Does High Cybersecurity Capability Lead to Openness in Digital Trade? The Mediation Effect of E-Government Maturity

Keman Huang
Sloan School of Management, MIT
keman@mit.edu

Stuart Madnick
Sloan School of Management, MIT
smadnick@mit.edu

Abstract

Cybersecurity risks threaten the digital economy, including digital trade enabled by digital technologies. As parts of cybersecurity capability building, governments implement fragmented, in-flux policies to manage cybersecurity threats from cross-border digital activities. However, the lack of shared understandings of cybersecurity within cross-border digital innovations raises an increasing debate about how cybersecurity capability building policies can impact digital trade restrictions. This study develops a National Cyber Trade Behavior model to examine the relationship between national cybersecurity capability and digital trade restrictions. Utilizing the PLS-SEM-based path analysis, we draw empirical evidence to verify the developed model and reveal that building cybersecurity capability can indirectly support an open digital trade system, mediated by E-government maturity.

1. Introduction

Our modern society is moving toward digital society driven by transformational information technology [17], including how trade happens and what is being traded. Digital trade, loosely defined as transactions of trade in goods and services which are digitally ordered, enabled, or delivered [25], has become a driving force of global digital economic growth. Although digital trade is unlocking more business opportunities, weak cybersecurity within digital technology is becoming a growing threat [8, 18]. As digital trade sits at the intersection of digitization and trade, it is affected by governments' increasing policies to manage cybersecurity threats from digital trade. Given the lack of standard rules of cybersecurity [22], we can observe two different policy implementations that can impact the cross-border digitization.

Some governments seek to implement policies to restrict digital innovation to maintain political stabilities, trust, personal and national cybersecurity, and enforce the cyber-sovereignty. For instance, on May 15, 2019, the U.S. issued the "executive order on securing the information and communications technology and services supply chain," declaring a national emergency to deal with the threats from information and communication technologies (ICTs). 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.

On the other hand, some nations are also implementing cybercrime legislation, national cybersecurity strategies (NCS), computer emergency response teams (CERTs), etc. to improve their capabilities to mitigate potential cyber threats and ensure cyberspace resilience. For example, as one of the first countries to create a cybersecurity strategy in 2008, Estonia has invested significantly in cybersecurity. The Estonian Information Security Association (EISA) was founded in 2018 to further coordinate cybersecurity commitments, including supporting the E.U. contractual Public-Private-Partnership model on cybersecurity.

Though these two types of policy implementations are not exclusive, some studies claimed that governments implement digital trade restrictions in the name of protecting critical infrastructure and national security from cyber threats, but have little to do with cybersecurity [14]. Others claim that these cybersecurity rules can address national security issues, ensure consumer privacy, and create a more secure digital society [22, 36]. Due to the lack of understanding of how cybersecurity and digital trade are connected, these debates create significant uncertainty for the global digital economy. Hence, this study aims to answer the following question: how does the national cybersecurity capability building impact digital trade restrictions?

By contextualizing the studies on security behaviors [1] to the digital trade system, we consider building cybersecurity capability as a national behavior to increase the endogenous ability to mitigate cyber threats, and implementing digital trade restrictions as a national behavior to control and avoid cyber threats. Furthermore, the policy diffusion theory [10] suggests that the path dependency, internal actor, and external actor can impact public policy adoption and diffusion, which can apply to digital trade systems. As the e-government maturity can increase transparency, public access to information, and digital innovation adoption

URI: https://hdl.handle.net/10125/71146
978-0-9981331-4-0

[21, 32], it can increase the governmental knowledge about digitization and twist the implementation of digital trade policies. Based on these propositions from information systems, public policy, digital trade, and the e-government discipline, this study develops a National Cyber Trade Behavior model to analyze the impact of national cybersecurity capability building on digital trade restrictions.

Based on the empirical evidence from 46 countries representing more than 80% of international trade in services, this study reveals a significant negative impact from national cybersecurity capability to the digital trade restrictions, which is indirect and mediated by E-government maturity. In other words, the cybersecurity capability building efforts which can improve the e-government maturity can eventually reduce digital trade restrictions. Otherwise, they may turn out as digital trade restrictions. Instead of deterring the adoption of digitization, cyber incidents can motivate investment in cybersecurity, promote E-government maturity, and foster a more open digital trade system.

These findings provide a tool for business leaders and policymakers to manage cybersecurity threats within digital trade systems. The developed model suggests that a nation with high trade dependency, high e-government maturity, and high cybersecurity capability will have low digital trade restrictions. If the cybersecurity policy can promote e-government maturity, it has a high potential to reduce digital trade restrictions. This mediation effect of e-government maturity will support international business, especially multinational enterprises, to evaluate the potential cybersecurity policy risk in a specific international market and align their global digital strategy to identify opportunities and avoid costly surprises. It also suggests that cybersecurity capability practices from those nations with high e-government maturity can be more practical to mitigate cybersecurity threats from digital trade. Hence the international community should learn from those practices to build applicable norms to manage cyber threats within digital trade.

