chain and national perceptions that such risks can influence national cybersecurity.

2.2. Cybersecurity governance through public private partnerships

Transnational governance refers to various institutionalized modes of collective action for managing transnational issues and ensuring the provision of collective goods, which involve state and non-state actors (Abbott and Snidal, 2009). Generally, most transnational governance initiatives are carried out through indirect governance (Abbott et al., 2020), such as delegation and orchestration (Abbott et al., 2016). Private sectors, especially corporations, are playing critical roles in international regimes (Haufler, 1993). Scott (2004) emphasized a nonhierarchical governance mode providing alternative policy tools beyond enforced law. In cybersecurity area, private sector plays a crucial role as it controls critical cyber infrastructure and is considered best equipped to respond to an evolving cyber risk (Kuerbis and Badiei, 2017). For example, Google controls about 90 per cent of the Internet search market. Facebook occupies two thirds of the global social media market and is the #1 social media platform in more than 90 per cent of the world's economies. Hence, an effective public private partnership is critical to secure cyberspace (Carr, 2016; Christensen and Petersen, 2017; Weiss and Jankauskas, 2019).

Verhulst and Price (2005) suggested two diametrically opposite ideal types of public private partnership: (1) the concerted mode where the state sets the legal and regulatory backdrop for rulemaking and enforcement; and (2) the voluntary mode with entirely self-regulatory and low levels of institutionalization. Using the case studies of online content regulation and personal data privacy protection in the US and the EU, Newman and Bach (Newman and Bach, 2004) distinguished two self-regulatory modes, including the legalistic self-regulation where the government induces self-regulation through the threat of stringent formal rules and costly litigation should industry fail to deliver socially desired outcomes, and the coordinated self-regulation where public sector representatives meet with industries and agree on a joint course of action. Treib et al. (2007) distinguished governance modes according to politics (referring to actor constellations), polity (referring to institutional properties), and policy (referring to instruments at the disposal of regulatory actors). Using the governance of the Internet country code Top-Level Domains (ccTLD) in the EU as a case, Christou and Simpson (2009) investigated how states have aimed to assert public interest governance authority in a system initially absent of its influence. By considering an incentivized adoption option for public private partnership and mapping the meta-governance activities into the public private partnership, Shore et al (2011) developed an enhanced taxonomy to provide a structured assessment of the requirements for a comprehensive cybersecurity strategy for New Zealand. Bossong and Wagner (2017) proposed the topology of public private interactions based on different layers of content and users, and the functions of information sharing and active assistance and then applied it to study the EU's efforts to develop public private partnership for cybersecurity.

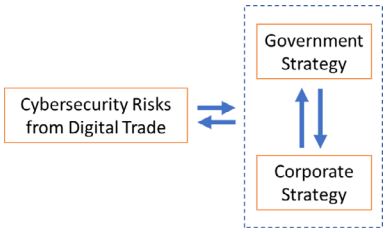
Provan and Kenis (2008) identified three network-governance modes to describe how different actors interact to govern actitivies within a networked environment: the participant- governed mode where members are highly equal; the lead-organization-governed mode where one actor coordinates the activities and decision makings within the network; and the network-administrative mode where one actor takes the authority to control the network's activities. Boeke (2018) demonstrated that the network governance modes for cyber crisis management can vary due to different institutional arrangements. Weiss and Jankauskas (2019) showcased the delegation and orchestration modes between governments and corporations in cybersecurity capability building. Through an analysis of Danish cybersecurity public private partnerships, Christensen and Petersen (2017) highlighted the disagreement between public and private actors on cybersecurity and emphasizes the importance of loyalty public private partnership. Through the analysis of the Initiative for the Integration of Regional Infrastructure in South America (IIRSA), Agostinis and Palestini (2020) showed that delegation, orchestration, and direct intergovernmental governance can evolve to each other.

While these studies provide fruitful frameworks to investigate transnational governance for cybersecurity risks from digital trade, most of them focused on the strategies taken by governments while the corporate strategies are overlooked. Also, the existing studies are built on a limited amount of cases that cannot provide a panoramic view to understand how different governance modes are being adopted. Additionally, little research explores how the context, like the cybersecurity risks from digital trade in this study, and different governance modes impact each other.

3. Conceptual model and methodology

As shown in the conceptual model in Figure 1, the cybersecurity risks from digital trade will drive governments and corporations to take various strategies to mitigate them. The misaligned interests and incommensurate cybersecurity

Figure 1. The conceptual framework for the governance of cybersecurity risks from digital trade.



capabilities between governments and corporations make their interactions more complicated. As their strategies can converge or diverge when responding to the embedded cybersecurity risks, the governance modes can further influence the cybersecurity risks within the digital trade.

Following this conceptual model, this study investigates different cybersecurity risks from digital trade and the diverse strategies that governments and corporations respond to these risks through a literature review, which together lead to a systematic taxonomy shown in Figure 2. Detailed discussion on different cybersecurity risks, governments and corporations strategies, and the governance modes emerging from their interactions are in Sections 4, 5, and 6 seperately. The research further identifies 75 cases related to cybersecurity within digital trade from the Technical Barriers to Trade (TBT) Information Management System (TBT IMS), the ECIPE Digital Trade Estimates (DTE) database, public reports and workshop discussions. Then the developed taxonomy is applied to categorize these cases, revealing how cybersecurity risks from digital trade and governance modes impact each other. The detailed analysis based on these cases is in Section 7.

4. Cybersecurity risks from digital trade

As discussed above, there exists two types of cybersecurity risks from digital trade, namely national cybersecurity risk and supply chain cybersecurity risk. This section dicusess each types of these risks, citing emperical cases from our database to elaborate them. The case is listed in a parenthese with a number. The detailed of the case is available within the support materials.

Figure 2. The taxonomy for representing the governance of cybersecurity risks within digital trade.

4.1. National cybersecurity risk

Governments emphasize different components of national cybersecurity risks. For instance, the US and UK national cybersecurity strategy focuses on three national cybersecurity components, including individual cybersecurity, business cybersecurity, and internet cybersecurity (Carr, 2016). North Atlantic Treaty Organization (NATO) identified five verticals of national cybersecurity, including military cyber capability, counter cybercrime, intelligence and counter-intelligence focusing on cyber espionage, critical infrastructure protection, national crisis management, and internet governance (Klimburg, 2012). Klimburg (2012) and Christensen and Petersen (2017) highlight societal risk from using technologies to disrupt economic, social, and political stability. Integrating these definitions, this study classifies national cybersecurity risks into four national cybersecurity risks: military, economic, political, and societal.

