Varieties of public-private co-governance on cybersecurity within the digital trade: Implications from Huawei's 5G

Keman Huang[a], Matthew Deegan[b], Stuart Madnick[c], Fang Zhang[d,*], and Michael Siegel[e]

[a] *Cybersecurity at MIT Sloan, Sloan School of Management, MIT, Cambridge, MA 02143, US; Email: keman@mit.edu*

[b] *Fletcher School, Tufts University, Medford, MA 02150, USA; Email: mdeegan18@gmail.com*

[c] *Cybersecurity at MIT Sloan, Sloan School of Management, MIT, Cambridge, MA 02143, US; Email: smadnick@mit.edu*

[d] *School of Public Policy and Management, Tsinghua University, Beijing, China, 100084; Harvard Kennedy School, Harvard, Cambridge, MA 02138, USA; Email: fangzhang@hks.harvard.edu;*

[e] *Cybersecurity at MIT Sloan, Sloan School of Management, MIT, Cambridge, MA 02143, US; Email: msiegel@mit.edu;*

Abstract: Cybersecurity is becoming an increasing hurdle for digital trade. The governance of cybersecurity in the global digital trade system is a bottom-up approach, where governments are implementing fragmental, inconsistent, sometimes even conflicting, trade policies and forming different modes of public-private co-governance. Based on network-governance theory, information security behavior theory, and international risk theory, we develop a conceptual model to investigate how various factors drive cybersecurity governance practices. Using Huawei's 5G as an example, this study explores how different governments—the United States, the United Kingdom, Germany, Australia, and India—take actions on the cybersecurity concerns from Huawei's offerings over the years. The comparative analysis demonstrates how balancing different factors drive governments' actions and discuss what international corporations like Huawei can do to align their strategies in digital trade system. This research guides for international firms to participate in cybersecurity governance constructions within the digital trade system.

Keywords: Cybersecurity within Digital Trade, Huawei, Case Study, Cybersecurity Governance, Digital Trade System

1. Introduction

Digitization is penetrating every aspect of contemporary society, including how trade happens and what is being traded. Nowadays, almost any modern cross-border product or service can be digitally ordered, enabled or delivered, making digital trade[1] the critical engine for global economic and international business growth. However, accompanied by sustained digital innovations, the weak cybersecurity that can occur in digital technology is becoming a growing threat. Cyber incidents are making headlines daily, raising concerns regarding the potential negative impact of cyber threats through global supply chains (Boyson, 2014; Madnick, 2019).

Unfortunately, global platforms such as WTO fail to make significant progress on digital trade governance (Meltzer, 2019). There are no widely-accepted international rules for managing digital trade, let alone rules to address challenges from cybersecurity issues within the digital trade system. Cybersecurity concerns from digital trade are increasingly being seen as a matter of "national security" (Welch, 2011). Consequently, the "security exceptions" principle has been abused in the international trade system (Voon, 2019). For example, on May 15th, 2019, the U.S. declared a national emergency to deal with the threats from information and communication technologies (ICTs) through the supply chain. The U.S. Department of Commerce's Bureau of Industry and Security (BIS) then added Huawei Technologies and its affiliates to the "Entity List," which bans U.S. firms doing business with Huawei (US White House, 2019). This action may expand the "ambiguities of cyber threats to national security" (Joseph, 2017)

[1] For discussions on definitions of digital trade, please refer to Appendix A for more details.

into the international trade system, and this overuse of the national cybersecurity exception is snowballing as it is being used by the largest trading partners in the WTO (Kho & Petersen, 2019).

This "new world" (Farrell & Newman, 2020) is putting global firms under pressure. Executives need to accept and understand this reality to align their global digital strategy. This emphasizes the importance of the public-private co-governance for cybersecurity within digital trade, where corporations are actively taking cybersecurity governance responsibility (Lambach, 2019; Weiss & Jankauskas, 2019). However, the increasingly political dispute due to cybersecurity concerns and the inconsistent interests among corporations, their home, and host states make the public-private cybersecurity co-governance much more complex and diverse within digital trade system. Business leaders and policymakers need to understand this dynamic phenomenon to make their decisions regarding cross-border digital innovations. Therefore, this study aims to provide a framework to understand *what* factors and *how* they drive the diverse outcomes when governments and corporations interact to manage the cybersecurity concerns associated with digital trade.

To achieve this goal, we develop a conceptual model and a comparative analysis through investigating how different governments—the United States, the United Kingdom, Germany, Australia, and India—take actions on the cybersecurity concerns from Huawei's offerings over these years. These cases have been selected purposefully as the telecommunication industry plays a critical role within the national cyberinfrastructure, which can quickly raise national cybersecurity concerns. Additionally, though the cybersecurity concerns are similar, the policy implementations and interactions among Huawei, its home state (China), and these five host states are quite different and result in various observable outcomes. Hence, these Huawei's 5G

cases can provide us plentiful information to dig into the dynamics within the public-private co-governance, enabling us to analyze the factors that drive their decisions and lead us toward a framework with which corporations and governments can evaluate their options.

The article is structured as follows. First, we discuss the cybersecurity co-governance within digital trade to develop a conceptual model. Second, we describe Huawei's cases regarding cybersecurity concerns within each state. Third, we briefly introduce the research methods and data collection. Fourth, using the conceptual model, we develop a comparative analysis to investigate the roles of different factors within the Huawei cases. Fifth, we discuss the major findings and their implications. Finally, we summarize this paper.

2. Theoretical Framework: Public-Private Cybersecurity Co-governance within Digital Trade

To understand the cybersecurity co-governance within digital trade, we turn to these fundamental questions: *what makes cybersecurity co-governance within digital trade so critical*, *what trade regimes governments can implement and result into what business impact*, *what public-private cyber co-governance mode exist*, and *what factors can impact the decision making regarding cybersecurity concerns*. Answering these questions will help us to develop a systematic analysis framework to compare different cases.

2.1 The Reterritorialization of Cyberspace

The reterritorialization of cyberspace as the national cyber territory has become a reality (Lambach, 2019), and cyberspace can no longer be conceived as being separated from the "offline world". Many nations have expanded or are expanding their authority into

cyberspace. Some states, especially powerful countries like the United States and coalitions like the E.U., are developing their laws and regulations in extraterritorial ways. For example, the United States CLOUD Act of 2018 and the European Union's General Data Protection Regulation (GDPR) empower their judiciaries to third countries (Daskal, 2018). This overlap of state cyber territory cross geographical national territory can result in cyber disputes, even cyberwar between nations (Choucri, 2012; Lindsay, 2017; Maness & Valeriano, 2016). We are witnessing cybersecurity concerns from digital trade, playing an increasing role in reshaping the international business environment.

On the other hand, most corporations rely on a global, interdependent supply chain (Linton, Boyson, & Aje, 2014; Voss & Williams, 2013), so their business ecosystem will cross the geographical border. Therefore, the corporate and state cyber territories now have significant overlap within the cross-border activities. As governments are generally regarded as lacking sufficient cybersecurity capability (Manjikian, 2010) while corporations have sufficient global reach to achieve the state's extraterritorial goal, delegating the enforcement of laws to corporate governors is becoming much more attractive (Berman, 2018). In some extreme cases, the strong control on the global cyberinfrastructure, like Google's Android operating system, Visa's payment channel, and Qualcomm's chips etc. which are supposed to facilitate international business, are being or can be weaponized by powerful countries (Farrell & Newman, 2020). Consequently, cyber disputes can escalate quickly, while the high level of distrust and tense relationship between nations and corporations can insinuate more digital protectionisms (Aaronson, 2018).

The public-private partnership (Boeke, 2018; Carr, 2016; Christensen & Petersen, 2017) between governments and private sectors is considered a cornerstone to

secure cyberspace. Governments tend to delegate the cybersecurity capability building to third-parties, including the private-sector (Weiss & Jankauskas, 2019). However, the interests between governments and corporations do not always align. The private sector tends to consider cybersecurity from a financial and reputational perspective. In contrast, the public sector approaches cybersecurity as a common public good to cyber-secure digital society as a whole (Carr, 2016). This inconsistency is much more significant between the corporations and their host and home countries in the cross-border context.

Therefore, given the trend of cyberspace reterritorialization, the responsibility delegation between governments and corporations on cybersecurity, and the inconsistency of interests among corporations, home and host states, are putting global firms under significant pressures. Cybersecurity issues within digital trade play an increasing role in the international business environment where business leaders and policymakers should understand its complexity and dynamics.