2. Literature Review

2.1 Information Security Behaviors

Many studies on individuals' security behaviors [1, 23][1] have made significant progress in understanding the processes that motivate individuals to take protective actions, seek help, or avoid different security threats. Many factors can influence individuals' cognitive reasoning, such as costs/rewards, facilitating conditions, formal/informal punishment, perceived behavioral control, response efficacy, severity, shame, subjective norms, susceptibility and violation motivation, national culture, etc. Such reasoning will drive individuals to take a problem-focused coping action to protect themselves against cyber threats or avoid adopting technologies to forbear the threats.

At the organizational level [6, 33], organizational factors such as the support of top management and the available internal resources, etc.; environmental factors such as the peer pressure, the availability of the external support resources and the national culture, etc.; and technical factors including the relative advantage, perceived complexity, compatibility, and trainability, etc., collectively influence the organizational decision to adopt new technologies. Whitman's framework [34] provides a holistic view of the policy development lifecycle and has been widely adopted to develop and implement organizational information security policies.

While these above studies have provided revelatory insights about individual security behavior and organizational adoption, the interaction between different behaviors is somewhat overlooked. When we consider security behavior at the national level, the mechanism for national-level policies can be somewhat different. A study revealing how nations balance the two cybersecurity behaviors is needed. Additionally, the current findings of the factors that influence behaviors, such as the response efficacy, self-efficacy, perceived costs, etc. are not always consistent from different studies [15]. These inconsistent results warrant more empirical studies and testing, especially when considering security behaviors within a different context: national cybersecurity behaviors for digital trade. Furthermore, many existing studies focus on compliance and non-compliance with information security policy [23, 37]. The understanding of the information security policy itself, especially within the digital trade system, are limited.

2.2 Impacts of Digital Trade Restriction

Due to the increasing importance of digital trade to economic growth, digital trade policy, innovation and governance are relatively new but critical. Drawing from case studies on health services, online advertising, and uses of customer data for operational efficiency, Goldfarb and Tucker revealed that privacy regulations

[1] A variety of theories, including deterrence theory, control theory, institutional theory, protection motivation theory, theory of planned behavior, emotional theory etc. have been developed to delve into the behavioral aspects of individual security behaviors. Due to space limitations, instead of acknowledging each paper, we refer to two recent literature review articles that summarize the state-of-the-art of studies on individual security behaviors.

negatively impact innovative activities [9]. A few empirical models are developed to quantify the effect of restrictive policies on innovation and productivity. For example, the Global Trade Analysis Project (GTAP) model is used to estimate the negative economic impact of the E.U. General Data Protection Regulation (GDPR), concluding a loss of more than 300,000 jobs and 1.3 percent of GDP due to trade reduction [20]. The restrictive data policies tend to reduce the company's productivity across different industry sectors, particularly those that are more data-intensive [7].

These studies mostly focus on the negative impact of data restriction policies. However, digital trade is much broader than just data flow [25]. Digital trade restrictions also include policies like tariffs on digital goods, filtering and blocking, Intellectual Property Rights (IPR) infringement, national standards, and burdensome conformity assessment and regulations to limit disinformation and DDoS attacks [22]. The implementation of these digital trade restrictions is also unclear, making it difficult for organizations to understand the global digitization environment. It is critical to study the factors that impact the adoption of such digital trade restrictions.

2.3 Policy Adoption and Diffusion

Policy diffusion theories have been developed to understand how states/nations adopt new public policies and the factors that influence policy adoption [10, 29, 30]. The Walker-Gray-Berry-and-Berry framework has served as the cornerstone framework for studies on policy diffusion: Walker conceptualized and tested the policy diffusion in the U.S. states' context, Gray developed the now-standard S-curve pattern to characterize policy adoption. The event history analysis (EHA) was introduced by Berry and Berry to study internal and regional influences on policy diffusion. Recent work builds on these frameworks has continued to analyze new features that impact policy diffusion, including policy entrepreneurs, actions of the national government, amendments to existing policies, the role of political institutions and policy success, national culture, and path dependence [10, 29].

Though policy diffusion patterns have been studied in many different areas and contexts, most of these studies focus on examining components of a single policy, while few looks into multiple policies simultaneously. The relationships between different policies are also overlooked. In this study, we distinguish the adoption of two different digital trade policies: building cybersecurity capability or implementing digital trade restrictions.

2.4 E-government Maturity Research

An increasing number of studies [2, 3, 13, 21, 24, 32] analyzed the e-government maturity model and the factors that influence e-government adoption, including technological, leadership, government, human, social-cultural, national culture, economic development, political, geographical and demographic factors. For example, information quality characteristics and channel characteristics, both mediated and moderated by transparency and trust, impact the citizens' intentions to use e-government services [3]. The public value of e-government on increasing transparency, digital innovation adoption, fostering an open, inclusive, and responsive government, and corruption controlling are widely discussed [32]. E-government maturity was considered an important manifestation of anti-corruption endeavors. The e-government can increase government transparency, enable citizens' participation in public policy adoption, and reduce the costs of transparency efforts, moderated by the national culture and the economic development [24]. However, the e-government's impact on the digital trade policy implementation is unclear, and more in-depth empirical evidence is valuable.

Additionally, increasing digital connectivity is creating cyber-attack vectors for attackers. Cyber incidents targeting governments are making headlines globally, including Bulgaria, India, Singapore, and the United States, to name just a few. It is necessary to understand whether these increasing cyber threats will deter E-government adoption and turn the government to develop more restrictive digital trade policies.