1. *Military cybersecurity risk* refers to the possibility of introducing cyber-attack vectors into the military system. It creates concerns about the military's cyber operation capabilities. One example is that the US Army prohibits using Chinese made DJI products in August 2017 because potential vulnerabilities in the DJI drone products could put the military's operation at risk (Case #1). Military cybersecurity risk can also come from improved adversarial cyber offensive capability when an adversary can access confidential information or sensitive technology. For example, the Chinese acquisition of a German semiconductor company Aixtron in 2016 was blocked by the US as Aixtron had a subsidiary in the US and its technology had potential military applications (Case #3).
2. *Economic cybersecurity risk* deals with the business, finance, and economic network (Albert and Buzan, 2011). The US has repeatedly emphasized controlling and punishing cyberattacks that involve economic espionage, like cyber theft of intellectual property and trade secrets. Another view on economic cybersecurity risks focuses on economic stability, as cybersecurity incidents can result in the lack of substitutability, loss of confidence, and data integrity (Kshetri, 2016). For example, China once required international IT service providers to turn over source code if selling IT systems to Chinese banks, concerning cybersecurity risks within the financial system (Case #14).
3. *Political cybersecurity risk* refers to the risk that cyberspace can be used to steal a government's secret information or impact the government's political authority, governing capability, and citizens' fundamental political self-concepts (Lane et al., 2019). One manifestation is political espionage. Since 2017, the US Department of Defense (DoD) suspected that the Russian government used Kaspersky Lab products to carry out espionage practices (Case #6). Another risk is that cyberspace can be used to spread hate speech, separatism and extremism, and other misinformation, which would threaten political stability (Case #48).
4. *Societal cybersecurity risk* involves risks to collective societal identities and value. For example, organized social media manipulation campaigns have been widely used to shape public attitudes (Howard and Bradshaw, 2018). Also, protecting civilian's privacy and regional culture has become an essential responsibility for many nations. For example, the Argentine Media Law requires 50 per cent of the news that is broadcast on the radio to be of Argentine origin (Case #58).

4.2. Supply chain cybersecurity risk

Following the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) framework, there are two types of supply chain cybersecurity risks.

1. The main risk for *buyers*, who use digital products and services, is that the supply chain can become an attack vector that attackers can exploit. For example, foreign states may abuse antivirus software to introduce surveillance equipment into their users' information systems. Hence, China implemented limitations for foreign antivirus software such as Russian-based Kaspersky and US-based Symantec in government procurement (Case #19).
2. For *suppliers*, protecting organizational digital assets such as trade secrets or intellectual property embedded in their global value chain is a common interest (Inkpen et al., 2019). Some suppliers and buyers may be in regions where cybersecurity practice is flawed, and these entities can become weak links for the whole supply chain. A typical example is that the Bangladesh Bank cyber heist took place in 2016 when the hackers succeeded in exploiting the weaknesses in Bangladesh Bank' access to the SWIFT global payment network, resulting in 81 million dollars stolen from the Bangladesh Bank (Case #65).

5. Strategies for addressing cybersecurity risk from digital trade

5.1. Government strategies

We followed the approach of previous work (Assaf, 2008; Shore et al., 2011) to identify three main strategies of governments to address cybersecurity risks from digital trade: information disclosure, trade policies implementation, and cyber trade norm development. Each cetergory can be further divided. For instance, we further divide the trade policies implementation to export-related and import-related by referring to the non-tariff barrier category from the United Nations Conference on Trade and Development (UNCTAD, 2012). Note that government can choose to do nothing especially when such risks are not publicly known or considered critical.

Information Disclosure refers to the government's use of oral or non-mandatory guidance to share information and direct private actions on cybersecurity issues. Governments can adopt a wide range of postures, including:

- *Express concern or offer recommendations* to increase cybersecurity awareness. In other words, governments focus on orchestrating market transactions and mobilize

cybersecurity capability building but with limited involvement (Weiss and Jankauskas, 2019). This is a middle way between totally hands-off and interventionist by coordinating authorities and industries.

- *Blame as trade barriers*. Governments can also list cybersecurity-related policies implemented by other nations as trade barriers, impacting the corporations' strategies before entering the market. This strategy may push the host nations to modify the listed trade policies, improve market access, and reduce risks for corporations. For example, the United States Trade Representative ('USTR') will annually identify and report the digital trade barriers implemented by other countries.

Taking an interventionist strategy, governments can implement trade policies to regulate import and export activities to manage the inherent cybersecurity risks:

- *Import-related trade policies*. The most common measure is to set prohibition, authorization, or registration requirements to regulate imports of products or services. Maintaining a blacklist to avoid the potential cyber risk from specific transnational offerings has been an increasingly popular approach. This can further turn into sanctions or indictments as a 'deterrence' approach for cyber espionage or coercive actions (Sheldon Whitehouse et al., 2017). Another manifestation is requiring specific testing and inspections or certifying the security assertion before entering the markets. One example is the requirement for information traceability, where the importer needs to offer 'log-level' detailed information on the products.

Government procurement restrictions are also common, as these policies are much easier to enact and process than other kinds of restrictions. Large government contracts will have the power to define cybersecurity-related standards that impact the private sectors.

Governments can implement foreign investment regulations to place limitations on foreign equity participation and access to government-funded research and development programs (John and Lawton, 2018). The most specific example is the US foreign investment risk review modernization act of 2018 (FIRRMA), which explicitly requires the Committee on Foreign Investment in the United States (CFIUS) to evaluate the cybersecurity risks from a transaction.

The restrictions on post-sales and digital services set requirements on the products or services which are already in the domestic market. The most relevant regulations are data localization requirements (Selby, 2017), whereby governments require data to be stored in the local jurisdiction. Another typical practice is mandatory intellectual property disclosure. For example, testing source codes is suggested as one of the best practices for supply chain cyber risk management. However, the disclosure of source codes can raise concerns regarding intelligent property protection.

- *Export-related trade policies*. Export-license, -quota, -prohibition, -certification and other quantitative restrictions can control export numbers or even prohibit certain exports. For example, Huawei Technologies and its affiliates were added into the BIS 'Entity List' in 2019 (Case #2), which bans US firms, including Google, Microsoft, Apple, and Qualcomm, from doing business with Huawei.

Another type of export-related trade policy is 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. One interesting example is the then-US company Netbotz who sold security cameras with a built-in backdoor at extremely low prices to government departments and corporations operating with high-tech and military hardware (Case #30).

Governments can promote international regime development for digital trade to develop a global cyber trade norm and harmonized trade policies for cybersecurity:

- *International organizations like the World Trade Organization (WTO)*. Though the impact of cybersecurity on international trade has not always been considered for WTO, regulations dealing with cybersecurity can be addressed by the Technical Barriers to Trade (TBT) Committee. The General Agreement on Trade in Services (GATS), the General Agreement on Tariffs and Trade (GATT), WTO Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, and WTO e-commerce negotiations also intend to develop digital trade rules at the WTO.
- *Free trade agreements (FTAs) and bilateral dialogue mechanisms*. Bilateral and multilateral/regional trade agreements have been promising platforms to build cybersecurity rules through digital trade. For example, the United States–Mexico–Canada Agreement (USMCA) explicitly includes a chapter focusing on cybersecurity and proposes a risk-based approach to manage cybersecurity risks in the trade system (Case #66). Note that several bilateral-dialogue mechanisms have been developed over these years to deal with increasing cybersecurity risks, but their effectiveness varied.

5.2. Corporate strategy

Based on how corporations involved in the trade policy implementation process, there exists three corporate strategies, which can further divided.