2.2 Trade Regimes and the Impact on Corporations

Trade regimes, including tariff and non-tariff policies on trade in goods, services, and foreign direct investments, are used as mechanisms to manage cybersecurity concerns (Grindal, 2019). As there is no global rule with cybersecurity governance within digital trade (Meltzer, 2019), governments implement various trade policies to mitigate their cybersecurity concerns. We can observe practices across all the non-tariff barrier categories covering digital products (Huang, Madnick, & Johnson, 2019). For example, governments can implement restrictions on the use of certain products given the cybersecurity concerns (Madnick, Johnson, & Huang, 2019). Export controls, tariffs, restrictions on foreign direct investment, and localization requirements are widely used to restrict trade on cybersecurity products or cybersecurity risks within the products

(Grindal, 2019). Especially for cross-border financial services, localization requirements, and pre-requirement for market access, including blacklist/whitelist, foreign direct investment investigations and restrictions are implemented by governments to mitigate the potential cybersecurity risk cross-border financial transactions (Huang & Madnick, 2020). Hence, this study focuses on their business impacts on cross-border activities to make these highly diverse trade regime implementations comparable.

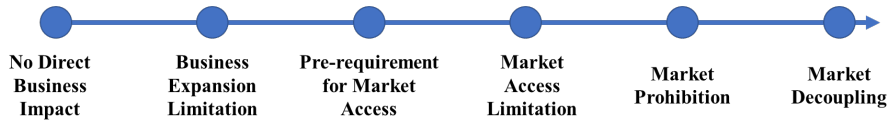

Figure 1. Business Impact from Cybersecurity Motivated Trade Policies.

As shown in Figure 1, we can identify the business impacts based on the restrictive level: governments can choose to hand off and completely delegate to the market. There is no direct business impact. Governments can then further develop restrictions to limit a specific corporation's growth to control the potential risk. One typical practice is that the foreign direct investments are subject to approval unless contrary to the national interest (John & Lawton, 2018). The most common implementation is that service providers must meet specific requirements like specific cybersecurity certifications and tests before entering the domestic market. Though this may increase the corporation's cost and delay their time to the market, foreign firms still can sell their products and services in that specific market. A more extreme policy, market access limitation, involves corporations being wholly restricted from particular markets. The most common policy implementation associated with this strategy is the government procurement restriction. Taking a step further, corporations can be "outright banned" and prohibited from getting into the market, given the potential cybersecurity threats. In this case, the corporation will lose access to the entire market. The most

severe impact for business operations is that corporations are blacklisted in the market where they are not only prohibited from providing products or services as a seller but also prohibited from purchasing products or services as a buyer. Therefore, corporations are definitively isolated from the domestic market.

2.3 Public-private Co-governance Modes

Public-private partnerships have been considered as the cornerstone for many national cybersecurity strategies, including cyber crisis management and cybersecurity capability building (Boeke, 2018; Carr, 2016; Christensen & Petersen, 2017; Weiss & Jankauskas, 2019). Provan and Kenis (Provan & Kenis, 2008) identified the three network-governance models to describe how different actors interact with each other to construct the governance modes for the networked environment: participant-governed networks with the equality of members and high levels of trust within the network; lead-organization-governed networks where government take the coordination responsibility for the activities and decision makings within the network; and the network administrative organization where government specifically governs the network's activities. The case study (Boeke, 2018) from the Netherlands, Denmark, Estonia, and the Czech Republic shows the practical implementations of these basic network governance modes on the national cyber crisis management. Weiss & Jankauskas (Weiss & Jankauskas, 2019) showcased the delegation and orchestration modes between governments and corporations in cybersecurity capability building, where delegation mode refers that government delegates related responsibility to agents using a hierarchical control relationship; while orchestration mode refers to soft and voluntary governance that government acts as a manager and cannot coerce the intermediary. Through an analysis of Danish cyber-security public-private partnerships, Christensen and Petersen (Christensen & Petersen, 2017) highlight the disagreement between public

and private actors on cybersecurity and emphasizes the importance of loyalty public-private partnership and the necessity of partnering through dissent beyond power-sharing and management reform. In the international market context, John and Lawton summarized three interaction modes between corporations and host governments, including reactive, proactive, and active (John & Lawton, 2018). Reactive strategy refers that firms align with the political environment by complying with regulatory standards, proactive strategy refers that firms create value out of political risk by shaping the non-market environment, while active strategy refers to firms actively managing and reducing political risk by influencing governments.

Table 1. Cybersecurity Governance Mode within Digital Trade

Mode	**Description**	**Network-governance Model**	**Interaction Mode**
Cyberspace Reterritorialization and Compliance	Government implements cybersecurity trade policies that corporations comply with.	Network-administrative	Reactive
Government Lead with Corporation Consultancy	Government takes inputs from corporations to refine the implementation of the specific cybersecurity trade policy	Network-administrative/ Lead organization	Reactive/ Proactive
Responsibility Delegation	Government initiates the trade policies process, and the corporation takes responsibility to develop the industrial best practices which become into a *de facto* standard or is implemented as a policy	Lead organization /Participant governed	Proactive/ Active

Hence, as summarized in Table 1, extending the network-governance theory into the international context, we can identify three basic cybersecurity governance modes within digital trade, including 1) *Cyberspace reterritorialization and compliance* where governments take the network administrative role while the corporations use the reactive strategy to comply with the policy; 2) *Government lead with corporation*

consultancy where governments take the lead-organizational role while the corporations use more proactive strategy to involve the policy implementations to twist the outcome; 3) *Responsibility delegation* where governments initiate the cybersecurity concern but delegate the responsibility to both domestic and international corporations, and coordinate corporations to build de facto standards, which can then become the policies.

Note that there can exit a mode where cybersecurity within digital trade is considered entirely as a supply-chain cybersecurity management issue for corporations, and governments do not regulate it. As we focus on the interactions between corporations and governments, this mode is not considered in this study.

2.4 Conceptual Model for Public-private Cybersecurity Co-governance

Regarding "*what factors can impact the cybersecurity behavior*," many information security behavior theories such as the coping theory (C.T.), the protection motivation theory (PMT), the technology threat avoidance theory (TTAT), the rational choice theory (RCT), and the deterrence theory (D.T.) have been developed to understand the processes and mechanisms that motivate individuals and organizations to take cybersecurity protective actions, seek help or avoid, against different security threats (Chen & Zahedi, 2016; Cram, D'Arcy, & Proudfoot, 2019; Liang, Xue, Pinsonneault, & Wu, 2019; Meijer, 2015; Moody, Siponen, & Pahnila, 2018; W.Welch, K.Feeney, & Park, 2016). For example, the deterrence theory (D.T.) suggests that formal and informal sanctions can negatively impact the violations as these sanctions increase the perceived cost. The coping theory (C.T.), the protection motivation theory (PMT), and technology threat avoidance theory (TTAT) have been widely used to explain individual behavior based on their assessments of threats and their capabilities to cope with these threats. The perceived threat is a critical component in motivating the coping behaviors

that avert potential harm. It represents the extent to which a particular event is perceived as dangerous or harmful, reflecting the objective's assessment of their susceptibility to the threat and of perceived severity of the threat. The perceived coping abilities, including response efficacy and self-efficacy, can motivate individuals to take protective actions and reduce the intention to avoid using digital technologies. Generally speaking, these previous studies reveal that there exist three key determinants impacting whether individuals and organization will take action: 1) there is a positive association between the high severity and susceptibility of the perceived threat and the likelihood to take a protective action; 2) the high benefit or low cost from taking an action will motivate the individual or organization to take it, and 3) a high capability to act will motivate individuals and organizations to take an action.

On the other hand, an extensive literature has developed theories and tools to investigate the cross-border political risks, which is among the most salient concerns for international business (Gamso & Nelson, 2019; John & Lawton, 2018). With the international business environment, organizations face different types of risks, such as institutional, cultural, political, economic, convertibility, and foreign exchange risks (Eduardsen & Marinova, 2020). Identifying, managing, and minimizing these various risks has become a fundamental responsibility for international business leaders. There exist three key factors impacting the decision-making for business leaders and policymakers, including 1) the institutional factors including a country's regulations and policies and the relations between home and host countries which forms the international business environments, 2) the resource dependence consideration regarding corporations' dependencies with other local or international organizations, and 3) the corporations' political capability to manage the risks (Gertz, 2018; Graham, Shipan, & Volden, 2013; Li, Newenham-Kahindi, Shapiro, & Chen, 2013; Mahoney,

2000; Pierson, 2000). Additionally, path dependency (Pierson, 2000) has been widely studied in policy diffusion studies to explain institutional history's impact on policy change. This is because the preceding situations will shape the meaning, purpose, and direction of future actions. In digital trade context, the way a nation manages the general trade within a specific industry will inevitably shape the policy implementation of cybersecurity within such industry.