3 Conceptual Model

As shown in Figure 1, in our conceptualization of the national cyber trade behavior model, we distinguish two main behaviors to handle cybersecurity issues within digital trade: building national cybersecurity capability to cope with cyber threats, named *building cybersecurity capability*, and implementing digital trade restrictions to avoid cyber threats through digital trade, named *implementing digital restriction*.

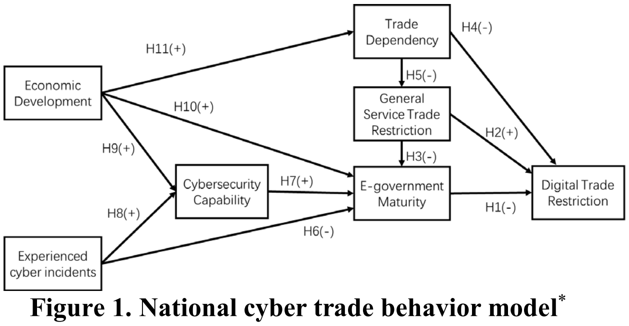

Figure 1. National cyber trade behavior model*

[*] We number the hypotheses from right bottom to left top to make it easier to digest the model.

From a resource-based view, available resources and knowledge about potential threats shape the decision making and the performance of the outcome [24]. Within the digital trade context, the government's digitization knowledge and capability can impact their behaviors in the digital trade policies implementation. More specifically, governments with better digitization capabilities will better understand digital trading, including cyber threats through digital trade. As the digital products and services to promote E-government maturity, including both software and hardware, rely heavily on global supply chains [4]. In contrast, restrictive digital trade policies will limit the capability to access necessary international resources and increase e-government development costs. Nations with higher E-government maturity intend to avoid restrictive digital trade policies. On the other hand, e-government development can increase government transparency and openness [2], driving a more open digital trade system. Therefore, we hypothesize the following:

Hypothesis 1: There is a negative relation between E-government maturity and digital trade restriction.

Path dependency [26] has been widely studied in public policy diffusion studies to explain the impact of institutional history on policy change, as the preceding situations will shape the meaning, purpose, and direction of future actions. In the context of digital trade, though there exist differences between digital trade and traditional trade in services, the way a nation manages the general trade in services can shape the implementation of digital trade policies. Therefore,

Hypothesis 2: There is a positive relation between general service trade restriction and digital trade restriction.

As discussed above, the restrictions on international trade, especially the trade in services, can limit the government's capability to utilize global digital innovations and resources, consequently impacting its e-government development. International trade in services [35] includes business and professional services like computer and related services, communication services like audiovisual services and telecommunications, educational services, health, and social services, all of which are essential components for e-government development. Hence, we hypothesize:

Hypothesis 3: There is a negative relation between the general service trade restriction and E-government maturity.

Many debates exist regarding trade protectionism and liberalism, as protectionism and free trade both have benefits and costs for economic growth [5, 31]. For a nation that highly depends on international trade, building restrictions on trade will reduce its international trade and consequently harm its economic growth, at least in the short term. Hence, restrictive trade policies can be costlier for a nation whose economy is built on international trade. The increased cost of trade restrictions will prevent the adoption of restrictive policies [1]. Therefore:

Hypothesis 4: There is a negative relation between national trade dependence and digital trade restriction.

Hypothesis 5: There is a negative relation between national trade dependence and general service trade restriction.

The perceived threat is a critical component in motivating the coping behaviors that avert potential harm [1]. 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 danger. Recently we have observed increasing cyberattacks targeting government information systems, such as the ransomware attack on the U.S. government in Baltimore City, the Wannacry cyber attack on the U.K.'s National Health Service (NHS). Such attacks may increase concerns about the potential threat and immature E-government, deterring governments from adopting such digital technology. Hence, we hypothesize:

Hypothesis 6: There is a negative relation between experienced cyber incidents and E-government maturity.

The coping capability, defined as the capability to mitigate the perceived threat, is another primary cognitive process used in various security behavior theories like protection motivation theory (PMT) and technology threat avoidance theory (TTAT) [23]. Previous studies demonstrate that the perceived coping abilities, including the response efficacy and self-efficacy, can motivate individuals to take protective actions and reduce the intention to avoid using digital technologies. Hence, if the government can manage potential cyber threats, they will have a positive attitude towards adopting, instead of avoiding, e-government. Thus, we hypothesize the following:

Hypothesis 7: There is a positive relation between national cybersecurity capability and E-government maturity.

Cyber-attacking is considered as a tactical tool within a state's arsenal of power, popular for politicians, policymakers, and defense contractors. States and non-state actors can use cyber-attacking as a foreign policy tool, as a means to "impact, change, or modify diplomatic and military interactions between entities" [19]. However, there is still a lack of empirical evidence to demonstrate that cyber operations can shift the targeted states' foreign policy. The impact of the cyber attacks can be limited [16]. Instead, the targeted governments will improve their cyber capabilities to manage potential further cyber threats. For example, after Russia infiltrated Estonia in 2007, Estonia began to develop its national cyber strategy in 2008. Thus:

Hypothesis 8: There is a positive relation between experienced cyber incidents and national cybersecurity capability.