Drawing on Oliver's strategic institutional pressures responses framework (Oliver, 1991), we identify three strategies that corporations have to react to trade policies:

1. *Accept policy as a whole or quit the market*. When the institutional systems are relatively well-defined (John and Lawton, 2018), a corporation will accept or pretend to comply with the cybersecurity-related regulations as a whole to access the market. When the market is relatively small, or complying with such policy is too costly, or the institutional pressures from the home or host state are too intense, a corporation can choose to exit the market. Google's withdrawal from China in 2010 (Case #18) and Huawei's quitting from US telecom market in 2014 (Case

#2) are two typical examples of such avoidance. Corporations may dismiss or challenge the cybersecurity policies implemented by the host state. For instance, LinkedIn stated that they would not follow Russian's requirement to move Russian user data to Russian territory (Case #41).
2. *Negotiate with the host state to change policies*. Corporations can negotiate with governments to refine policies for their interests. This strategy can be more effective when dealing with governments having weak governmental structures or unclear institutional systems regarding cybersecurity governance. Some ban–overturn cases indicate the importance of effective negotiations between corporations and governments: Indonesia removed its ban on Chinese video app Tik Tok in 2018 (Case #24); United Arab Emirates (Case #48), Saudi Arabia (Case #49), and Pakistan (Case #50) rescinded the restriction of BlackBerry in 2010.
3. *Involve home state government to push policy changes in host state*. Corporations can use an active approach to collaborate with both their home and host states to mitigate the regulations' negative impact. Regarding the requirement to turn over source codes for testing if selling IT systems to Chinese banks (Case #14), EU and US companies had asked their governments for urgent help in stopping such policy. The US trade representative took up this issue in informal talks with Chinese regulators and brought it into the WTO TBT discussion. Finally, China proposed a new regulation without the requirement of source code disclosure.

As suggested by the resource dependency theory (Hillman et al., 2009), corporations can take a more active strategy and supplement the existing institutional structures (Dorobantu et al., 2017):

- *Commit to cybersecurity responsibility*. Corporations can actively take cybersecurity responsibility by committing to mitigate cybersecurity risks within their global supply chain. For example, in September 2017, Facebook told congressional investigators it had discovered hundreds of fake accounts linked to a Russian troll farm which had bought $100,000 in advertisements targeting the 2016 US election audience (Case #7).
- *Promote international standard adoption*. Corporations can develop consortiums to initiate digital trade policies where governments fail to see and then sell these policies to governments or international organizations. For example, on 9 August 2017, ten major cybersecurity companies in the US wrote to the US Trade Representative, suggesting incorporating cybersecurity into the free trade agreement negotiation (Case #66).
- *Help build national cybersecurity capability*. Another strategy for corporations is improving their governments' capacity to manage the potential cyber risks, especially those directly related to their products and services. For example, Huawei opened the Huawei Cyber Security Evaluation Centre (HCSEC) UK in 2010 and then assisted in establishing the HCSEC Oversight Board in 2014, in mitigating risks to UK national security (Case #33).

There exist two types of risk management efforts in the global supply chain. The two efforts are not exclusive but can be adopted simultaneously:

1. *Cyber supply chain auditing & vendor management*. Organizations are demanding stronger security functionality in the IT procurement process to prevent introducing cyber attack vectors through their global supply chains. Some critical infrastructure organizations perform in-depth vendor security due diligence, making IT procurement decisions based on the auditing result and protecting the external IT relationship with strong security policies and proactive oversight.
2. *Cyber-security practices baseline establishing*. To mitigate the cyber risk from the global supply chain as a whole, some organizations, particularly the dominant market players, use their power to establish a cybersecurity baseline through their global supply chain. SWIFT designed the Customer Security Controls Framework (CSCF) and required each organization to comply with this framework to secure the SWIFT-related infrastructure (Case #65).

6. Cybersecurity governance mode

Public-private partnerships have been the cornerstone for cybersecurity governance (Carr, 2016; Christensen and Petersen, 2017; Weiss and Jankauskas, 2019). The national and corporate strategies described above however are not a one-to-one correspondence. For example, when governments take the 'trade policy implementation' strategy or the 'cyber trade norms development' strategy, corporations can both use the 'institutional pressure response' strategy. When governments use the 'information disclosure' strategy, corporations can take the 'cybersecurity management supplement' or 'supply chain cybersecurity management' strategy.

Therefore, unlike other studies (Boeke, 2018; Christou and Simpson, 2009; Shore et al., 2011) focusing on the strategies taken by governments, this study focuses on the interactions between governments and corporations. Based on what strategies governments and corporates can take, we can draw four basic governance modes as shown in Figure 3. We further adopt Provan and Kenis's (2008) networked governance theory to categorize the interaction pattern within each mode, enabling us to identify who, the government or corporation, take the leading roles:

- *Cyberspace Compliance Requirements*. Within this mode, governments implement trade policies, individually or through international collaboration, to manage cybersecurity risks from digital trade with which corporations need to comply. Intuitively, governments take the leading role, and corporations use the 'Institutional pressure response' strategy, while the networked governance mode is the network-administrative mode.
- *Government Lead with Corporation Consultancy*. Corporations are invited to help refine polices developed by the government. So the trade policy represent to some extent balance between the nation and corporation

Figure 3. The governance modes for cybersecurity risks from digital trade.

		Corporate Strategy		
		Supply Chain Cybersecurity Management	**Cybersecurity Management Supplement**	**Institutional Pressure Response**
Government Strategy	**Do nothing**	Corporation Driven Governance	Responsibility Delegation	/
	Information Disclosure	Corporation Driven Governance	Responsibility Delegation	Government Lead with Corporation Consultancy
	Trade Policy Implementation	Responsibility Delegation	Government Lead with Corporation Consultancy	Cyberspace Compliance Requirements
	Cyber Trade Norms Development	Responsibility Delegation	Government Lead with Corporation Consultancy	Cyberspace Compliance Requirements

interests. Within this mode, the networked governance mode is more like the lead-organization-govern mode where governments act as the lead organization, and corporations provide capabilities to support policy making.

- *Responsibility Delegation*. Governments delegate some cybersecurity responsibilities to corporations. Corporations develop industry best practices, which become a voluntary or actual *de facto* standard. To promote the adoption of such a standard globally, corporations work together with governments to implement it as a trade policy or include it into free trade agreements. Meanwhile, corporations can help governments improve their capability to manage cybersecurity risk. Hence, in this mode, governments and corporations coordinate on a relatively equal basis, adopting the participant-governed networked governance mode, while corporations take more leading role to promote the development of transnational cybersecurity governance.
- *Corporation Driven Governance*. Governments do not manage cybersecurity risks from digital trade adequately partially due to lack of capacities, or cybersecurity is not on governments' agenda. In such a case, governments do not regulate or provide related information. Corporations, especially those who strongly control the global cyber-physical infrastructure, code, algorithms, or data, have the *de facto* power to set cybersecurity rules within their supply chains. Therefore, the networked governance mode is more like the lead-organization-govern mode, while corporations take the leading role.

