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

Keman Huang, Stuart Madnick

Working Paper CISL# 2020-01

December 2019

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

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

Keman Huang*, Stuart Madnick†

Abstract: Cybersecurity risks are bringing new threats to digital trade, the cross-border transactions enabled by digital technologies. Governments are implementing fragmented, in-flux cybersecurity policies to regulate digital innovations. Organizations need to understand such a trend to align their global digital strategy. The lack of common understandings of cybersecurity within cross-border digital innovations, however, raises an increasing debate about whether and how cybersecurity capability building policies can impact digital trade restrictions. To answer this question, this study develops a National Cyber Trade Behavior model to examine the relation between national cybersecurity capability and digital trade restrictions. Utilizing the PLS-SEM based path analysis, we draw empirical evidences from 46 countries, which represent more than 80% of international trade in services, to verify the developed model. The results reveal that building cybersecurity capability can help to create an open digital trade system, not directly but mediated by E-government maturity. Beyond the theoretical contributions for information systems, digital trade, and e-government discipline, this study develops a governance framework for a secure and open digital trade system, and also supports business to effectively evaluate policy risks to align their global strategy with cross-border digital innovations.

Keywords: Cross-border Digital Innovation, Digital Trade Restriction, Cybersecurity Capability Building Policy, E-government Maturity, Global Digital Strategy

Acknowledgements

This research was supported in part by the MIT Internet Research Policy Initiative, which is funded by the Hewlett Foundation and Cybersecurity at MIT Sloan, which is funded by a consortium of organizations. All errors remain the responsibilities of the authors.

* Dr. Keman Huang is a research scientist of the research group Cybersecurity at MIT Sloan (MIT CAMS) at the MIT Sloan School of Management. Address: E94-1567, 245 First St, Cambridge, MA 02142. Email: keman@mit.edu.

† Prof. Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies at the MIT Sloan School of Management, Professor of engineering systems in the MIT School of Engineering, and founding director of cybersecurity at MIT Sloan (CAMS): The Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. Address: E62-422, 100 Main St, Cambridge, MA 02142. Email: smadnick@mit.edu

1 Introduction

Digitization, the transformation precipitated by a transformational information technology [1], is penetrating every aspect of contemporary society, including how trade happens and what is being traded. Over these years, digital trade, the cross-border transactions enabled by digital innovations such as e-commerce [2], continues to increase in importance: the McKinsey 2016 Digital Globalization shows that approximately 12% of cross-border trades are enabled by e-commerce while digital trade accounts for 50% of the world's traded services Report [3]. While digital trade is unlocking more business opportunities, weak cybersecurity that can occur in digital technology is becoming a growing threat. It was reported that cyber attacks through supply chain increased significantly and it is necessary to reduce cybersecurity risk by securing the global supply chain [4]. Safeguarding the digital assets when adopting digital innovations has become a strategic priority and common interest for many organizations [5,6]. As digital trade sits at the intersection of digitization and trade, it is affected by the increasingly policies implemented by governments to manage cybersecurity concerns from digital innovations. Organizations need to understand the trend of these in-flux digital trade policies to align their global digital strategy. However, given the lack of common understanding of cybersecurity [7], we can observe two different types of national policy implications which can impact the cross-border digitization:

- *Implementing Digital Trade Restriction*. Some governments seek to implement policies to restrict digital innovation to maintain political stabilities, trust, personal and national cybersecurity, or enforce the cyber-sovereignty [7,8]. For instance, the United States Trade Representative (USTR) identified digital restrictions such as data flow restrictions, localization requirement and customized national standards etc. in many of its trade partners, including Indonesia, Russia, China, the EU and Turkey [9]. Furthermore, 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 [10].

• *Building Cybersecurity Capability*. Many nations are implementing "*cybercrime legislation, national cybersecurity strategies (NCS), computer emergency response teams (CERTs), awareness and capacity to spread out the strategies, and capabilities and programmes in the field of cybersecurity*", to ensure cyberspace resilience and mitigate potential cyber threats. For example, as one of first countries to create a cybersecurity strategy in 2008, Estonia has invested significantly in cybersecurity. The Estonian Information Security Association (EISA) was further founded in 2018 to coordinate cybersecurity commitments, including supporting the EU contractual Public Private Partnership model on cybersecurity [11].