The economic development has also been viewed as an essential factor for e-government adoption [24]. Countries with greater economic capacity are better poised to accomplish e-government actions and invest in cybersecurity capability building. Thus, we hypothesize the following:

Hypothesis 9: There is a positive relation between economic development level and national cybersecurity capability.

Hypothesis 10: There is a positive relation between economic development level and E-government maturity.

Empirical studies confirm that comparative advantages across countries can partially explain international trade, and economic development will impact a country's comparative advantages in international trade [12]. Therefore, we can expect that a nation with a higher economic development level will have a higher dependency on international trade.

Hypothesis 11: There is a positive relation between economic development level and trade dependency.

4. Data and Research Methodology

4.1 Data

To verify the developed conceptual national cyber trade behavior model, we create a dataset of indicators from different sources.

The general trade restriction on services, and the digital trade restriction, are derived from the OECD trade restrictiveness index database. OECD launched a project in 2014 aimed at providing an objective overview of service trade restrictions. Based on the investigation of more than 16,000 laws and regulations from 22 sectors in 46 countries, the OECD Service Trade Restrictiveness Index database (STRI) offers an unprecedented depth of information, covering nearly 400 different policy measures. The OECD Digital Service Trade Restrictiveness Index (D-STRI) is further developed to capture the impediments that specifically affect digital trade, including the infrastructure and connectivity, electronic transactions, payment systems, intellectual property rights, and other barriers affecting trade in digitally-enabled services such as online advertising, encryption and technology transfers.

The national trade dependency is from the World Bank Trade index. This study uses Trade (% of GDP), the sum of exports and imports of goods and services measured as a share of gross domestic product (GDP), to quantify the importance of international trade for a given nation. The World Bank's PPP GNI per capita, which refers to the gross national income (GNI) converted to international dollars using purchasing power parity rates, has been widely used to evaluate each nation's economic development level. In this study, we use the log values of PPP GNI per capita to represent economic capacity.

E-government maturity captures each nation's maturity of e-government services and digitization capability. Since 2003, the United Nations Department of Economic and Social Affairs has conducted surveys every two years on its member states' e-government development. The e-government development index, EGDI, is considered as the widely adopted indicator for e-government maturity.

We use the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU) for the national cybersecurity capability. The GCI reference assesses cybersecurity commitments across five pillars (legal, technical, organizational, capacity building, and cooperation) based on 25 sub-indicators. An overall GCI score is generated to evaluate each government's cybersecurity capability.

To quantify the cyber threats for each nation, we use events from the Council on Foreign Relations' Cyber Operations Tracker (https://www.cfr.org/interactive/cyber-operations), which lists all publicly known instances of significant and state-sponsored cyberattacks since 2005. This study then calculates the experienced cyber incidents index as the aggregate number of incidents that had occurred for each country up through the specified year.

4.2 Descriptive Statistics

Table 1 reports the descriptive statistics for each variable within our dataset. In this study, we use the 2017 data for analysis. We make this decision because GCI data in 2016 is not available, and trade dependency data for JPN, USA, ISR, and NZL, and GNI data for ISL, LVA, and LTU in 2018 is not available when we conducted this study. The Shapiro-Wilk test shows a significant w-score for all variables expect GCI, which indicates that the datasets we are handling are significant, non-normal. Thus PLS-SEM analysis technology is a suitable method for this study.

Table 1: Summary Statistics

Variable	Obs	Mean	Min	Max	Std. Dev	W-score
Digital Trade Restriction (D_STRI)	46	0.178	0.043	0.488	0.097	**0.874*****
General Service Trade Restriction (STRI)	45$^{\#\#}$	0.262	0.137	0.491	0.080	**0.901****
Trade Dependency (TRD)	46	92.709	24.144	412.869	67.059	**0.760*****
Economic Development (GNI)	46	4.530	3.851	4.883	0.226	**0.935***
E-government Maturity (EGDI)$^{\#}$	46	0.766	0.487	0.910	0.100	**0.942***
Cybersecurity Capability (GCI)	46	0.634	0.336	0.919	0.145	0.966
Experienced Cyber Incidents (CC)	46	10.429	1.000	88.000	14.691	**0.592*****

$^{\#}$: EGDI is available bi-yearly. We use the average between EDGI_2016 and EDGI_2018 to calculate the EGDI_2017.
$^{\#\#}$: The STRI data for ARG is not available to include ARG in this study, resulting in 45 nations in this study. We will use the Pairwise Deletion strategy, which only deletes those cases that exhibit missing values in each pair of variables.
*** p<0.001 ** p<0.01 * p<0.05 ‡ p<0.1

4.3 Research Method

Partial least squares structural equation modeling (PLS-SEM) is considered as a powerful method for path analysis in many disciplines, including strategic management, marketing, accounting, operations management, and human resource management, etc. [11, 27, 28]. Specifically, PLS-SEM is more suitable when the study (1) focuses on understanding the nature of relationships as opposed to the magnitude of those relationships, (2) uses single-item constructs as PLS allows for "unrestricted use of single-item constructs" and (3) involves non-normal data. As we are developing a new national cyber trade behavior model to investigate relationships among digital trading, E-government maturity, and cybersecurity capability, PLS-SEM is the most suitable analysis approach. This study used SmartPLS 3.0 to implement the PLS-SEM method and analyze the dataset.