7. Empirically exploring governance of cybersecurity risk from digital trade: case collection and coding

We use the following methods and steps to create a representative collection of cases to understand the governance of cybersecurity risks from digital trade.

First, we start with the Technical Barriers to Trade (TBT) Information Management System (TBT IMS), which lists all TBT notifications and specific trade concerns (STCs) raised by the TBT Committee. Keywords, including 'cyber security', 'cybersecurity', 'information security', 'ICT', and 'national security' are used to identify the relevant TBT notifications and STCs. Second, we also collect data from the ECIPE Digital Trade Estimates (DTE) database, and the keyword 'security' is used to identify the relevant policies. We examine each case from the two above sources independently to identify and categorize cases based on the developed taxonomy. Third, we further identified missing cases in the previous two data sources by combing the digital trade barriers listed by the USTR, publicly available reports, and literature using a snowball strategy. Fourth, we hosted a workshop which invited 20 senior executives, managers, and researchers from Fortune 500 companies and cybersecurity solution providers, who are the industrial members of our consortium, to discuss these cases and identify additional ones. Fifth, after we get the list of cases, we search the timeline for each case to identify the related events, representing strategies taken by governments or corporations within that case, to grasp their interactions. This searching process enabled us to collect 75 cases with 228 events involving 31 different nations.

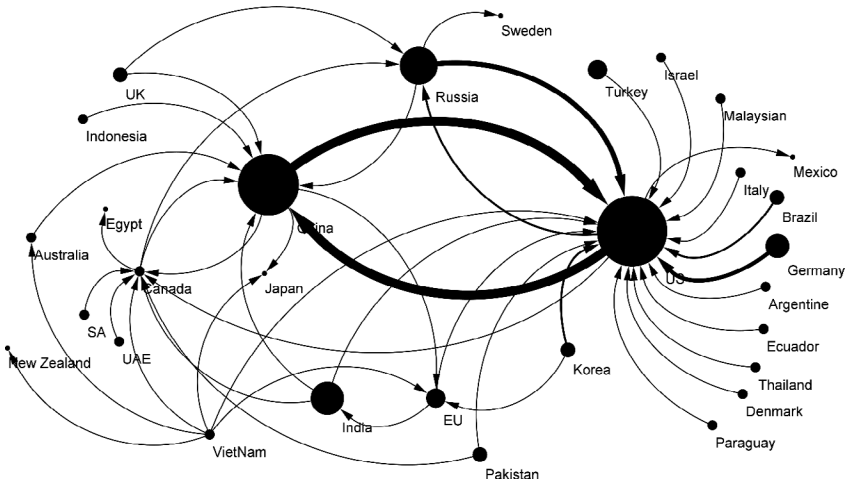
We use the developed framework, especially the detailed strategies adopted by governments and corporations in Section 6, to label each case. To ensure unbiased annotations, we invite a second coder to code each case. After the coding procedure, the two coders met to thoroughly and collaboratively review, edit the annotation, and generate the final annotations. Please note that we focus on developing a panoramic view of this complex phenomenon. We do not seek to delve in-depth into each case to understand the factors that drive the dynamics of interactions.

7.1. Results

7.1.1. Q1: What are the cybersecurity risks from digital trade, and who raises the concerns?

As shown in Figure 4, most major economies, such as G20 and OECD members are involved in the collected cases. 26 states out of 31 initiates strategies to manage cybersecurity risks from digital trade, for at least one case. Institutively,

Figure 4. Network view of national interaction. Each node refers to a state. Node size represents the number of cases where this state acts as a host state. For each edge, the source node refers to the host state, target node refers to the home state, and its width refers to the number of related cases.



while the press has primarily focused on transnational cybersecurity issues among the US, China and Russia, making the misperception that this issue is only among these three countries, our data indicate that the governance of cybersecurity risks from digital trade is genuinely a global governance issue.

Of the 75 collected cases, as reported in Table 1, most cases address risks related to political (52/75) and societal (32/75) cybersecurity risks, while only a few are related to economic (17/75) and military (5/75) cybersecurity risks. From the supply chain view, in most cases (59/75), governments raise cybersecurity concerns when purchasing transnational digital products as buyers with only 19 cases concerning the cybersecurity risks for the supplied digital products.

Finding 1: Governments mostly take strategies regarding cybersecurity risks within the purchasing transnational digital products, with a primary focus on the influence to their domestic political and societal system, while they can be lacking the capability to mitigate such risks.

7.1.2. Q2: What strategies do governments and corporations use to manage these risks, and what governance modes emerge through their strategic interactions?

As reported in Figure 5, the predominant government strategy to manage cybersecurity risks from digital trade is implementing import-related trade policies. The most popular policy is import limitation/requirement. Post-sales and digital service requirements are then implemented to regulate how the offerings are operated within the domestic market. Very few cases involve WTO, free trade agreements, or dialogue mechanisms. Interestingly, expressing cybersecurity concerns or offering recommendations without mandatory requirements is the third most common option for governments, comfirming the magnitude of indirect governance choices for governments (Abbott et al., 2016).

Table 1. Relations of cybersecurity risk and national cybersecurity capability

	Supply chain cybersecurity risk			
	Buyer	Supplier	Cases	Average GCI
National cybersecurity risk				
Military	2	3	5	0.911
Political	42	12	52	0.797
Economic	11	7	17	0.799
Societal	28	5	32	0.758
Cases	59	19	75	/
Average GCI	0.787	0.872***	/	/

Notes: For each case, we further use the ITU Global Cybersecurity Index (GCI) to assess the host state's cybersecurity commitment, representing its capability to mitigate potential cybersecurity risks.

***The one-sided Welch's t-test confirms that those states that raise cybersecurity risks as buyers have a statistically significantly lower GCI value than states as suppliers ($p = 0.002$). This indicates that governments acting as buyers may not effectively mitigate cybersecurity risks from digital trade compared with those acting as suppliers. However, the differences in GCI values among the four national cybersecurity risks are not significant.

Figure 6 demonstrates that in most cases, corporations choose to comply with the given policies from governments. Negotiating with host states to refine the implemented policies is the second most popular option. A few cases exist in which corporations take more aggressive strategies to cyber-secure the supply chain or improve governments' cybersecurity capability to manage potential cyber risks. Rarely do corporations involve themselves in industrial trade norms development or engage governments to coordinate specific cybersecurity-related trade policies. However, we

Figure 5. The distribution of government strategies.