Hence, when investigating how governments and corporations make decisions regarding cybersecurity concerns from cross-border digital trade, it is necessary to account for how they balance perceived cost and benefit, the severity and susceptibility of cybersecurity risk, and their capability to manage such cyber risk. Importantly, this study does not intend to develop a comprehensive list of factors that can impact the decision or evaluate each factor's effectiveness. Instead, our goal is to understand in the selected states, how different factors shape the implementation of trade policies and the different modes of public-private co-governance in response to the cybersecurity concerns.

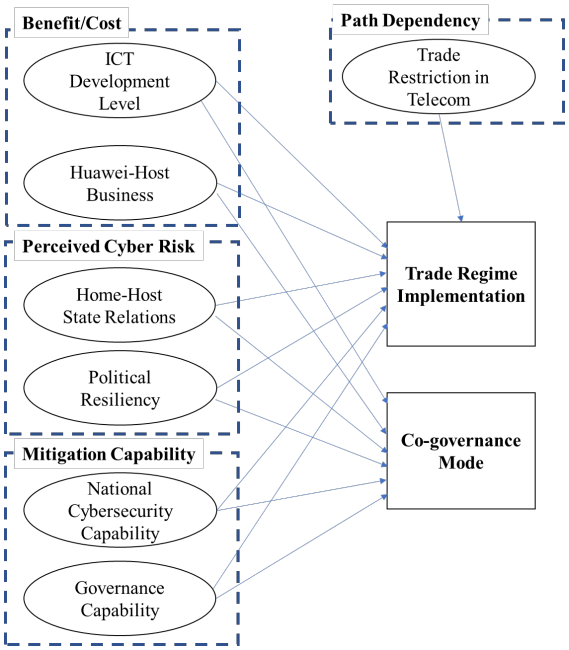

Figure 2. A conceptual framework to understand the public-private cybersecurity co-governance within the digital trade system.

Hence, in the context of 5G network implementation, as shown in Figure 2, the perceived benefit from implementing 5G networks will be related to a state's development in information communications technology (ICT): a high ICT development level indicates that the country is ready to roll out the 5G network construction. Huawei's existing business within the host state can influence mutual trust and shape the perception of costs to implement trade restrictions targeting Huawei. As Huawei's products' technological risk can be considered the same for different states, the perceived cybersecurity risks associated with using Huawei's 5G products will be primarily determined by home-host state relations and governments' institutional resilience against external interference. Commitment for cybersecurity capability building and the public sector's capacity to effectively formulate and implement sound policies will quantify the capability to mitigate the potential cybersecurity risk. Combined with the trade restriction on telecommunication caused by the path dependence effect, these factors will impact policy implementations and public-private co-governance mode. This paper will use this model to guide the study to investigate how these factors influence Huawei's cases across the United States, the United Kingdom, Australia, Germany, and India.

It is worth to note that the developed model above, including the different factors, the variance governance modes, and outcomes, is a general model of managing cybersecurity threat in digital trade. They can apply to not only Huawei but also other multinational enterprises.

3. Huawei's Cases on Cybersecurity Governance within Digital Trade

This section will briefly describe the Huawei's cases regarding to cybersecurity concerns in the United States, United Kingdom, Germany, Australia, and India. Note

that we collect these cases based on publicly available information, and we will offer the related links separately as support material instead of using references.

It is essential to focus on Huawei's 5G network because the telecommunication industry plays a critical role within national cyberinfrastructure, which is necessary for everything from banking to humanitarian aid. Given the cyberspace reterritorialization trend, some global cyberinfrastructures are being weaponized by influential countries. For example, the Society for Worldwide Interbank Financial Telecommunication's (SWIFT) secure financial-messaging service that is used for most global financial transactions is a viable option in sanction toolkits for the U.S and E.U. Therefore, the 5G network implementation can quickly raise national cybersecurity concerns.

Since its founding in 1987, Huawei has developed into a leading global distributor in technology and provider of telecommunications networks and related services, especially in 5G network development and deployment. As shown in Figure 3, Huawei's market share grew from 27.7% in 2018 to 28.1% in the first half of 2019, dominating the global telecom equipment market. Furthermore, as reported by Counterpoint' Market Monitor service, with a 16% market share, Huawei also surpassed Apple to become the second-largest brand in the Smartphone shipment market in 2019.

Figure 3. Huawei's Global Telecom Equipment Market Share. Source: Dell' Oro Group.

The cybersecurity concerns surrounding Huawei's offerings can be dated back to 2008, providing us plenty of material to understand how the dynamic of interactions has progressed over the years. Though the cybersecurity concerns from Huawei's 5G network development and deployments are similar, as we demonstrated in the following sections, the policy implementations and interactions among Huawei, its home state (China), and these five host states are different.

3.1 United States

Huawei's jungle journey regarding cybersecurity in the United States started in 2008 when the U.S. Committee on Foreign Investment placed Huawei's proposal to buy 3Com on hold. At that time, the Department of Defense was using 3Com's intrusion detection products, and Huawei's involvement was considered a potential security concern. The government later blocked Huawei's bid to build a national wireless network for first responders. In October 2012, the U.S. House Intelligence Committee released a warning discouraging telecom companies from doing business with Huawei. The report offered virtually no evidence of the security threat, while the U.S. government's later security review also found no evidence of Chinese spying technology.

From 2013-2014, tensions escalated as the U.S. government required the certification application for all Chinese I.T. products before they are purchased and accused Huawei of spying. The U.S. NSA broke into Huawei's headquarters, claiming to monitor the security of exported Huawei technology. Huawei's CEO declares the company's exit from the U.S. telecom market. The U.S. then banned the firm from bidding for any government contracts.

In 2018, both AT&T and Verizon dropped plans to sell Huawei phones in U.S. President Trump banned most Huawei technology from government use based on the

Defense Authorization Act and the number of products excluded has since increased. In response to the U.S.'s growing hostility, Huawei sued the U.S. for its purchasing ban. In late 2018, Huawei filed a request to the United States Federal Trade Commission (FTC) to reconsider how the FTC was policing privacy and approaching cybersecurity matters. On being asked about the request, a Huawei representative responded, "*Open competition promotes both innovation and investment… Unfortunately, competition in U.S. telecommunications markets has not been fully open for a long time. Instead, Huawei and certain other foreign entities have faced, and continue to face, regulatory intervention that has inhibited their ability to compete on the merits*".

In March 2019, Huawei sued the U.S. government over the unfair ban, quoted, "*This ban not only is unlawful, but also restricts Huawei from engaging in fair competition, ultimately harming U.S. consumers*". In May of 2019, the U.S. Commerce Department placed Huawei on a banned "Entity List", restricting exports of U.S. technology to Huawei. This resulted in Google rescinding Huawei's Android license for new phones, Microsoft temporarily removing Huawei laptops from its online store, and many other U.S. companies complying with the new regulation in ways that negatively affected Huawei's business. In October 2019, the U.S. FTC proposed banning carriers from using money from the Universal Service Fund to buy equipment from Huawei, ZTE, or other companies deemed to pose a national security risk, and further remove existing Huawei and ZTE equipment from their networks. However, the U.S. restrictions on domestic firms trading with Huawei could be a severe threat to their survival as a company. The U.S. has not followed through on these sanctions against Huawei by postponing its ban through May 15th, 2020. Huawei can still access to offerings from the U.S. market but at the mercy of the U.S. government. The U.S. semiconductor industry also quietly lobbied the Commerce Department and the White

House to ease the restrictions. On May 19th, 2020, the U.S. Commerce Department tightens the export rules by imposing license requirements for chipmakers using U.S. machines and software for manufacturing semiconductors for Huawei after September 15th. However, the U.S. Commerce Department license granted to the U.S. companies Intel, allowing it to continue supplying certain products to Huawei on September 22nd, while others are still waiting for the U.S. government's approval[2].

3.2 Australia

During Australia's National Broadband Network (NBN) construction, Australia allowed ZTE to tender for contracts in the NBN while blocking Huawei from doing the same. To counter its negative public security perception, Huawei offered up access to software codes and proposed creating a national security center to verify Huawei's products' security level. Australia accepted their offer. Several liberal-leaning officials supported a review of the ban in hopes of scrapping it, but the Prime Minister, Tony Abbott, ruled out changes of the ban. Huawei then turned to collaborate on Optus and Vodafone's 4G infrastructures throughout 2015 and 2016. Since June of 2017, Australia has banned Huawei from supplying its phones to Australia Defense and banned Huawei equipment in 5G networks.