5. Result

5.1 Assessment of the Structural Model

To evaluate the construct measures' reliability and validity in the developed model, we investigate the composite reliability indicators, including Cronbach's Alpha, rbo_A, and average variance extracted (AVE), which are all 1.000. The Discriminant Validity based on the Fornell-Larcker test shows that the AVE's square root exceeds all correlations between each factor and every other construct. Hence, the developed model contains strong psychometric properties.

To enhance confidence in the PLS-SEM results, we apply bootstrapping to determine the level of significance. We also conduct the Stone-Geisser test using blindfolding to evaluate the developed path model's cross-validated predictive relevance. Finally, we use the PLSpredict procedure to assess the model's out-of-sample predictive power.

Table 2 Structural Model Assessment

Key Variable	R^2 Adjusted $^{\#\#}$	Q^2	PLS		LM	
			RMSE	MAE	RMSE	MAE
Cybersecurity Capability (GCI)	*0.253** (0.103)*	*0.234*	*0.133*	*0.105*	*0.541*	*0.510*
E-government Maturity (EGDI)	0.777*** (0.064)	0.696	0.068	0.051	0.882	0.877
Digital Trade Restriction (D_STRI)	*0.484*** (0.109)*	*0.439*	*0.082*	*0.062*	*1.452*	*1.448*
General Service Trade Restriction (STRI)	0.087 (0.061)	0.110	0.087	0.064	1.070	1.062
Trade Dependency (TRD)	*0.142* (0.074)*	*0.150*	*64.943*	*46.453*	*483.760*	*470.934*

$^{\#\#}$: The standard deviation is reported in parentheses; *** p<0.001 ** p<0.01 * p<0.05

As reported in Table 2, the VIF values are all lower than 3, eliminating collinearity as an issue for this study. The R^2 values for the key variables: cybersecurity capability, E-government maturity, and digital trade restriction are all significant, indicating a sufficient explanatory power of the developed model. The Q^2 values are all larger than zero, indicating good predictive accuracy. Using the 10-fold cross-validation setting in PLSpredict, the results show that comparing with the naïve LM (linear regression model) benchmark, and the RMSE (root mean squared error) and MAE (mean absolute error) in the PLS-SEM analysis are both significantly lower. Therefore, the developed structural model has high predictive power and is satisfactory.

5.2 Hypothesis Assessment

Figure 2 reports the path analysis result. We can see that the developed hypotheses, except the impact of the general restriction on digital restriction (H2), and the impact of cyber threats on governmental digitization (H6), are significantly supported. It is worth noting that the general service trade restriction does have a positive, though not significant, direct impact on the digital trade restriction adoption (H2). The experienced cyber incidents have a positive, though not significant, direct effect on E-government maturity (H6). Hence, the previous cyber incidents do not deter nations from e-government adoption.

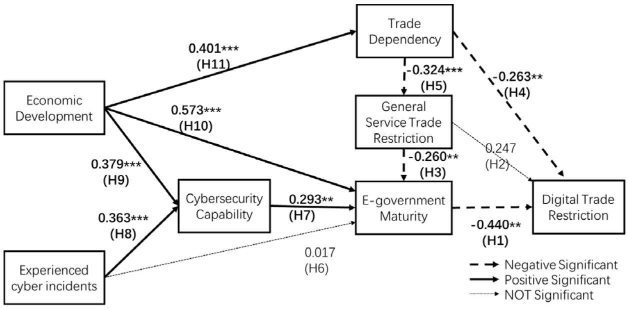

Figure 2. Path Coefficients Result

Table 3 summarizes the direct, indirect, and total effect for the predictors on the key outcome variables: digital trade restriction, E-government maturity, and cybersecurity capability. E-government maturity, trade dependency, economic development, and cybersecurity capability all significantly impact digital trade restriction. Though the direct impact of general service trade restriction on digital trade restriction is not significant, we observe a significant indirect effect, resulting in a significant, overall positive impact. The path dependence effect from general trade in service to digital trade does exist.

The trade dependency, economic development, and cybersecurity capability all have significant positive impacts on E-government maturity. The general service trade restriction has a significant negative effect on E-government maturity, indicating that trade restrictions limit a government's capability to promote its e-government maturity.

The economic capability significantly supports the cybersecurity capability building, and the experienced cyber incidents do push governments to invest in cybersecurity. Interestingly, the cyber incidents themselves do not significantly impact either the e-government maturity or the digital trade restriction.

5.3 Mediation Effect

To evaluate the mediation effect from E-government maturity and cybersecurity capability, we further report the specific indirect effects in Table 4. It shows that the E-government maturity has a significant indirect-only mediation impact on the effect from cybersecurity capability, economic development, and general trade service restriction to digital trade restriction. This confirms the critical role of E-government maturity for the digital trade system.

For effect of experienced cyber incidents on E-government maturity, the cybersecurity capability shows a significant, positive, indirect-only mediation impact. Cyber capability also has a significant, partial mediation effect on the impact of economic development on E-government maturity. This indicates that cybersecurity capability can turn the economic ability and experienced cyber incidents into motivations to promote E-government maturity.

Cybersecurity capability and E-government maturity together show a negative mediation effect for the impact of cyber incidents on digital trade restriction. Hence, rather than deterring a society from digitization, previous cyber incidents can push cybersecurity capability building, increase E-government maturity, and finally motivate less digital trade restrictions.