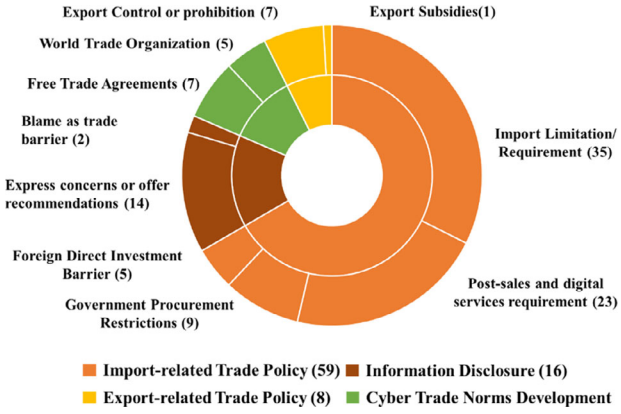
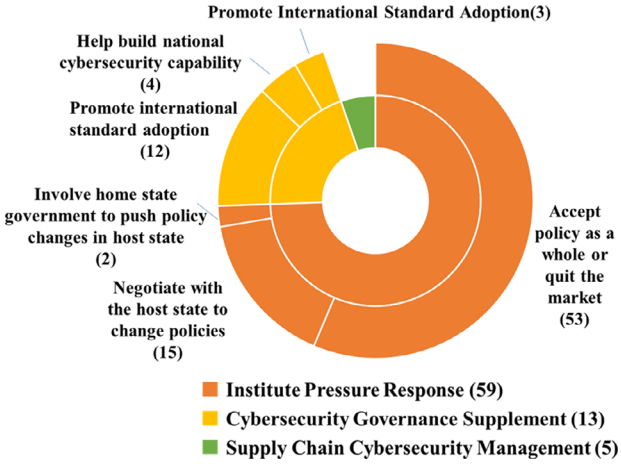


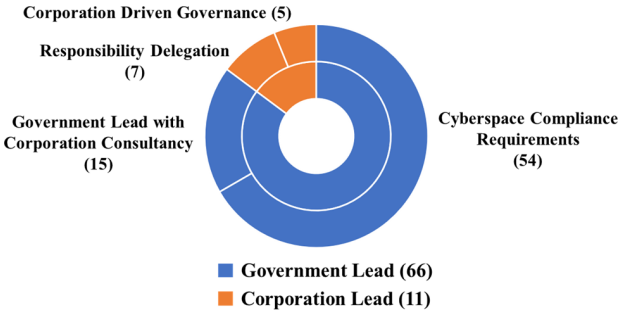
Figure 6. The distribution of corporation strategies.



observe several cases where Google (Case #10), WhatsApp (Case #56), Microsoft (Case #64), SWIFT (Case #65), and Cloud service providers (Case #70) use their controls over digital infrastructures to set cybersecurity standards throughout their global supply chain, sometimes refining governments' actions.

As reported in Figure 7, it is clear that the mainstream cybersecurity governance mode is 'cyberspace compliance

Figure 7. The distribution of governance modes.



requirements, ' wherein governments take the leading role. However, corporations can shape the governance schema in certain situations. The cases we collect show that corporations can utilize the notification period, when governments propose or preliminarily implement regulations and gather feedback, to provide input to refine the policies. Corporations can also develop the *de facto* standards, which are further adopted as parts of the governance schema, or can utilize their dominant market positions and political capability to overturn governments' strategies or share the responsibilities to mitigate cybersecurity risks with governments.

Finding 2: The governance practices are diverse, with a mainstream pattern where governments implement import-related trade policies and corporations comply. The Cyberspace Compliance Requirements Mode is the predominant pattern, but corporations do have chances to take a leading role in the cybersecurity governance mode in a few situations.

7.1.3. Q3: Will cybersecurity risks from digital trade impact different governance modes?

As reported in Table 2, we can see that most lifts for national cybersecurity risks to governance modes are not statistically significant, meaning variation in the type of national cybersecurity risks has no significant effect on the selection of governance mode. On the other hand, when a cybersecurity risk is raised from the buyer perspective, there is a significantly higher chance that governments will take the initiative, given a lift significantly higher than 1 ($p < 0.05$) for the rule '*Buyer* ➔ *Government Lead*', and corporations have fewer opportunities to gain leadership roles given a lift significantly lower than 1 ($p < 0.1$) for the rule 'Buyer ➔ Corporation Lead'. On the contrary, we observe a lift significantly lower than 1 for the rule 'Supplier ➔ Government Lead' and a lift significantly higher than 1 for 'Supplier ➔ Corporation Lead', meaning that when a cybersecurity risk arises from the supplier perspective, corporations have a higher probability of introducing their strategies to take the lead. The lift for rule 'Buyer ➔ Government Lead with Corporation Consultancy' is significantly higher than 1, while the lift for rule 'Buyer ➔ Corporation Driven Governance' is significantly lower than 1. This indicates that when governments act as buyers, they have a higher probability of choosing the 'Government Lead with Corporation Consultancy' mode to engage corporations in the governance practices, but a lower likelihood of handing off primary responsibility to corporations using 'Corporation Driven Governance' mode. However, if the cybersecurity risks are from the supplier perspective, corporations have a higher opportunity to adopt the 'Corporation Driven Governance' mode.

Due to the unbalanced samples, we should not over-interpret these association rules, but this observation nevertheless indicates that different cybersecurity risks, especially from the supply chain perspective, can impact the roles and strategies that governments and corporations take.

Finding 3: Different national cybersecurity risks don't significantly impact transnational cybersecurity governance modes, but the supply chain cybersecurity risks do.

Table 2. Association rules between cybersecurity risks and governance modes.

		National cybersecurity				Supply chain cybersecurity	
Governance model	Total	Military	Economic	Political	Societal	Buyer	Supplier
Government lead	66	4 (0.909)	14 (0.936)	48 (1.049*)	29 (1.030)	55 (1.059**)	13 (0.778***)
Cyberspace compliance requirements	54	4 (1.111)	12 (0.980)	40 (1.068)	22 (0.955)	43 (1.012)	13 (0.950)
Government lead with corporation consultancy	15	/	3 (0.882)	10 (0.962)	7 (1.094)	15 (1.271**)	/
Corporation lead	11	1 (1.364)	3 (1.203)	6 (0.787)	3 (0.639)	6 (0.693*)	6 (2.153**)
Responsibility Delegation	7	1 (2.143)	1 (0.630)	5 (1.030)	2 (0.670)	5 (0.908)	3 (1.692)
corporation driven governance	5	/	2 (1.765)	2 (0.577)	2 (0.938)	2 (0.508**)	3 (2.368*)
Total	75	5	17	52	32	59	19

Notes: The number in brackets represents the lift of the given rule, that is, the ratio of the observed support to that expected if the cybersecurity risk and governance mode were independent, and its significance level. A lift larger than 1.0 implies that the relationship between the antecedent (cybersecurity risk) and the consequent (govern mode) is more significant than would be expected if the two sets were independent. The statistical significance is marked as a superscript, with *, **, ***representing significance levels of 0.1,0.05, and 0.01, respectively. '/' means that there exist no such rules in our cases. For details about the calculation of the lift and the significance level, please refer to Support Material Section D.

7.1.4. Q4: Will different governance modes impact the cybersecurity risks from digital trade?

In many of the collected cases, governments take more than one strategy. For example, in the case of Huawei's conflict with the US (Case #2), six different strategies were taken by the US government over the years. Similarly, corporations may take various actions throughout a case. Hence, we chronologically order the strategies taken by governments and corporations in each case to identify the interaction sequences. We aggregate these interaction sequences for all the collected cases, creating a panoramic view of dynamic interactions between governments and corporations, as shown in Figure 8.