In August of 2018, after much debate and discussion, Australia stated Huawei's exclusion from 5G networks, saying they could not develop, "*any combination of technical security controls that could sufficiently mitigate the risks*". Australia's ban resulted from the fear of critical infrastructure's foreign involvement, as allowing

[2] It was reported that the U.S. company AMD was also granted the license to supply Huawei. But we cannot find any official information. It was also reported that other chipmakers including Qualcomm, Micron Technology, Samsung, SK Hynix, Macronix International, MediaTek and Semiconductor Manufacturing International Corp also applied for the special licenses. But “non-U.S. firms may not have a high chance of getting U.S. approval”.

Huawei to establish its telecommunications network could give access to Chinese hackers. As hackers can access the network regardless of the country of origin of the equipment if the cybersecurity vulnerabilities exist, the basis of this argument indicates that the drivers for the decision to ban Huawei's 5G products are not just the technological vulnerabilities, but the concerns from geopolitical risks and the capability to manage such risks.

3.3 India

In 2006, India's Telecom Ministry blocked Huawei's application for a license to bid as an equipment supplier for large-scale Indian telecom projects. India's Intelligence Bureau suspected Huawei of ties to Chinese intelligence and military and had performed debugging sweeps of the Chinese Embassy in India. Later, in 2009, the Ministry of Defense warned telecom giant BSNL not to award equipment contracts to Huawei in suspicion of its connections with the Chinese communist party. India's Intelligence Bureau backed the Ministry of Defense's concerns.

In 2010, India's government issued a ban on Chinese network equipment companies, including Huawei, requiring all telecom projects to receive security approval by India's Home Ministry. In response, Huawei attempted to convince Indian security officials that they did not pose a security threat, emphasizing that its Indian operations were majority Indian nationals. India lifted the ban three months later but required all network equipment to pass strict security inspections for import approvals. Imports resume after Huawei complies with certification restrictions.

Since then, Huawei has maintained a relatively stable relationship with the Indian government and grow in the Indian market. In January 2020, India announced that "5G trials will be done with all vendors and operators... We have taken an in-principle decision to give 5G spectrum for trials." Though no 5G network rollout

contracts have been given to Huawei, Huawei is allowed to participate in the trials and access the India 5G market.

The tensions between India and China have been on the rise since June 2020, and 59 apps provided by China-based companies such as TikTok and Wechat are blocked on June 29th, 2020, Indian government ministers discussed the country's 5G rollout plans and whether Huawei should be allowed to participate. However, on September 17th, 2020, the Indian minister of state for electronics and information technology Sanjay Dhotre confirmed that the government had no plan to exclude Huawei from 5G network infrastructure contracts.

3.4 United Kingdom

For the United Kingdom, recent events involving Huawei have progressed in a much more positive direction than many other countries. In 2011, Huawei opened the Cyber Security Evaluation Centre (HCSEC) in the U.K., intending to improve cybersecurity trust between the company and the nation, while developing the U.K.'s cyber networks. A branch of the U.K.'s government intelligence agency would oversee the center's testing process.

In 2013, Parliamentary intelligence (ISC) voiced security concerns about Huawei's equipment, leading to a review of operations at the evaluation center. The review approved the center's operations. The U.K.'s national security adviser then established the Huawei Cyber Security Evaluation Centre Oversight Board to oversee and regularly report on the center's operational processes.

In their 2018 annual report, the HCSEC notes that a variety of Huawei's critical third-party software did not pass security-testing. The U.K.'s National Cyber Security Center (NCSC) concludes that using Huawei in 5G is a manageable risk by: "*As was made clear in July's HCSEC oversight board, the NCSC has concerns around Huawei's*

engineering and security capabilities," an NCSC spokesperson said. "*We have set out the improvements we expect the company to make*."

On April 24th of 2019, Theresa May agreed to let Huawei supply equipment for non-core elements of the United Kingdom's 5G network. The U.K. has made its cautious approach to Huawei's role in developing its 5G network. Still, their government ultimately believes they can implement specific measures to mitigate this risk. Huawei has reaffirmed this commitment by agreeing to sign "No-Spy" agreements with the United Kingdom and Germany, as well as extending one to the United States. This commitment will only be proven through an extended period free of incident, but Huawei has put themselves in a position to penetrate the European market, despite the U.S.' efforts to prevent this from happening.

Since the U.K. and Huawei entered in agreement for 5G development, several important occurrences have reflected the relationship between Huawei and the U.K. On October 1st, Huawei purchased a stake in Oxford Sciences Innovation (OSI), a large research fund company for the University of Oxford.

On November 1st of 2019, the U.K. chose to suspend a decision on Huawei's participation in 5G infrastructure until the next government, which reflects Britain's continued uncertainty about the security of Huawei's networks. This is most likely a result of the tension between the Trump and Johnson administrations, as the U.K. does not want to anger their most potent ally.

On January 28th, 2020, the United Kingdom followed through its agreement to let Huawei develop non-core elements of its 5G network. On June 25th, 2020, Huawei announced a 1.25 billion dollar investment to build a research facility in the U.K. However, on July 14th, 2020, the U.K.'s decision is changed again, requiring telecom operators not to buy any new equipment from Huawei since the end of 2020 and remove

Huawei equipment by 2027. But Huawei still announced a 10 million pounds investment later to open three new experience stores and customer service centers in the U.K.

3.5 Germany

In 2014, Huawei launched a program with the North Rhine-Westphalia government of Germany to allow German students to study Chinese by learning digital technology skills. This program was designed by Huawei for the students' intellectual benefit and helped establish the foundation for a healthy partnership between the telecom company and the German government.

In early February of 2019, Germany was caught between pressures from the U.S. and the European Union to ban Huawei and the importance of their relationship with the Chinese consumer market. The BDI industry association warned the German government that a ban on Huawei products could cause Beijing to retaliate against German companies operating in China. Along with the fear of direct retaliation, the German automobile industry also relies heavily on the sale of cars in China, potentially a problem if Germany refused Huawei's inclusion in its domestic market. In October of 2019, the German administration asserted that they would not ban Huawei from participating in developing the German 5G network despite the external pressures to do so. Government spokesman Steffen Seibert stated, "*Essentially our approach is as follows: We are not taking a pre-emptive decision to ban any actor, or any company*".

For Huawei, partnership with Germany this as an opportunity to build a different reputation in the eyes of the international community. In an emailed statement, a Huawei spokesperson noted, "*We welcome the move the German government has taken to create a level playing field for 5G network vendors…Politicizing cyber security will only hinder technology development and social progress while doing nothing to address*

the security challenges all countries face. Huawei will continue to work openly with regulators, customers, and industry organizations to ensure that mobile networks are secure". This also reflects one of Huawei's primary goals: to focus their 5G rollout on economic and communicational benefits instead of letting political constrictions dictate their growth.

Huawei has already been working closely with Germany's largest telecom provider, Deutsche Telekom, and Telekom claimed that a ban on Huawei would delay 5G rollout of up to 2 years. This necessity may be the deciding factor in how Germany proceeds with Huawei. Other 5G providers like Nokia and Ericsson remain significantly behind Huawei in technology development, which gives Germany little alternative if they want to move forward with 5G.

Late in 2019, Huawei secured an agreement from the German government to develop its 5G network elements. Shortly after this announcement, Germany suspended definitive commitment to permitting Huawei to supply 5G equipment until 2020. China has aided Huawei in its pursuit for 5G in Germany by threatening consequences if Germany chooses not to use Huawei in its new internet infrastructure.

On February 11th, 2020, Germany adopted the 5G strategy to tighten security requirements on all suppliers and bar untrustworthy companies that fail to fulfill a "clearly defined security catalogue which excludes the possibility of a foreign state exerting influence on our 5G infrastructure". This strategy opposes any attempt to single out Huawei but takes a risk-management approach to mitigate the potential cybersecurity risk from 5G network construction effectively.

4. Data Collection

As summarized in Table 2, following the model presented in Section 2, we further create a dataset of indicators to measure critical factors, which drive the diverse outcomes within the above cases.

Table 2: Measurements and Data Source

Variable	Measurements	Source
ICT Development Level	ICT Development Index (IDI)	ITU
Huawei-Host Business	Huawei's revenue and employee within the selected state.	Capital IQ
Home-Host State Relations	The Sino Bilateral Relation Index. PEW Opinion of the United States.	Tsinghua Sino Bilateral Relation Dataset; PEW Global Indicators Database
Political Resiliency	Marsh Political Risk Index. A higher score represents a more stable political environment for business and trade	Marsh, Fitch Solutions
National Cybersecurity Capability	Global Cybersecurity Index (GCI).	ITU
Governance Capability	Government effectiveness represents the quality of public services, the degree of its independence from political pressures, and the quality of policy formulation and implementation; Control of corruption represents the extent to which public power is exercised for private gain.	WGI
Trade Restriction in Telecom	OECD Service Trade Restriction in the Telecommunication sector.	OECD

The ICT development level is derived from the ITU ICT Development Index (IDI), a widely adopted indicator to monitor and compare ICT developments between nations. A higher IDI score represents a better level of ICT development. Regarding Huawei's business within the selected states, we extract the revenue and employee number of Huawei's subsidiaries within the selected states from Capital I.Q. The higher value represents a stronger business relationship within the selected state.