Table 3 Results of PLS-SEM path analysis

Outcome	Predictor	Direct Effect	Indirect Effect	Total Effect
Digital Trade Restriction (D_STRI)	E-government maturity	**-0.440** (0.147)**		**-0.440** (0.147)**
	Trade Dependency	**-0.263**(0.083)**	**-0.117*(0.054)**	**-0.380***(0.071)**
	Economic Development		**-0.454***(0.110)**	**-0.454***(0.110)**
	Cybersecurity Capability		**-0.129*(0.060)**	**-0.129*(0.060)**
	General Service Trade Restriction	0.247(0.158)	**0.115‡(0.066)**	**0.361**(0.131)**
	Experienced Cyber Incidents		-0.054(0.046)	-0.054(0.046)
E-government Maturity (EGDI)	Trade Dependency		**0.084‡(0.044)**	**0.084‡(0.044)**
	Economic Development	**0.573***(0.101)**	**0.145*(0.057)**	**0.718***(0.063)**
	Cybersecurity Capability	**0.293**(0.093)**		**0.293**(0.093)**
	General Service Trade Restriction	**-0.260*(0.110)**		**-0.260*(0.110)**
	Experienced Cyber Incidents	0.017(0.098)	**0.107**(0.041)**	0.124(0.088)
Cybersecurity Capability (GCI)	Economic Development	**0.379***(0.106)**		**0.379***(0.106)**
	Experienced Cyber Incidents	**0.363***(0.088)**		**0.363***(0.088)**

The standard deviation is reported in parentheses; *** p<0.001 **p<0.01 *p<0.05 ‡p<0.1

Table 4 The Mediation Effect of Cybersecurity Capability and Governmental Digitization

Specific Indirect Effects	Mediation Effect	Point Estimate	Bootstrapping			
			Percentile BC 95% CI		Bca 95% CI	
			Lower	Upper	Lower	Upper
Mediation Effect from E-government maturity						
Cybersecurity Capability -> E-government maturity -> Digital Trade Restriction	Indirect-only	**-0.129*** **(0.060)**	-0.256	-0.040	-0.253	-0.050
Experienced Cyber Incidents -> E-government maturity -> Digital Restriction	NO	-0.008 (0.047)	-0.099	0.046	-0.102	0.047
Economic Development -> E-government maturity -> Digital Trade Restriction	Indirect-only	**-0.252**** **(0.095)**	-0.406	-0.104	-0.407	-0.098
General Restriction -> E-government maturity -> Digital Trade Restriction	Indirect-only	**0.115**‡ **(0.066)**	0.030	0.243	0.029	0.243
Mediation Effect from Cybersecurity Capability						
Experienced Cyber Incidents -> Cybersecurity Capability -> E-government maturity	Indirect-Only	**0.107**** **(0.041)**	0.053	0.189	0.052	0.186
Economic Development -> Cybersecurity Capability -> E-government maturity	Partial	**0.111*** **(0.052)**	0.044	0.210	0.047	0.215
Mediation Effect from Cybersecurity Capability and E-government maturity						
Experienced Cyber Incidents -> Cybersecurity Capability -> E-government maturity -> Digital Trade Restriction	Indirect-Only	**-0.047**‡ **(0.025)**	-0.104	-0.017	-0.101	-0.016
Economic Development -> Cybersecurity Capability -> E-government maturity -> Digital Trade Restriction	Indirect-Only	**-0.049**‡ **(0.029)**	-0.117	-0.015	-0.114	-0.015

The standard deviation is reported in parentheses; *** p<0.001 **p<0.01 *p<0.05 ‡p<0.1

6 Conclusion and Discussion

6.1 Theoretical implications

This study sought to investigate the relationships between cybersecurity commitment and digital trade restrictions. The evidence from 46 countries show that there exists no significant direct impact from cybersecurity capability building to digital trade restriction, but indirect impact mediated by E-government maturity. If the policy for cybersecurity capability building can promote e-government maturity, it can eventually motivate a less restrictive digital trade system. However, the cybersecurity capability building practices that counteract the e-government adoption may result in a more stringent digital trade system. This elaborates on the debates about the impact of cybersecurity on digital trade restriction, satisfying our original objective.

Secondly, our work contextualizes information security behavior theories into the national policy adoption context by considering building cybersecurity capability as taking a protective action, and implementing digital restriction as an avoidance action. This study empirically shows that the perceived cyber threat can motivate the protective action by building cybersecurity capability within the context of digital trade policy. This observation is consistent with many studies on individual and organizational behaviors [1, 23]. However, there is no significant direct relationship between the experienced cyber incidents and the e-government maturity or digital trade restriction. Hence, unlike individual security behavior, the perceived cyber threat will not trigger avoidance behavior for nations. Conversely, mediated by the cybersecurity capability building, cyber incidents can motivate governments to invest in cybersecurity, improve e-government maturity, and eventually foster a more open digital trade system. This study confirms the value of extending the behavioral and organizational studies of cybersecurity to the public policy and highlighting the differences within the national level policies context.