Though these two national policy implementations are not exclusive, some argue that the policy implications for cybersecurity capability building will negatively impact trade in information technology products because they discriminate against foreign companies and may lead to unnecessary disclosure of commercially confidential and technical data. On the other hand, others claim that cybersecurity rules are needed to address national security issues, ensure consumer privacy and create a more secure digital society [12]. Some studies even claimed that the digital trade restrictions are implemented in the name of protecting critical infrastructure and national security from cyber threat, but actually have less to do with cybersecurity [13]. These inconsistent conclusions are due to the lack of understandings on connections between cybersecurity and digital trade, which is creating significant uncertainty for cross-border digital innovation. Hence, this study aims to shed lights on such debate by asking the following question: *whether and how does the national cybersecurity capability building impact the implementation of the digital trade restrictions*?

More specifically, by contextualizing the studies on individual/organizational security behaviors [14] to the digital trade system, we consider "*building cybersecurity capability*" as a national behavior to increase endogenous capability to mitigate cyber threats and "*implementing digital trade restrictions*" as a national behavior to control and avoid cyber risk through cross-border digitization. Hence the national cybersecurity capability building to enhance the capability to handle cyber threats can be expected to encourage more open digital trade policies. Furthermore, the policy diffusion theory [15] suggests that the path dependency, internal actor and external actor can impact the public

policy adoption and diffusion, which is expected to be applicable to digital trade system. As e-government strategy can increase transparency, public access to information and digital innovation adoption [16–18], it can increase the governmental knowledge about digitization, which in turn impacts the implementation of digital trade policies. Based on these propositions from information systems, public policy, digital trade and 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. Using empirical evidences from 46 countries, including OECD and other major economic countries which represent more than 80% of international trade in services, the results based on the Partial Least Squares Structural Equation Modeling (PLS-SEM) reveal a significant negative impact from national cybersecurity capability to the digital trade restrictions. However, this impact is actually indirect and mediated by E-government maturity. Also, rather than scaring governments away from digitization, cyber incident actually motivates governments to increase cybersecurity commitment, consequently promoting e-government maturity and reducing digital restrictions.

This developed holistic model -- *National Cyber Trade Behavior Model*, and empirical evidences together provide an answer to the on-going debates about whether cybersecurity capability building will result into a more restrictive digital trade system. Instead of direct connection, the impact from cybersecurity capability building to digital trade restrictions is mediated by the e-government maturity. In another word, the cybersecurity capability building efforts which can improve the e-government maturity, can eventually reduce the digital trade restrictions. Otherwise, it may turn out as digital trade restrictions. Furthermore, instead of deterring the adoption of digitization, within the digital trade system, cyber threat actually motivates a society to invest in cybersecurity, improve governmental digitization, and may foster a more open digital trade system.

These findings provide a governance framework for the international efforts to promote a more open and secure digital trade system. The empirical evidences confirm the mediation effect of e-government maturity so that cybersecurity capability practices from those nations with high e-government maturity can be more practical to effectively mitigate cybersecurity threats from digital trade. Hence the international community should learn from those practices and continually promote national commitment to

cybersecurity capability building and e-government maturity.

On the other hand, recently there are no global rules for managing digital trade, let alone rules to address challenges to cybersecurity issues from digital innovations within digital trade. The in-flux cybersecurity and digital trade policies require organizations to understand the trends and properly align their global digital strategy to identify opportunities and avoid costly surprises. The developed model suggests that a nation with high trade dependency, high e-government maturity and high cybersecurity capability building will have low digital trade restriction. In another word, if the cybersecurity capability building policy implementation can promote the e-government maturity, it has a high potential to eventually reduce the digital trade restrictions and support the cross-border digital innovation. This provides a tool to support the international business, especially the multi-national enterprises, to evaluate the potential policy risk and provide a base line for their global digital strategy design.

The remainder of this paper is organized as follows. We will discuss previous studies focusing on individual/organizational security behavior studies, the impact of the digital trade restrictions, policy diffusion theories, and e-government studies. Building on the core constructs from these theories, we develop our hypotheses and the nation cyber trade behavior model. Empirical data and the PLS-SEM method are used to validate the created theory. Following a discussion about the theoretical and practical implications, the limitations and future directions, we conclude this paper.