To compare the international relation between China and the selected state, we refer to the database developed by Tsinghua University, which quantifies the relations between China and other states over time. A higher score represents a better relation between China and the selected state. Because the U.S. has been pressuring other states to ban Huawei, the U.S and other four selected states' relations can impact the outcome.

Therefore, we include the PEW Opinion of the United States to determine the relations between the U.S. and other states. A higher score represents a more favorable opinion of the United States. For political risk, we use the Marsh Political Risk Index, which evaluates political and economic stability.

For the capability to mitigate potential cybersecurity risks, we use the Global Cybersecurity Index (GCI) published by the ITU to assess each nation's commitment to cybersecurity across five pillars (legal, technical, organizational, capacity building and cooperation) and evaluate each nation's general cybersecurity capability. A higher GCI score represents a better cybersecurity capability. We refer to the Worldwide Governance Indicators (WGI), which evaluate the quality of governance. A higher value corresponds to better governance. We consider two specific dimensions in this study: the government's effectiveness captures its degree of independence from political pressures, and policy formulation and implementation quality. The control of corruption captures perceptions of the extent to which public power is exercised for private gain.

Finally, for the path dependency effect, we consider the effect of trade restrictions on the telecommunications sector using the OECD Service Trade Restrictiveness Index database, which provides an objective overview of service trade restrictions. A higher score represents a more restrictive trade policy.

5. Comparative Analysis

5.1 Diversity in Public-private Co-governance Mode and Outcomes

Regarding the similar cybersecurity concern from Huawei's offerings, we observed diversity public-private co-governance behavior and outcomes, as shown in Table 3.

Table 3: Comparative Analysis of factors impacted Huawei's cases within selected states

	United States	Australia	India	United Kingdom	Germany

Trade policies' Impact	Market Decoupling	Market Prohibition	Pre-requirement for Market Access	Market Access Limitation	Pre-requirement for Market Access*
Public-private Mode	Cyberspace reterritorialization and compliance	Cyberspace reterritorialization and compliance	Government lead with corporation consultancy	Responsibility delegation	Responsibility delegation

*: Note that the implementation of the pre-requirement for market access in Germany is for 5G deployment and all the vendors need to fulfill the same requirements. In India, the current stage for 5G is only trials, while the security test requirements in 2010 are just for Huawei.

For the United States and Australia cases, the mode is *Cyberspace Reterritorialization and Compliance (CRC)* where governments implement the trade restrictions in response to national cybersecurity concerns and Huawei has very limited space to maneuver. With the United States case, the government's restrictions on Huawei are continuously escalating: from foreign investment limitation which limits Huawei's business expansion in U.S. market; to government procurement prohibition which builds restrictions of market access for Huawei products; to certification requirement to make pre-requirement for market access, the U.S. government has tried to create a standard under which including Huawei products is not acceptable, further isolating Huawei's products from the U.S. market. After attempting to comply and negotiate with the U.S. government, Huawei eventually decided to exit the U.S. market and sue the U.S. government for unfair treatment. Huawei's situation in Australia is very similar to the United States in that Australia built up the restrictions on Huawei over the years and eventually prevented Huawei from supplying 5G equipment in Australia. Unlike the U.S., Huawei's other offerings in Australia have not been prohibited yet.

For the United Kingdom and Germany cases, the mode is *Responsibility Delegation,* where governments delegate the responsibility to agencies to evaluate the related cybersecurity risks and coordinate 5G network construction where local telecom companies can choose different vendors, including Huawei, for 5G network development. In the United Kingdom, the effective operation of the Huawei Cyber

Security Evaluation Centre and Huawei Cyber Security Evaluation Centre Oversight Board enables the U.K. government to manage the potential cybersecurity risk from Huawei's offerings. Also, the signature of the "no-spy agreement" and continuing investments in the U.K. enhance the trust between Huawei and the U.K. government. Huawei was able to secure an agreement from the U.K. to develop non-core components for its 5G network. Though due to the increasing geopolitical pressure from the U.S., the U.K. decided to ban the purchase of new Huawei 5G equipment after December 31st, 2020, and require all Huawei 5G equipment should be removed from by the end of 2017, this did not close the door for Huawei's 5G business immediately but push it to future legislation. Germany has decided not to ban Huawei from participation in their 5G network directly but to adopt a risk-management approach to mitigate the potential cyber risk, creating an equal competition environment for Huawei and other 5G vendors. Germany's 5G market is the most open market for Huawei. Germany is implementing a risk-management approach distinction between access, transport, and core network, thus allowing different handling of components in the various parts of the 5G network where all the 5G vendors, including Huawei, must meet the same cybersecurity requirement.

For the India case, the mode is closest to *Government Lead with Corporation Consultancy* where the Indian government has implemented related trade restrictions, and Huawei took an active approach to negotiate, collaborate and twist the policies to get a better outcome. India has a different situation in comparison to the other four states. Before 2010, India quickly escalated restrictions on Huawei with government procurement restrictions, warning the local telecom companies not to purchase Huawei's offerings and setting the pre-requirements for importing Huawei, which is *de facto* market prohibition. After effective negotiation with the Indian government,

Huawei succeeded in convincing India that it poses no security threat to India through restructuring local management with more employee localization, downgrading the restrictions to certification requirement by security testing. Since then, Huawei's business spans across research and development (R & D), manufacturing and services in India, including an R & D centre in Bengaluru, which improves Huawei's relation with India. Eventually, Huawei received a green light from India for 5G trials.

5.2 Main Drivers behind the variance in different governance modes

Now we turn to investigate the key factors that drive these different public-private governance modes and outcomes within each case. This creates a comprehensive understanding of why interactions between different governments and Huawei have resulted in different governance modes and outcomes. The research deploys the conceptual framework developed in Section 2 to explain how benefit/cost factors, political concerns, and mitigation capacities in each country influence the dynamic interactions between governments and Huawei in the five-country cases (as shown in Table 4).

Table 4: Factors impacted Huawei's cases within selected states

		United States	Australia	India	United Kingdom	Germany
Benefit /costs	**ICT Development Level**	High	High	Low	High	High
	Huawei-Host Employee	High - Medium	Low	High	Medium	High
	Huawei-Host Revenue	Low	Low	High- Medium	High- Medium	High
Perceived Risk	**China-Host relationship**	Low	High- Medium	Medium- Low	Medium	High
	Opinion of the United States	/	High	High	High	Medium
	Political Resiliency	High	High	Medium	High	High
Mitigation Capability	**National Cybersecurity Capability**	High	High - Medium	Medium	High	High - Medium
	Governance Effectiveness	High	High	Low	High	High

	Control of Corruption	High	High	Low	High	High
Path Dependence	**Trade Restriction in Telecom**	Medium-low	Medium-low	High	Medium-low	Low
Trade Regimes' Impact		Market Decoupling	Market Prohibition	Pre-requirement for Market Access	Market Access Limitation	Pre-requirement for Market Access*
Public-private Mode		Cyberspace reterritorialization and compliance	Cyberspace reterritorialization and compliance	Government lead with corporation consultancy	Responsibility delegation	Responsibility delegation

The United States. As reported in Table 4, the U.S. faces less cybersecurity risk than other countries considering Huawei as the U.S. has the best cyber offensive and defensive capability globally. This means the U.S. could potentially exact significant benefit from partnering with Huawei without compromising cybersecurity. Furthermore, the U.S.'s score in the development of information and technology is lower than both Germany and the United Kingdom, which means that they could benefit from Huawei's comparatively higher data processing speeds and 5G capability. The high government effectiveness, control of corruption, high political stability, and low trade restrictions in telecommunication, reveal a low-risk environment for international business. Huawei has a large group of employees in the U.S. subsidiary, which is founded dated back to 1993. This indicates a related strong business loyalty for Huawei in the U.S. market. However, we can see that the United States government has expressed an increasing level of hostility towards Huawei and its international development over these years. Since Huawei was placed on the Banned Entity list, the U.S. has generally excluded platforms associated with Huawei from the U.S. market. The only factor identified in our conceptual model that can move the direction toward such restriction is the increasingly tensive relation between U.S. and China. This means that the Huawei ban in the U.S. market is more driven by the cyberspace reterritorialization trend. It has been politicized, which is consistent with the argument

that cybersecurity-related trade restrictions have less to do with cybersecurity (Ikenson, 2017).