This study's third contribution is to extend the previous research scope for e-government studies [32]. Our study reveals the critical role of e-government maturity for a more secure, open digital trade system. A mature E-government system can encourage less restrictive digital trade policies and mediate the impact from cybersecurity capability building, economic development, and general service trade restrictions to digital trade restrictions. Additionally, a growing body of literature has discussed the driving factors for e-government adoption, including national culture, economic development, political, information quality, trust and transparency, geographical and demographic factors [3]. Beyond these factors, this study further confirms that access to global resources through international trade and the capability to handle cyber threats by cybersecurity capability building can significantly impact the E-government maturity.

6.2 Practical implications

While digital trade is unlocking more global business opportunities, governments' in-flux digital trade policies to manage cyber threats are creating significant political risks for business. Organizations need to understand these policies to align their global digital strategy. This study suggests that a nation with high trade dependency, high cybersecurity commitment, advantaged e-government maturity, and low general trade restrictions would have low digital trade restrictions. More specifically, if the implementation of a cybersecurity capability building policy cannot promote e-government maturity, such a policy may turn out as a digital trade barrier. For example, our data shows that Indonesia has the lowest e-government maturity, low trade dependency, low cybersecurity capability, and a restrictive trade environment. Business leaders should prepare for a restrictive digital trade environment when entering Indonesia's digital market. However, given the significant increase in cybersecurity capability and e-government maturity, we can expect that Indonesia's digital trade environment will become less restrictive, which opens new business opportunities. Hence, the developed framework can serve as a baseline for business leaders to evaluate the consequences of increasing cybersecurity policies and understand the trend of digital trade environments, which can help them effectively design their global digital strategy.

On the other hand, the international community needs to develop a cyber-secure digital trade system that can simultaneously defend against growing cyber threats through digital trade and support the global digital innovations. This study reveals the mediation effect of E-government maturity on the impact from cybersecurity capability building to digital trade restrictions. Hence, when implementing the cybersecurity capability building policy, governments should avoid those practices that can hinder the promotion of E-government maturity. Additionally, the practices from those nations with high cybersecurity capability building, high e-government maturity, and low digital trade restrictions can provide useful insights to develop practical guidance to manage cybersecurity issues within the digital trade system effectively. Hence, given the significant commitment to cybersecurity, the best digital governmental capabilities, and the national strategy to build the global digital supply chain hub, Singapore is best positioned to coordinate the cybersecurity governance framework for the digital trade system.

6.3 Limitations and Future Research

Like all studies, this empirical analysis has its limitations, and some of them open up opportunities for future work. First, only 46 countries from the OECD Digital Service Trade Restrictiveness Index have the required data for this study. However, these 46 countries represent over 80% of international trade in services. Hence, this study's conclusion is representative enough to describe the relationships between cybersecurity commitment, e-government maturity, and digital trade restriction. Additionally, this study employs the PLS-SEM based path analysis method, which can handle small sample sizes.

We acknowledge that the unobserved countries have significantly different economic development levels, e-government maturities, trade dependencies, and cybersecurity commitments. Once their digital trade restriction data is available, further studies to generalize the developed theory will be valuable.

The study does not consider other possible factors, such as political capacity and national culture. Including more diverse interactions could help in investigating the cross-country effects. Future studies should explore additional variables, especially those related to cross-country effects, to construct a more refined picture of national cyber trade behaviors.

In this study, all factors are measured through single items, which could be viewed as a limitation. However, many previous researchers have argued that "the single-item measures can provide an acceptable balance between practical needs and psychometric concerns" [28] and that these single-item measures can be high in validity. PLS-SEM is a suitable method when a study uses single-item constructs, as PLS-SEM allows for the unrestricted use of single-item constructs [11]. However, further studies that include more than one item for each factor are valuable to increase the results' validity.

Given the data availability, this study does not consider the developed theory's evolution. Future research should look into this model's dynamic, such as further analysis when data from subsequent years is released. More empirical studies to reveal trigger factors for such evolution will be precious.

Finally, this study provides the first step towards a governance framework to manage the increasing cybersecurity concerns within the digital trade system. Further studies to identify the norms from practices to guide business leaders and policymakers' decision-making are also critical.

Acknowledgement

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

References

[1] Alec Cram, W., J. D'Arcy, and J.G. Proudfoot, "Seeing the forest and the trees: A meta-analysis of the antecedents