2. Literature Review

2.1 Information Security Behaviors Studies: Protection Action or Avoidance

Many studies on individuals' security behaviors have made great progress in understanding the processes that motivate individuals to take protective actions, seeking help or avoidance against different security threats [19–26]. The major theories [25] applied include the coping theory (CT), the protection motivation theory (PMT), the technology threat avoidance theory (TTAT), the theory of reasoned action (TRA) and self-regulation (TSR), the health belief model (HBM), the theory of planned behavior (TPB), the rational choice theory (RCT) and the control balance theory (CBT). These studies reveal that based on a cognitive reasoning, influencing by affect, control balance, costs/rewards, facilitating conditions, formal/informal punishment, perceived behavioral

control, response efficacy, roles, self-concept, self-control, self-efficacy, severity, shame, social factors, subjective norms, susceptibility and violation motivation, national culture etc., individuals take a problem-focused coping action to protect themselves against cyber threats, or avoid the adoption of related technologies to forbear the threats. The emotions and different emotion-based defense mechanisms regarding cyber threats also play a critical role in shaping individuals' reactions to security threats [22].

At the organizational level, there exists two commonly used frameworks to investigate the adoption behaviors: the technology-organization-environment framework (TOE) [27] and the diffusion of innovation model (DOI) [28]. Building on these two frameworks, organizational factors such as the support of top management and leadership, the available internal resources, the size of the organization; the environmental factors such as the peer pressure, the availability of the external support resources and the national culture; and the technical factors including the relative advantage, perceived complexity, with existing practices and values, accessibility, compatibility and trainability, collectively influence the organizational decision to adopt new technologies [29–31].

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 in the national level, a study revealing the mechanisms of how nations balance between the two cybersecurity behaviors and how they impact each other is needed. Additionally, the findings about the factors that influence behaviors, including the response efficacy, self-efficacy and perceived costs etc. are not always consistent [22,23]. These inconsistent results warrant more empirical studies and testing, especially when we consider security behaviors within a different context: national cybersecurity behaviors for digital trade. Furthermore, many existing studies are focusing on individual's and organization's compliance and noncompliance behavior with information security policy [6,32]. 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, the topic of digital trade policy, innovation and governance is 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 have a negative impact on innovative activities [33]. The discussion within the context of Artificial Intelligence (AI) argues that trade policies related privacy, data localization, privileged access to government data, inconsistent industrial regulations related to standards and source code, can have a negative impact on international trade [34]. A few empirical models are developed to quantify the effect of restrictive policies on innovation and productivity. The calibration techniques [35] and computable general equilibrium Global Trade Analysis Project (GTAP) model [36] are used to estimate the negative economic impact of the EU General Data Protection Regulation (GDPR), concluding a loss of more than 300,000 jobs and 1.3 percent of GDP due to the reduction of trade. The data restrictive policies also tend to reduce the company's productivity across different industry sectors, particularly for those that are more data-intensive [37,38].

These studies mostly focus on the negative impact of data restriction policies [39]. However, digital trade, the digitally-enabled transactions of trade in goods and services, is much broader than just data flow. 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 [8,9]. The implementation process of these digital trade restrictions is also unclear, which makes it difficult for organizations to understand the trend of global digitization environment. It is critical to study the factors that impact the adoption of such digital trade restrictions, which is one goal of this studies.

2.3 Nation/State Policy Adoption and Diffusion Theory

Policy diffusion theories have been developed to understand the process of when and how states or nations adopt new policies and the factors which influence the decision of policy adoption [15]. The Walker-Gray-Berry-and-Berry framework [8,40,41] has served as the cornerstone framework for studies on policy diffusion: Walker conceptualized and tested the policy diffusion in the context of the U.S. states, Gray developed the now-standard S-curve pattern to characterize policy adoption, and 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 [15,17,42–44] has continued to

analyze new features that impact policy diffusion including policy entrepreneurs, actions of the national government, amendments to existing policies, role of political institutions and policy success, national culture and path dependence. The horizontal mechanisms like learning, competition and imitation, and the vertical mechanisms like coercion mechanism, bottom-up and top-down federalism have been examined [45].

Though the patterns of policy diffusion 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 groups of policies related to cross-border digitization: building cybersecurity capability or implementing digital trade restrictions. To the best of our knowledge, no empirical study has been conducted to investigate the relations between the adoption of cybersecurity policies and digital trade restrictions, while they can fundamentally influence each other.