Australia. Recently, Australia has made it clear that they can't fully rely on the internal ability to mitigate the cybersecurity risks that have been associated with Huawei. However, Australia's GCI score is, in fact, relatively high, even higher than Germany's, indicating that the high risk-mitigation capacity exists in Australia. Australia has the potential for significant benefit in using Huawei equipment, specifically in expediting a 5G rollout that would be significantly slowed by not using Huawei. Australia also has a relatively low political risk level, high government effectiveness, reasonable control of corruption, and low trade restrictions in telecommunication. Furthermore, Australia and China have a good international relation, which indicates that the home and host state relations will not hinder but benefit Huawei's business in Australia. The main factor driving Australia to ban Huawei's 5G business is another political concern, namely its close relations with the United States. Australia is a member of the Five Eyes intelligence community, and the U.S. has threatened to limit intelligence sharing with nations that give Huawei a 5G role. Therefore, Huawei's 5G prohibition in Australia can be considered as a manifestation of balancing the U.S. and China's influence in Australia.

India. In terms of factors determining final decisions, India has the most contradicting self-interests. They have significantly less capability in mitigating cybersecurity risks with the lowest cybersecurity capability and a much higher level of political risk. Additionally, India's trade restrictions in telecommunication remain considerably higher than in the other four countries. These factors contribute to the development of restrictions on Huawei's 5G offering. On the other hand, India lags behind the other four

countries around 5 points in ICT score, meaning that they seek serious advancement in technological development. Hence, India stands to gain the most from partnering with Huawei. Their domestic telecom companies are struggling, and Huawei would provide much needed economic relief to these companies. The CEO of Bharti Airtel, like many others, has proclaimed Huawei as far superior to competitors Nokia and Eriksson. Additionally, the low government effectiveness and control of corruption in India enable the international business to take a more active approach to bargain with the local authority to assimilate into the regions of interest. For example, Huawei's effective negotiations with India in 2010 to degrade the prohibition to security testing was critical to enabling Huawei's further investment in India to build up their market reputation, which initiated the loop to reduce the business restrictions. We can see that the governance mode between India and Huawei belongs to the Government Lead with Corporation Consultancy.

United Kingdom. The United Kingdom has the highest GCI, meaning that they have the best capabilities for mitigating cybersecurity risks. The U.K. announced they would allow Huawei to develop their 5G network elements because of the conclusion that taking on Huawei would be a manageable risk. The United Kingdom's partnership with Huawei can be seen as a positive boost for Huawei's international reputation. This indicates that cybersecurity risks are unavoidable under any circumstances and that what is more important is each country's ability to protect infrastructure from cyber-attacks. Out of the five selected countries, the U.K. has the highest score for the development of the internet and technology. This means that they are almost ready to move toward 5G, which would explain why they took the first step to build their 5G infrastructure. However, the relationship between the United Kingdom and the United States, specifically Donald Trump, must also be considered. Trump has made it clear

that he wants nothing to do with Huawei in the United States and has persistently encouraged his allies to do the same. Because of this, the U.K. held off on a decision until 2020. The U.K. allows Huawei a limited role in its 5G network on January 28th, 2020 which prevents Huawei's equipment from being used in sensitive core parts of 5G and cap Huawei's involvement at 35% of non-sensitive parts.

Therefore, though the U.K. takes the responsibility delegation mode to govern the potential cybersecurity risks from Huawei's 5G adoption, the pressure from the U.S.' politicization of 5G networks has pushed the U.K. to implement limitations in their market. As the U.K. has deemed Huawei's offerings a "manageable risk", Huawei can help move countries in the right direction so that, again, they achieve a model for Carrier Business in which Huawei's clients feel comfortable purchasing their 5G equipment. As they have invested in research in the U.K. related to cybersecurity, Huawei has aided the U.K. in building its capabilities to achieve benefits for both parties.

Germany. Germany has a relatively high ICT development level, indicating its readiness to roll out its 5G network. Though Germany's cyber risk mitigation capability remains inferior to the United States and the United Kingdom, which could influence their decision on Huawei, first-echelon cybersecurity capability still provides Germany with the confidence to manage potential cyber risks from 5G development and deployment. Additionally, the high political stability represented by a high Marsh Political Risk score, superior government effectiveness, and control of corruption, and the lowest trade restrictions in telecommunication presents Germany as a friendly business environment for 5G service providers. Therefore, cybersecurity governance in Germany is closer to responsibility delegation. Among the five selected states, Germany has the closest relation with China and the lowest opinion of the United States, which means

that Germany should be able to resist pressure from the U.S and pursue their interests without significant external interference.

Huawei also has the largest number of employees and gains the highest revenues in the German market. Germany's three network operators are all using Huawei technology. In December 2019, German network provider Telefonica Deutschland chose Huawei, partnering with Nokia to develop the first part of its radio access network. However, in February 2020, Nokia was dropped from all but one of Telefonica Deutschland' dozen markets and required to improve its products and service.

6. Discussion and policy implications

6.1 Determinants of public-private co-governance modes

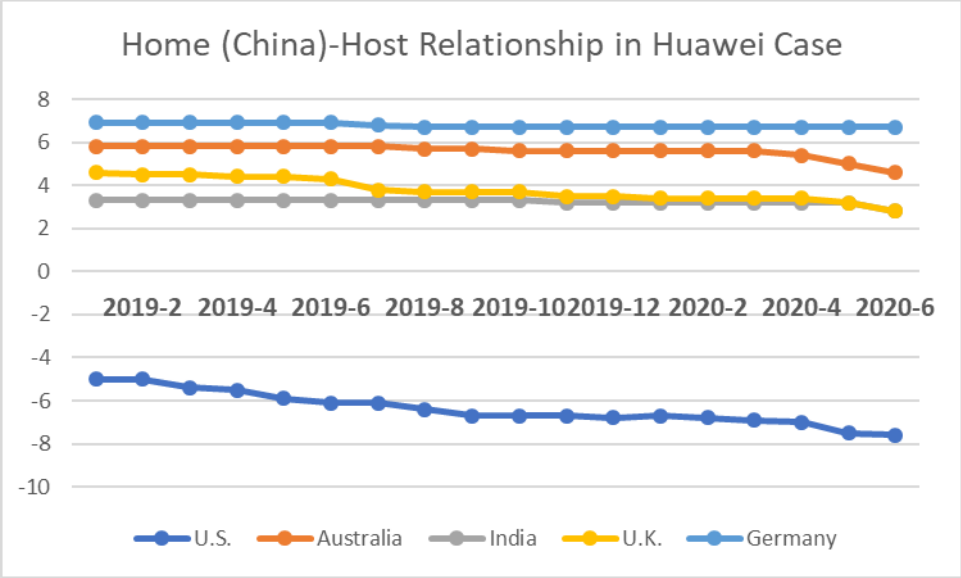

Figure 4. The Evolution of Home-Host Relationship in Huawei case from Jan 2019 to Jun 2020. Source: Tsinghua Sino Bilateral Relation Dataset.

Huawei's future direction will be significantly dictated by the balance between the United States and China regarding the U.S. politicization of cybersecurity within 5G networks. The U.S. has made it clear that it will continue to influence their allies' decisions on how to handle Huawei. The impacts of U.S. restrictions on Huawei are different. As shown in Australia, the U.S.' efforts to interfere with Huawei's business

are more effective, given Australia's highest reliance upon the U.S. Though the U.K has agreed to let Huawei participate in developing their 5G network, we can observe restrictions that would not exist without the U.S.' political pressure. Notably, as shown in Figure 4, the China-U.K. relation is significantly decreasing since Feb 2020, this somehow explains the increasing restrictions to Huawei's 5G equipment in the U.K. On the other hand, Germany's capability to balance between China and the U.S. results in a relatively fair 5G market environment for all vendors, including Huawei.

The host government's capability to manage cybersecurity risks plays a critical role in the decision-making process. Governments with a high cybersecurity capability will consider the cybersecurity risk from Huawei's offering as manageable, so they are more likely to take the responsibility delegation mode and adopt a risk-oriented approach. Comparing the Australia and United Kingdom cases, given the similar pressure from the U.S. and political stability, higher cybersecurity capability moved the U.K. to implement market limitations instead of resort to completely prohibition like Australia.