Intuitively, we can observe a predominant pattern wherein cybersecurity risks result in the implementation of trade policies, and companies take strategies to respond to these policies. This confirms that the primary governance mode is the 'cyberspace compliance requirements mode'. Importantly, it is clear that there are many different paths, resulting in different outcomes for specific cases. Hence, governments and corporations have more available alternative strategies. Additionally, this model reveals two loops of interaction sequences between governments and corporations, which can drive the transnational cybersecurity governance into different directions:

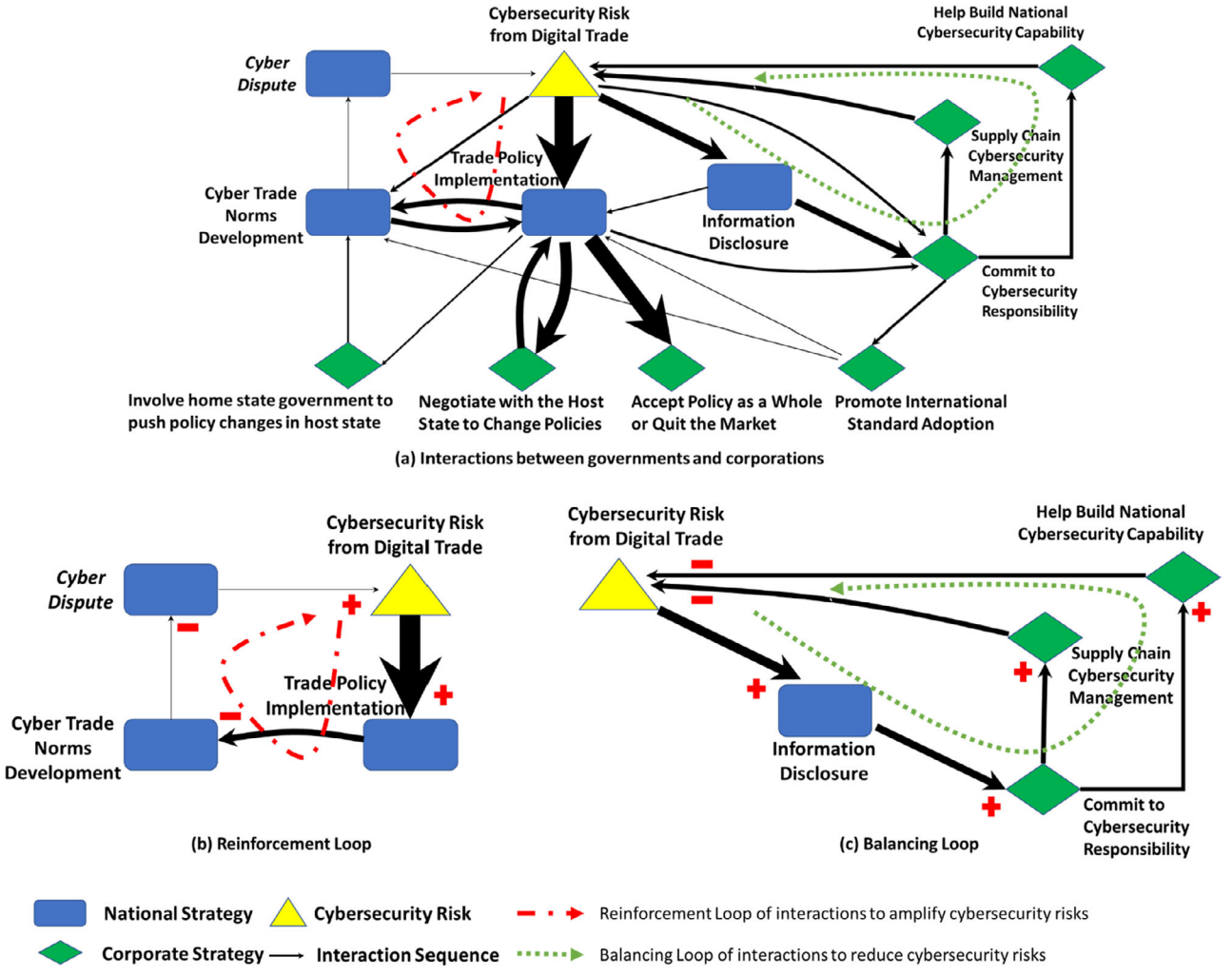
- *The reinforcement loop*: as shown in Figure 8(b), governments implement trade policies to manage cybersecurity risks from digital trade. The fragment or conflicts among trade policies can make it more challenging to develop an effective cyber trade norms development platform, as noted by the '–' sign in the figure. The absence of such platforms can amplify the cyber dispute and, in turn, increase cybersecurity risks within digital trade, as noted by the '+' sign. Hence, the strategies taken by governments and corporations to manage cybersecurity risks from digital trade eventually increase cybersecurity risks. This creates a reinforcement loop that can escalate the risks. On the other hand, we observe several cases where free trade agreements such as the USMCA FTAs (Case #66), and Korea's FTAs with the EU and US (Case #54) can harmonize trade policies for cybersecurity risks, as noted by the '–' sign, highlighting the critical balancing role of the cyber trade norms development platform.
- *The balancing loop*: as shown in Figure 8(c), governments take information disclosure strategy and express their cybersecurity concerns. Corporations then take responsibility for cybersecurity and make efforts to manage cybersecurity risks through their global supply chain, or improve the government's ability to mitigate potential cybersecurity risks. This, in turn, reduces cybersecurity risks, as noted by the '–' sign. Hence, governments and corporations' interactions mitigate the risks, resulting in a balancing feedback loop. However, we can observe that governments can turn from information disclosure to trade policy implementation if an effective responsibility commitment mechanism is missing. This can trap the system in the reinforcement loop with ever-increasing cybersecurity risks.

Finding 4: The interactions between governments and corporations can amplify or reduce the cybersecurity risks from digital trade. The cyber trade norms development platform and corporate responsibility commitment mechanisms play critical gateway roles to shape the direction.

8. Conclusions

Governing cybersecurity risks arising from digital trade is an increasingly critical task for both governments and corporations to secure their cyber territories. We developed a systematic framework to unfold this complex and dynamic global governance issue, including the cybersecurity risks, and the strategies governments and corporations take to manage these risks. Using this framework, we collected and categorized a collection of cases to provide a panoramic view.

Figure 8. The dynamic interaction between governments and corporation. Blue squares represent national strategies, and green diamonds represent corporate strategies. Each solid black link represents the sequence taken by governments and corporations, and its width refers to the number of related cases. Please check Support Material Section B and C for more details.



Our study demonstrates governments still take authority role although the complexity of cybersecurity is making corporations more powerful in cyberspace. The most typical mode between governments and corporations in transnational cybersecurity governance is that governments implement trade policies with which corporations comply. This is in line with the previous studies on states' governance design for cybersecurity capability building (Weiss and Jankauskas, 2019). Hence, states' approach to managing transnational cybersecurity risks is also hardly revolutionary. However, governments can take a more indirect approach beyond that predominant governance pattern, and corporations have opportunities to refine the governance schema. This highlights the necessity for corporations to take a more active role in transnational cybersecurity governance.