2.4 E-government Maturity Research

An increasing number of studies [16,17,51–54,30,31,44,46–50] 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 [54]. The public value of e-government on increasing transparency, trust in government, digital innovation adoption, fostering an open inclusive and responsive government, and corruptions controlling are widely discussed [18]. E-government strategy was considered as an important manifestation of anti-corruption endeavors, as the e-government can increase government transparency, enable citizens' participations into public policy adoption and reduce the costs of transparency efforts [55], which can be moderated by the national culture and the economic development [16,44]. However, the e-government's impact on the digital trade policy implementation is unclear and more in-depth empirical evidences are needed. Furthermore, the technological perspective is playing a vital role for e-government development as the e-government utilizes information and communication technologies (ICTs) to deliver government information

and services to citizens [56]. The United Nation E-Government Development Index assesses national e-government development by the maturity in telecommunications infrastructure, human capital and online services [57].

However, the increasing digital connectivity are 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 if these increasing cyber threats will deter the adoption of E-government and turn the government to develop more restrictive digital trade policies.

3 Theory Development and Model Conceptualization

In our conceptualization of the national cyber trade behavior model, we distinguish two main national 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 control cyber risk through global digital supply chains, named *implementing digital restriction*. As shown in Figure 1, we develop a conceptual model based on prior studies in information security behavior research, national policy diffusion theory, comparative advantage theory in international trade, and e-government studies to understand the relationships among cybersecurity capability, digital trade restrictions, and E-government maturity.

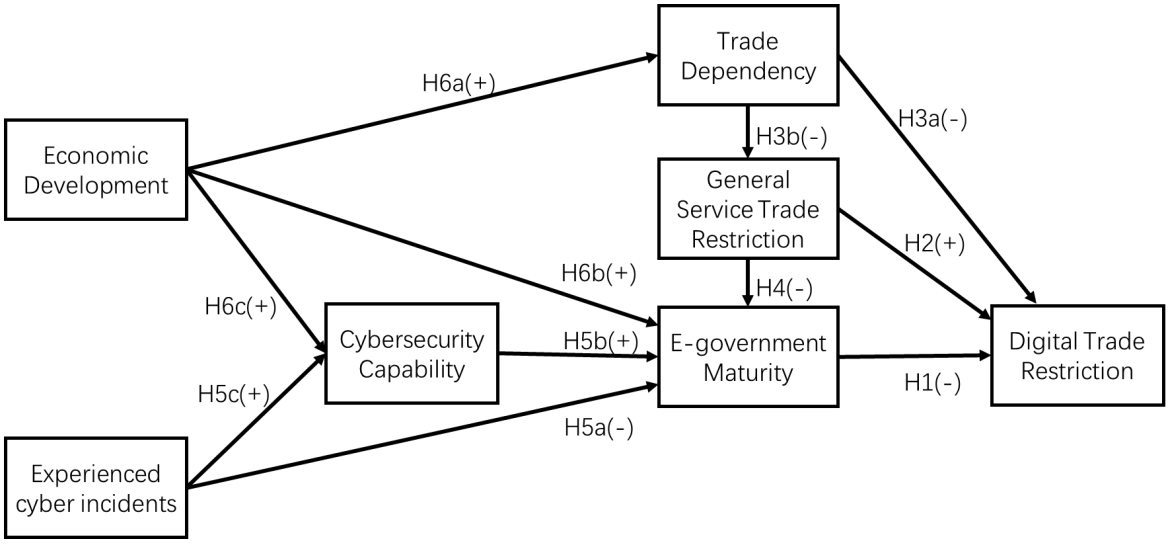

Figure 1: National Cyber Trade Behavior Model

From a resource-based view, available resources and knowledge about potential threats shape the decision making and the performance of the outcome [58–61]. Similarly, within

the context of digital trade, 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 have a better understanding of digital trading, including the potential cyber risks through digital trade. As the digital products and services for E-government strategy, including both software and hardware, rely heavily on global supply chains [62], nations with higher E-government maturity intend to avoid restrictive digital trade policies because such policies will limit their capability to access necessary international resources and increase the cost for e-government development. On the other hand, e-government development can increase government transparency and openness [55], which may also drive a more open digital trade system. Therefore, we hypothesize the following:

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

Path dependency has been widely studied in 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 [17,63,64]. In the context of digital trade, though there exists differences between digital trade and traditional trade in services [8], the way a nation manage 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.