Being consistent with previous studies for political risk mitigation (Gamso & Nelson, 2019; John & Lawton, 2018), building trust and effective collaboration mechanisms with government and businesses in the host state is important for corporations to mitigate the national cybersecurity concerns. As the Germany case demonstrates, trust and business loyalty developed over time can result in governance modes like responsibility delegation, where a cyber-risk-management-oriented approach is adopted, and the cyber risks from digital innovation adoption are depoliticalized. On the other hand, for a government like India that has a lower governance capability and national cybersecurity capability, but also has a desire to play a more critical role in cyberspace, given the ill-defined institutional systems for cybersecurity governance, the

government lead with corporation consultancy is more likely to be adopted. In contrast, restrictions based on cybersecurity concerns can be used as a tool to focus international corporations on collaborating with local governments and allocating resources to build cybersecurity capability. Involvement in the policy-making process and enhancement of political capacity is critical for corporations to avoid, or at least alleviate the impact of potential restrictions related to cybersecurity concerns.

6.2 Strategies of corporations in the fragmented cybersecurity governance system

Considering the inherent cybersecurity risks from digital technologies, it is clear that the fundamental implication for Huawei moving forward will be its commitment to and reputation of establishing networks secure from cyber threats and developing effective cyber incident response capabilities. Given the fragmented cybersecurity governance in the digital trade system, corporations like Huawei and other corporations related to cross-border digital innovations should align their different strategies to support their global business.

In a market where cybersecurity concerns have been politicized, and the feedback loop of cyberspace reterritorialization is too strong to break, temporarily exiting the market can be a good option. Recently, Huawei has made a case for unconstitutional treatment by the U.S. government in U.S. courts. In this case, Judge Mazzant, has distanced Huawei from similar cases (i.e. Kaspersky) by expressing confusion in how to proceed. This will not result in Huawei's tangible progress in the near future, and the U.S. market is naturally a much more distant goal than any other for Huawei. However, by defending its reputation in the U.S., Huawei will improve its long-term partnership with other countries.

However, corporations should pay attention to the foreign market re-entry strategy after exiting the market, especially when market prohibition only covers a

subset of a corporation's business and is driven by external influences. It is uncommon for global firms to re-enter foreign markets; however, an effective re-entry strategy is critical for market performance when corporations can come back to the market (Javalgi, Deligonul, Dixit, & Cavusgil, 2011; Surdu, Mellahi, & Glaister, 2019; Surdu, Mellahi, Glaister, & Nardella, 2018). Huawei owns around 55% of 4G market share in Australia. However, due to the 5G ban, it is drying up its pipeline of work, indicated by a relatively low number of employees and revenues generated from Australia's subsidiary. This may initiate a "dangerous" loop that would continue to reduce Huawei's business in Australia, which can then harm the perception of its loyalty within the Australian market, consequently decreasing the capability to balance the U.S. pressure and resulting in a higher-level of restriction for Huawei in other markets. This is a situation that Huawei should avoid. Regarding that it is unlikely that Australia will lift the 5G ban on Huawei in the short term, a better strategy for Huawei is to temporarily exit the Australian 5G market, and delegate resources to other offerings to improve their reputation within the market and prepare a re-entry strategy when it is suitable. Like they had done before, when Huawei was excluded from the National Broadband Network (NBN) due to similar cybersecurity concerns, Huawei moved on to develop other business aspects, including 4G infrastructure and mobile phone, to forge different positive business relationships. Additionally, as the Australian government has excluded Huawei 5G because they believe they "cannot successfully mitigate the risk", there is a good opportunity for Huawei to invest in private firms that could improve Australia's cybersecurity infrastructure.

In markets where the host government has a limited cybersecurity governance capability, corporations should take a more active approach by developing their political capacity and continuing the trend of cybersecurity depoliticization (Holburn & Zelner,

2010; John & Lawton, 2018). Though Huawei was allowed to participate in India's 5G trial phase, it is critical for Huawei to further enhance their bargaining power with India governments to avoid market prohibition in the future 5G development and deployment. Beyond improving their connections with the local business and government, Huawei can also take a more active approach by delegating more resources to support India's cybersecurity capability building, reducing the concerns on potential cybersecurity risks from the adoption of Huawei's offerings. Building an effective collaboration with the India government to balance the desire to develop ICT and the concern of potential cyber risks from cyberspace reterritorialization should be a top issue for Huawei's executive. An inspiring example is that in Mexico, Huawei worked out a deal that entailed a 1% interest loan in 4G into the Mexican market on their part, conditional upon 80% of funding in Mexico being spent with Huawei.

7. Conclusion

Cybersecurity concerns are becoming a critical roadblock for cross-border digital activities, especially those related to essential cyberinfrastructure like 5G networks. The public-private co-governance on cybersecurity concerns within digital trade is crucial in effectively managing the cybersecurity risks and supporting these cross-border digital innovation adoptions. By highlighting the cyberspace reterritorialization trend, the diversity of trade regimes for cybersecurity risk mitigation, and the public-private co-governance, this study conceptualizes a systematic framework to understand the factors driving the implementation of trade policies and public-private co-governance mode selections. Using this model, the comparative case study regarding cybersecurity concerns around Huawei's 5G offerings in the United States, Australia, India, United Kingdom, and Germany, reveals the main drivers for decision-making within these states. Importantly, the developed framework can provide valid explanations of the

changing outcomes within each case, demonstrating the robustness of this study's findings.

As each country has its own unique political and economic ecosystem, this study unfolds cybersecurity governance's complexity within digital trade by developing a comparative analysis framework. The cyberspace reterritorialization is already a reality that business leaders and policymakers need to accept (Farrell & Newman, 2020). This study shows that businesses in both developing and developed countries need to confront the political risk from cybersecurity concerns. Such political risk can be determined by the host state's own government and the balance between the U.S and China and how it affects the specific country. The national cybersecurity capability and governance capability will shape the co-governance mode selections and corporations' active involvement in government systems, including cybersecurity capability building, business loyalty construction, and bargaining power enhancement. These provide a baseline for business leaders and policymakers to develop the cybersecurity co-governance schema within digital trade.

Not only the 5G network can raise cybersecurity concerns in digital trade. Given the growing global digitalization, we can expect that all products and services related to digital infrastructure, algorithm and code, and data will be impacted. For example, on January 5th, 2020, the U.S. imposed restrictions on the export of certain artificial intelligence (A.I.) programs, which are considered as emerging technologies essential to national security. Therefore, all international firms need to acknowledge this trend. The public-private co-governance modes and the drivers behind the variance in different governance modes discussed in this paper will enable these multinational firms to prepare for it actively. Otherwise, they are likely to run into serious trouble.

The limitation of this study raises more questions that open up opportunities for future work. Only publicly available reports are used in this study, and some interaction details are not considered. A follow-up study to grasp more details on the interaction dynamic will be valuable. Additionally, we can identify the main drivers for each selected case that causes diverse outcomes. Notably, the dynamic balancing of these factors within these cases are changing the decisions. Therefore, a future study to understand the effectiveness and dynamics of different factors within different contexts can produce more systematically-relevant insights for cybersecurity governance within digital trade.

Acknowledgement

This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium. Fang Zhang is the corresponding author.

Reference

Aaronson, S. A. (2018). What are We Talking About When We Discuss Digital Protectionism? In *SSRN*. https://doi.org/10.2139/ssrn.3032108

Berman, P. S. (2018). Legal Jurisdiction and the Deterritorialization of Data. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3134782

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical I.T. systems. *Technovation*, *34*(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001

Carr, M. (2016). Public – private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and

Behaviors Polycontextual Contrasts Between the united states and china. *MIS Quarterly*, *40*(1), 205–222.

Choucri, N. (2012). Cyberpolitics in International Relations. In *Cyberpolitics in International Relations*. https://doi.org/10.7551/mitpress/7736.001.0001

Christensen, K. K., & Petersen, K. L. (2017). Public-private partnerships on cyber security: A practice of loyalty. *International Affairs*, *93*(6), 1435–1452. https://doi.org/10.1093/ia/iix189

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi.org/10.25300/misq/2019/15117

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

Eduardsen, J., & Marinova, S. (2020). Internationalisation and risk: Literature review, integrative framework and research agenda. *International Business Review*, *29*(3), 101688. https://doi.org/10.1016/j.ibusrev.2020.101688

Farrell, H., & Newman, A. L. (2020). Choke Points. *Harvard Business Review*, (February).

Gamso, J., & Nelson, R. C. (2019). Does partnering with the World Bank shield investors from political risks in less developed countries ? *Journal of World Business*, *54*(5), 100997. https://doi.org/10.1016/j.jwb.2019.100997

Gertz, G. (2018). Commercial diplomacy and political risk. *International Studies Quarterly*, *62*(1), 94–107. https://doi.org/10.1093/isq/sqx079

Graham, E., Shipan, C., & Volden, C. (2013). The Diffusion of Policy Diffusion Research. *British Journal of Political Science*, *43*(3), 673–701.