Governments that act in a supplier role have a higher cybersecurity capability and give corporations more rooms to participate in the governance system, whereas governments acting as buyers typically have a lower cybersecurity capability but intend to lead the governance effort. However, the different national cybersecurity risks have limited effects on the governance mode. Therefore, it is essential to consider the government's supply chain mindset and cybersecurity capability when understanding the transnational cybersecurity governance mode, instead of just different national cybersecurity functionalities.

Notably, the analysis of interactions between governments and corporations provides a holistic view that sheds light on cybersecurity governance dynamics. It reveals a reinforcement loop that can escalate cybersecurity risks and a balancing loop that can effectively mitigate the cybersecurity risks. These two loops can drive cybersecurity governance towards different outcomes. Given a lack of effective cyber trade norm development platforms (Meltzer, 2019), and global business infrastructures are increasingly treated as a political tool (Farrell and Newman, 2020), the transnational cybersecurity governance is currently moving towards more conflicting trade policies and cyber disputes (Huang

and Madnick, 2020; Huang et al., 2021). Escaping from such a whirlpool through cyber trade norm development and cyberinfrastructure depoliticization is the most critical task that scholars, policy makers, and business leaders should undertake.

The taxonomy, collection of cases, and empirical results implemented in this study provide the first systematic approach to panoramically understand transnational cybersecurity governance for digital trade. This contributes to theorizing cybersecurity governance but also raises further research questions. First, this study only uses publicly available information. Though we supplement this study with literature reviews, public reports and workshop discussions, future study should go on a further semi-structural-based study to gain more domain insights. Second, this study reveals the dynamics of transnational cybersecurity governance. The future study should go more in-depth case studies to explore mechanisms that drive the dynamics of governance mode. Third, a further investigation to distinguish adopted, negotiable, or conflicting cyber trade norms can guide the cyber trade norm development for the transnational cybersecurity governance. Also, given the importance of cyberinfrastructure depoliticization where corporations can play critical roles, it is valuable to investigate how corporations design their strategies and take a more active role to depoliticize the transnational cybersecurity risks. Fourth, this study focus on the transnational cybersecurity governance for digital trade where global norms are absent and the governance system is still in its infant stage. A comparison with other more mature fields such as the Internet country code Top-Level Domains (Christou and Simpson, 2009) or the national Computer Network Emergency Response Technical Team/Coordination Center (CERT/CC) would be valuable.

Acknowledgements

The research reported herein was supported in part by National Natural Science Foundation of China (6217071254, 7210040816) and Cybersecurity at MIT Sloan, which is funded by a consortium of organizations. All errors remain the responsibilities of the authors.

REFERENCES

Abbott, K. W., Genschel, P., Snidal, D. and Zangl, B. (2016) 'Two Logics of Indirect Governance: Delegation and Orchestration', *British Journal of Political Science*, 46 (4), pp. 719–729.

Abbott, K. W., Genschel, P., Snidal, D. and Zangl, B. (2020) 'Competence Versus Control: The Governor's Dilemma', *Regulation and Governance*, 14 (4), pp. 619–636.

Abbott, K. W. and Snidal, D. (2009) 'The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State', in M. Walter and W. Ngaire (eds.), *The Politics of Global Regulation*. Princeton: Princeton University Press, pp. 44–88. https://doi.org/10.1515/9781400830732.44

Agostinis, G. and Palestini, S. (2020) 'Transnational Governance in Motion: Regional Development Banks, Power Politics, and the Rise and Fall of South America's Infrastructure Integration', *Governance*, 34 (3), pp. 765–784.

Albert, M. and Buzan, B. (2011) 'Securitization, Sectors and Functional Differentiation', *Security Dialogue*, 42 (4–5), pp. 413–425.

Assaf, D. (2008) 'Models of critical information infrastructure protection', *International Journal of Critical Infrastructure Protection*, 1, pp. 6–14.

Azmeh, S., Foster, C. and Echavarri, J. (2019) 'The International Trade Regime and the Quest for Free Digital Trade', *International Studies Review*, 22 (3), pp. 671–692.

Bendiek, A. and Römer, M. (2019) 'Externalizing Europe: the Global Effects of European Data Protection', *Digital Policy, Regulation and Governance*, 21 (1), pp. 32–43.

Boeke, S. (2018) 'National Cyber Crisis Management: Different European Approaches', *Governance*, 31 (3), pp. 449–464.

Bossong, R. and Wagner, B. (2017) 'A typology of Cybersecurity and Public-private Partnerships in the Context of the EU', *Crime, Law and Social Change*, 67 (3), pp. 265–288.

Boyson, S. (2014) 'Cyber supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems', *Technovation*, 34 (7), pp. 342–353.

Carr, M. (2016) 'Public Private Partnerships in National Cyber-security Strategies', *International Affairs*, 92 (1), pp. 43–62.

Choucri, N. and Clark, D. D. (2019) *International Relations in the Cyber Age: The Co-Evolution Dilemma*, Cambridge, MA: MIT Press.

Christensen, K. K. and Petersen, K. L. (2017) 'Public-private Partnerships on Cyber Security: A Practice of Loyalty', *International Affairs*, 93 (6), pp. 1435–1452.

Christou, G. and Simpson, S. (2009) 'New Governance, the Internet, and Country code Top-level Domains in Europe', *Governance*, 22 (4), pp. 599–624.

Daskal, J. (2018) 'Borders and Bits', *Vanderbilt Law Review*, 71 (1), pp. 179–240.

Dorobantu, S., Kaul, A. and Zelner, B. A. (2017) 'Non-market Strategy Research through the Lens of New Institutional Economics: An Integrative Review and Future Directions', *Strategic Management Journal*, 38, pp. 114–140.

Eduardsen, J. and Marinova, S. (2020) 'Internationalisation and Risk: Literature Review, Integrative Framework and Research Agenda', *International Business Review*, 29 (3), 101688.

Eriksson, J. and Giacomello, G. (2006) 'The Information Revolution, Security, and International Relations: (IR)relevant Theory?', *International Political Science Review*, 27 (3), pp. 221–244. https://doi.org/10.1177/0192512106064462

Farrell, H. and Newman, A. L. (2020) 'Choke Points', *Harvard Business Review*, (February). Available from: https://hbr.org/2020/01/choke-points [Accessed 21 August 2021].

Haufler, V. (1993) 'Crossing the Boundary between Public and Private: International Regimes and Non-state Actors', in R. Volker and M. Peter (eds.), *Regime Theory and International Relations*. Oxford: Clarendon Press, pp. 94–111.

Helfat, C. E. and Peteraf, M. A. (2003) 'The Dynamic Resource-based View: Capability Lifecycles', *Strategic Management Journal*, 24 (10), pp. 997–1010.

Hillman, A. J., Withers, M. C. and Collins, B. J. (2009) 'Resource Dependence Theory: A Review', *Journal of Management*, 35 (6), pp. 1404–1427.