to information security policy compliance", *MIS Quarterly 43*(2), 2019, pp. 525–554.
[2] Bertot, J.C., P.T. Jaeger, and J.M. Grimes, "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies", *Government Information Quarterly 27*(3), 2010, pp. 264–271.
[3] Blohm, I., C. Riedl, J. Füller, and J.M. Leimeister, "Managing Citizens' Uncertainty in E-Government Services: The Mediating and Moderating Roles of Transparency and Trust", *Information Systems Research 27*(1), 2016, pp. 87–111.
[4] Boyson, S., "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems", *Technovation 34*(7), 2014, pp. 342–353.
[5] Costinot, A., "Jobs, Jobs, Jobs: A 'new' perspective", *Journal of the European Economic Association 7*(5), 2009, pp. 1011–1041.
[6] DePietro, R., E. Wiarda, and M. Fleischer, "The context for change: Organization, Technology and Environment", In *The process of technology innovation*. 1990, 151–232.
[7] Ferracane, M., J. Kren, and E. van der Marel, "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?", *SSRN Electronic Journal*, 2019.
[8] Friedman, A.A., "Cybersecurity and Trade: National Policies, Global and Local Consequences", *Brookings Institution Center for Technology Innovation*(September), 2013, pp. 1–18.
[9] Goldfarb, A., and C. Tucker, "Privacy and Innovation", *Innovation Policy and the Economy 1*(12), 2012, pp. 65–90.
[10] Graham, E., C. Shipan, and C. Volden, "The Diffusion of Policy Diffusion Research", *British Journal of Political Science 43*(3), 2013, pp. 673–701.
[11] Hair, J.F., J.J. Risher, M. Sarstedt, and C.M. Ringle, "When to use and how to report the results of PLS-SEM", *European Business Review 31*(1), 2019, pp. 2–24.
[12] Hidalgo, C.A., B. Klinger, A.-L. Barabási, and R. Hausmann, "The Product Space Conditions the Development of Nations", *Science 317*(5837), 2007, pp. 482–487.
[13] Iannacci, F., A.P. Seepma, C. de Blok, and A. Resca, "Reappraising maturity models in e-Government research: The trajectory-turning point theory", *Journal of Strategic Information Systems*, 2019.
[14] Ikenson, D., "Cybersecurity or Protectionism: Defusing the Most Volatile Issue in the U.S.-China Relationship", *Cato Institute*(815), 2017.
[15] Liang, H., Y. Xue, A. Pinsonneault, and Y. "Andy" Wu, "What Users Do Besides Problem-Focused Coping in the IT Security Context: An Emotion-Focused Coping Perspective", *MIS Ouarterly 43*(X), 2019, pp. 1–22.
[16] Lindsay, J.R., "Stuxnet and the Limits of Cyber Warfare", *Security Studies 22*(3), 2013, pp. 365–404.
[17] Lucas, H.C., R. Agarwal, E.K. Clemons, O. a El Sawy, and B. Weber, "Impactful Research on Transformational Information Technology : an Opportunity", *MIS Quarterly 37*(2), 2013, pp. 371–382.
[18] Madnick, S., S. Johnson, and K. Huang, "What Countries and Companies Can Do When Trade and Cybersecurity Overlap", *Harvard Business Review January*, 2019, pp. 1–6.
[19] Maness, R.C., and B. Valeriano, "The Impact of Cyber Conflict on International Interactions", *Armed Forces and Society 42*(2), 2016, pp. 301–323.
[20] van der Marel, E., M. Bauer, H. Lee-Makiyama, and B. Verschelde, "A methodology to estimate the costs of data regulations", *International Economics 146*, 2016, pp. 12–39.
[21] Meijer, A., "E-governance innovation: Barriers and strategies.", *Government Information Quarterly 32*(2), 2015, pp. 198–206.
[22] Meltzer, J.P., "Governing Digital Trade", *World Trade Review 18*(S1), 2019, pp. S23–S48.
[23] Moody, G.D., M. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance", *MIS Quarterly: Management Information Systems 42*(1), 2018, pp. 285–311.
[24] Nam, T., "Examining the anti-corruption effect of e-government and the moderating effect of national culture: A cross-country study", *Government Information Quarterly 35*(2), 2018, pp. 273–282.
[25] OECD-IMF, *Towards a Handbook on Measuring Digital Trade*, 2018.
[26] Pierson, P., "Increasing Returns, Path Dependence, and the Study of Politics", *American Political Science Review 94*(2), 2000, pp. 251–267.
[27] Ringle, C.M., M. Sarstedt, and D.W. Straub, "A Critical Look at the Use of PLS-SEM in MIS Quarterly", *MIS Quarterly 36*(1), 2012, pp. 19.
[28] Sarker, S., M. Ahuja, and S. Sarker, "Work–Life Conflict of Globally Distributed Software Development Personnel: An Empirical Investigation Using Border Theory", *Information Systems Research 29*(2), 2018, pp. 103–126.
[29] Shipan, C.R., "The Mechanisms of Policy Diffusion", *American Journal of Political Science 52*(4), 2018, pp. 840–857.
[30] Shipan, C.R., and C. Volden, "Policy diffusion: Seven lessons for scholars and practitioners", *Public Administration Review 72*(6), 2012, pp. 788–796.
[31] Thompson, W.R., and R. Reuveny, "Tariffs and trade fluctuations: Does protectionism matter as much as we think?", *International Organization 52*(2), 1998, pp. 421–440.
[32] Twizeyimana, J.D., and A. Andersson, "The public value of E-Government – A literature review", *Government Information Quarterly 36*(2), 2019, pp. 167–178.
[33] W.Welch, E., M. K.Feeney, and C.H. Park, "Determinants of data sharing in U.S. city governments.", *Government Information Quarterly 33*(3), 2016, pp. 393–403.
[34] Whitman, M.E., "Security Policy: From Design to Maintenance", *Advances in Management Information Systems 11*, 2008, pp. 123–151.
[35] WTO, *Trade in services：The most dynamic segment of international trade*, 2015.
[36] WTO, "Members debate cyber security and chemicals at technical barriers to trade committee", 2017.
[37] Yoo, C.W., J. Goo, and H.R. Rao, "Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness", *MIS Quarterly 44*(2), 2020, pp. 907–931.