Grindal, K. (2019). Trade regimes as a tool for cyber policy. *Digital Policy, Regulation and Governance* , *21*(1), 19–31. https://doi.org/10.1108/DPRG-08-2018-0042

Holburn, G. L. F., & Zelner, B. A. (2010). Political capabilities, policy risk, and international investment strategy: Evidence from the global electric power generation industry. *Strategic Management Journal*, *31*(12), 1290–1315. https://doi.org/10.1002/smj.860

Huang, K., & Madnick, S. E. (2020). Cyber Securing Cross-border Financial Services: Calling for a Financial Cybersecurity Action Task Force. *19th Annual Security Conference*. Las Vegas.

Huang, K., Madnick, S. E., & Johnson, S. (2019). Interactions Between Cybersecurity and International Trade: A Systematic Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3370562

Javalgi, R. (Raj) G., Deligonul, S., Dixit, A., & Cavusgil, S. T. (2011). International Market Reentry: A Review and Research Framework. *International Business Review*, *20*(4), 377–393. https://doi.org/10.1016/j.ibusrev.2010.08.001

John, A., & Lawton, T. C. (2018). International Political Risk Management : Perspectives , Approaches and Emerging Agendas. *International Journal of Management Reviews*, *20*, 847–879. https://doi.org/10.1111/ijmr.12166

Joseph, S. N. J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71. https://doi.org/10.1162/ISEC

Kho, S., & Petersen, T. (2019). Turning the tables: The United States, China, and the WTO national security exception. *China Business Review*, *2018*(August), 5–9.

Lambach, D. (2019). The Territorialization of Cyberspace. *International Studies Review*, 1–25. https://doi.org/10.1093/isr/viz022

Li, J., Newenham-Kahindi, A., Shapiro, D. M., & Chen, V. Z. (2013). The Two-Tier Bargaining Model Revisited: Theory and Evidence from China's Natural Resource Investments in Africa. *Global Strategy Journal*, *3*(4), 300–321.

https://doi.org/10.1111/j.2042-5805.2013.01062.x

Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. "Andy." (2019). What Users Do Besides Problem-Focused Coping in the I.T. Security Context: An Emotion-Focused Coping Perspective. *MIS Ouarterly*, *43*(X), 1–22. https://doi.org/10.25300/MISQ/2019/14360

Lindsay, J. R. (2017). Restrained by design: the political economy of cybersecurity. *Digital Policy, Regulation and Governance* , *19*(6), 493–514. https://doi.org/10.1108/DPRG-05-2017-0023

Linton, J. D., Boyson, S., & Aje, J. (2014). The challenge of cyber supply chain security to research and practice - An introduction. *Technovation*, *34*(7), 339–341. https://doi.org/10.1016/j.technovation.2014.05.001

Madnick, S. (2019). These are the cyberthreats lurking in your supply chain. *MIT Sloan IDEAS MADE TO MATTER*, 1–5.

Madnick, S., Johnson, S., & Huang, K. (2019). What Countries and Companies Can Do When Trade and Cybersecurity Overlap. *Harvard Business Review*, *January*, 1–6. Retrieved from http://web.b.ebscohost.com.ezproxy.northampton.ac.uk/ehost/pdfviewer/pdfviewer?vid=17&sid=2b1ec8bb-7ab9-4061-8f64-7044e3bdde2f%40sessionmgr103

Mahoney, J. (2000). Path dependence in historical sociology. *Theory and Society*, *29*(4), 507–548. https://doi.org/10.1023/A:1007113830879

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

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), 381–401. https://doi.org/10.1111/j.1468-2478.2010.00592.x

Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly*, *32*(2), 198–206.

Meltzer, J. P. (2019). Governing Digital Trade. *World Trade Review*, *18*(S1), S23–S48. https://doi.org/10.1017/S1474745618000502

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/misq/2018/13853

Pierson, P. (2000). Increasing Returns, Path Dependence, and the Study of Politics. *American Political Science Review*, *94*(2), 251–267.

Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229–252. https://doi.org/10.1093/jopart/mum015

Surdu, I., Mellahi, K., & Glaister, K. W. (2019). Once bitten, not necessarily shy? Determinants of foreign market re-entry commitment strategies. *Journal of International Business Studies*, *50*(3), 393–422. https://doi.org/10.1057/s41267-018-0167-3

Surdu, I., Mellahi, K., Glaister, K. W., & Nardella, G. (2018). Why wait? Organizational learning, institutional quality and the speed of foreign market re-entry after initial entry and exit. *Journal of World Business*, *53*(6), 911–929. https://doi.org/10.1016/j.jwb.2018.07.008

Tang, T., & Ho, A. T. K. (2019). A path-dependence perspective on the adoption of Internet of Things: Evidence from early adopters of smart and connected sensors in the United States. *Government Information Quarterly*, *36*(2), 321–332. https://doi.org/10.1016/j.giq.2018.09.010

US White House. (2019). Executive Order on Securing the Information and Communications Technology and Services Supply Chain.

Voon, T. (2019). The Security Exception In WTO Law: Entering a New Era. *AJIL Unbound*, *113*(ii), 45–50. https://doi.org/10.1017/aju.2019.3

Voss, M. D., & Williams, Z. (2013). Public-private partnerships and supply chain security: C-TPAT as an indicator of relational security. *Journal of Business Logistics*, *34*(4), 320–334. https://doi.org/10.1111/jbl.12030

W.Welch, E., K.Feeney, M., & Park, C. H. (2016). Determinants of data sharing in U.S. city governments. *Government Information Quarterly*, *33*(3), 393–403.

Weiss, M., & Jankauskas, V. (2019). Securing cyberspace: how states design governance arrangements. *Governance*, *32*(2), 259–275. https://doi.org/10.1111/gove.12368

Welch, G. L. D. (2011). Cyberspace – the Fifth Operational Domain. *IDA Research Notes*, 1–7.

Appendix

A. Definition of Digital Trade

Digital trade is a very broad concept, and there is no single, recognized and accepted definition. As shown in Table S.A., its scope and definitions can vary across countries and organizations.

Table S.A. Definition of Digital Trade

Organization	Definition of Digital Trade	Reference
U.S. International Trade Commission (USITC)	The delivery of products and services over either fixed-line or wireless digital networks	United States International Trade Commission. (2017). Global digital trade 1: Market opportunities and key foreign trade restrictions, (August), 332–561.
McKinsey	The use of digital technologies (ICTs) to conduct cross-border business, including the direct exchange of digital goods, digitally enabled exchanges of services or labor, and cross-border data flows that would not normally be considered as "trade"	Lund, S., & Manyika, J. (2016). How Digital Trade is Transforming Globalisation. E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, (January).
United Nations Conference on Trade and Development (UNCTAD)	Purchases and sales conducted over computer networks, involving physical goods as well as intangible (digital) products and services that can be delivered digitally	UNCTAD Intergovernmental Group of Experts on E-Commerce and the Digital Economy, UNCTAD Manual for the Production of Statistics on the Digital Economy, 2019

WTO	The production, distribution, marketing, sale or delivery of goods and services by electronic means	WTO, Electronic commerce, https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm
OECD	Digitally enabled transactions in trade in goods and services which can be either digitally or physically delivered involving consumers, firms and governments	Lopez-Gonzalez, J., & Jouanjean, M. (2017). Digital Trade: Developing a Framework for Analysis Digital Trade View project. OECD Trade Policy Papers, (July), 24. https://doi.org/10.1787/524c8c83-en
OECD-IMF	All international trade flows that are either digitally ordered, digital-platform-enabled, or digitally delivered	IMF. (2018). Towards a Handbook on Measuring Digital Trade. Thirty-First Meeting of the IMF Committee on Balance of Payments Statistics.
Brookings	The use of internet data flows globally by businesses and consumers for communication, e-commerce, and as a source of access to information and innovation, which is transforming international trade into digital trade	Meltzer, J. P. (2019). Cybersecurity and Digital Trade: What Role for International Trade Rules? Brookings. https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-and-digital-trade_final-11.20.pdf

In this study, we focus on cybersecurity risks from digital trade, as services and products with internet connectivity can introduce cyber attack vectors. Hence, governance of cybersecurity risks within digital trade covers a broad array of products and services, including computers and networking equipment, medical devices, videoconference services, software products, security software, social media, security cameras, banking I.T. systems, drones, smartphones, smart toys, online content services, satellite communications, A.I. software, and financial services such as international

fund transfers and payment systems. In essence, almost any product or service that contains or uses a computer (usually connected to a network) constitutes digital trade – which is almost every modern product or service.