Howard, P. and Bradshaw, S. (2018) 'The Global Organization of Social Media Disinformation Campaigns', *Journal of International Affairs*, 71 (1.5), pp. 23–32. Available from: https://www.jstor.org/stable/26508115 [Accessed 21 August 2021].

Hua, J. and Bapna, S. (2013) 'The Economic Impact of Cyber Terrorism', *The Journal of Strategic Information Systems*, 22 (2), pp. 175–186.

Huang, K. and Madnick, S. (2020) 'The TikTok Ban Should Worry Every Company', *Harvard Business Review*. Available from: https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company [Accessed 21 August 2021].

Huang, K., Madnick, S., Zhang, F. and Siegel, M. (2021) 'Varieties of public-private co-governance on cybersecurity within the digital

trade: Implications from Huawei's 5G', *Journal of Chinese Governance*, PP (99), pp. 1–45. https://doi.org/10.1080/23812346.2021.1923230
Inkpen, A., Minbaeva, D. and Tsang, E. W. K. (2019) 'Unintentional, Unavoidable, and Beneficial Knowledge Leakage from the Multinational Enterprise', *Journal of International Business Studies*, 50 (2), pp. 250–260.
ITU (2019) *Global Cybersecurity Index (GCI) 2018, International Telecommunication Union Report*. https://doi.org/10.1111/j.1745-4514.2008.00161.x
Jalali, M., Siegel, M. and Madnick, S. E. (2019) 'Decision-making and Biases in Cybersecurity Capability Development: Evidence From a Simulation Game Experiment', *The Journal of Strategic Information Systems*, 28 (1), pp. 66–82.
John, A. and Lawton, T. C. (2018) 'International Political Risk Management: Perspectives, Approaches and Emerging Agendas', *International Journal of Management Reviews*, 20 (4), pp. 847–879.
Klimburg, A. (2012) *National Cyber Security Framework Manual*, NATO CCD COE Publication. https://doi.org/10.1017/CBO9781107415324.004
Kshetri, N. (2016) *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, Berlin: Springer.
Kuerbis, B. and Badiei, F. (2017) 'Mapping the Cybersecurity Institutional Landscape', *Digital Policy, Regulation and Governance*, 19 (6), pp. 466–492.
Lambach, D. (2020) 'The Territorialization of Cyberspace', *International Studies Review*, 22 (3), pp. 482–506. https://doi.org/10.1093/isr/viz022
Lane, D. S., Lee, S. S., Liang, F., Kim, D. H., Shen, L., Weeks, B. E. and Kwak, N. (2019) 'Social Media Expression and the Political Self', *Journal of Communication*, 69 (1), pp. 49–72.
Madnick, S. (2019) 'These are the Cyberthreats Lurking in Your Supply Chain', in *MIT Sloan Ideas Made to Matter*, pp. 1–5. Available from: https://mitsloan.mit.edu/ideas-made-to-matter/these-are-cyberthreats-lurking-your-supply-chain [Accessed 21 August 2021].
Madnick, S., Johnson, S. and Huang, K. (2019) 'What Countries and Companies Can Do When Trade and Cybersecurity Overlap', *Harvard Business Review*, pp. 1–6. Available from: https://hbr.org/2019/01/what-countries-and-companies-can-do-when-trade-and-cybersecurity-overlap [Accessed 21 August 2021].
Manjikian, M. M. E. (2010) 'From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik', *International Studies Quarterly*, 54 (2), pp. 381–401.
Meltzer, J. P. (2019) 'Governing Digital Trade', *World Trade Review*, 18 (S1), pp. S23–S48.
Naseemullah, A. and Staniland, P. (2016) 'Indirect Rule and Varieties of Governance', *Governance*, 29 (1), pp. 13–30.
Newman, A. L. and Bach, D. (2004) 'Self-regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States', *Governance*, 17 (3), pp. 387–413.
OECD-IMF (2018) 'Towards a Handbook on Measuring Digital Trade', *Thirty-First Meeting of the IMF Committee on Balance of Payments Statistics*, BOPCOM (18/07), pp. 1–39. Available from: https://www.imf.org/external/pubs/ft/bop/2018/pdf/18-07.pdf [Accessed 21 August 2021].
Oliver, C. (1991) 'Strategic Responses to Institutional Processes', *Academy of Management Review*, 16 (1), pp. 145–179.
Provan, K. G. and Kenis, P. (2008) 'Modes of Network Governance: Structure, Management, and Effectiveness', *Journal of Public Administration Research and Theory*, 18 (2), pp. 229–252.
Scott, C. (2004) 'Regulation in the Age of Governance: The Rise of the Post-regulatory State', in J. Jacint and L.-F. David (eds.), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance*. Northampton, MA: Edward Elgar Publishing, pp. 145–174.
Selby, J. (2017) 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?', *International Journal of Law and Information Technology*, 25 (3), pp. 213–232.
Sheldon, W., Michael, T. M., Karen, E. and Sameer, B. (2017) *From Awareness to Action: A Cybersecurity Agenda for the 45th President*. Washington, D.C: Center for Strategic and International Studies (CSIS), pp. 1–16. Available from: https://www.jstor.org/stable/resrep23137.4 [Accessed 21 August 2021].
Shore, M., Du, Y. and Zeadally, S. (2011) 'A Public-private Partnership Model for National Cybersecurity', *Policy & Internet*, 3 (2), pp. 168–190.
Treib, O., Bähr, H. and Falkner, G. (2007) 'Modes of Governance: Towards a Conceptual Clarification', *Journal of European Public Policy*, 14 (1), pp. 1–20.
UNCTAD (2012) *Classification of Non-Tariff Measures*. New York: United Nations.
Verhulst, S. G. and Price, M. E. (2005) *Self Regulation And The Internet*. The Hague: Kluwer Law International.
Voon, T. (2019) 'The Security Exception In WTO Law: Entering a New Era', *AJIL Unbound*, 113 (2), pp. 45–50.
Weiss, M. and Jankauskas, V. (2019) 'Securing Cyberspace: How States Design Governance Arrangements', *Governance*, 32 (2), pp. 259–275.

Supporting Information

Additional supporting information may be found online in the Supporting Information section at the end of the article.

Supplementary Material

Author Information

Keman Huang is an Associate Professor at the Renmin University of China and a Research Affiliate at the MIT Sloan School of Management, where he works on cybersecurity management and policy, innovation ecosystems, and big data analysis.

Stuart Madnick is John Norris Maguire Professor of Information Technologies in MIT Sloan School of Management and Founding Director of Cybersecurity at MIT Sloan (CAMS), formerly the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. Dr. Madnick holds a Ph.D. in computer science from MIT and has been a faculty member of MIT since 1972.

Nazli Choucri is the Professor of Political Science, Faculty Affiliate at MIT Institute for Science and Data (IDSS) and Senior Faculty at the Center for International Studies (CIS). Her research focuses on international relations, with special attention to growth and expansion – in "real" and cybersystems.

Fang Zhang is an Assistant Professor at School of Public Policy and Management, Tsinghua University. She gained a PhD degree in international affairs from Tufts University, and PhD in public administration from Tsinghua University China. Her research topics include public policy analysis, technology innovation and transfer, and global governance.