Many debates exist regarding trade protectionism and liberalism, as protectionism and free trade both have benefits and costs for economic growth [65–68]. However, 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 [68]. This means that 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. Therefore:

Hypothesis 3a: There is a negative relation between national trade dependence and digital trade restriction.

Hypothesis 3b: There is a negative relation between national trade dependence and general service trade restriction.

As discussed above, the restrictions on international trade, especially the trade in services, can limit the government's capability to utilize international digital innovations and resources, consequently impacting the nation's e-government development. Actually, international trade in services [69] 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 important components for e-government development. Hence, we hypothesize:

Hypothesis 4: There is a negative relation between the general service trade restriction and the E-government maturity.

The perceived threat is a critical component in motivating the coping behaviors that avert the potential harm [70]. 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 prior victimization experience can lead to an increased concern about threat [23]. Recently we have observed increasing cyber attacks targeting government information systems, such as the ransomware attack on the U.S. government in Baltimore City, the Wannacry cyber attack on the UK's National Health Service (NHS). Such attacks may increase concerns about the potential threat and immature of E-government, and then deter governments from adopting such digital technology. Hence, we hypothesize:

Hypothesis 5a: There is a negative relation between the experienced cyber incidents and the 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) [22,25]. Previous studies demonstrate that the perceived coping abilities, including the response efficacy and the self-efficacy, can motivate individual to take protective actions and reduce the intention to avoid using digital technologies. Hence, if the government has the capability to manage potential cyber threats, they will have a positive attitude towards

the adoption, instead of avoidance, of e-government strategy. Thus, we hypothesize the following:

Hypothesis 5b: 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, policy makers and defense contractors [71]. 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*" [72]. However, there is still a lack of empirical evidences to demonstrate that cyber operations can cause a shift for the targeted states' foreign policy [72] and the impact of the cyber attacks can be limited [73]. Instead, the targeted governments will take actions to improve their cyber capabilities in order to manage potential further cyber threats. For example, after Russia infiltrated Estonia in 2007, Estonia began to develop its national cyber strategy in 2008 [74]. Thus:

Hypothesis 5c: There is a positive relation between the experienced cyber incidents and the national cybersecurity capability.

Empirical studies based on comparative advantage theory confirm that international trade can be partially explained by the differences in comparative advantages across countries. The economic development will impact a country's comparative advantages in international trade [75,76]. Therefore, we can expect that a nation with a higher economic development level will have a higher dependency on international trade.

Hypothesis 6a: There is a positive relation between the economic development level and the trade dependency.

The economic development of a country has also been viewed as an important factor for e-government adoption [16,44]. Countries with greater economic capacity are better poised to accomplish e-government actions, as well as to invest in cybersecurity capability building. Thus, we hypothesize the following:

Hypothesis 6b: There is a positive relation between the economic development level and

the E-government maturity.

Hypothesis 6c: There is a positive relation between the economic development level and the national cybersecurity capability.

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. Table 1 summarizes the measurements and data sources.

Table 1: Measurements and Data Source

Variable	Measurements	Source
Digital Trade Restriction	OECD Digital Service Trade Restriction (**D-STRI**). A higher D-STRI score represents a more restrictive digital trade policy.	OECD
General Service Trade Restriction	OECD Service Trade Restriction (**STRI**). A higher STRI score represents a more restrictive trade policy for services.	OECD
Trade Dependency	The sum of exports and imports of goods and services measured as a share of gross domestic product (**TRD**). A higher value represents a higher dependence on trade.	World Bank
Economic Development	PPP GNI per capita, the gross national income (**GNI**) converted to international dollars using purchasing power parity rates	World Bank
E-government Maturity	UN E-government Development Index (**EGDI**). A higher EDI represents a better digitization level of the government at the given nation.	UN
Cybersecurity Capability	Global Cybersecurity Index (**GCI**). A higher GCI score represents a better cybersecurity capability.	ITU
Experienced Cyber Incidents	The number of publicly known cyber attack incidents targeted at given nations (**CT**).	Council on Foreign Relations

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 [77]. To identify, catalogue and quantify the barriers that affect digital trade, the OECD Digital Service Trade Restrictiveness Index (D-STRI) is further developed to capture the impediments that specifically affect digital trade [78], 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, software, encryption and

technology transfers.

The national trade dependency is sourced from the World Bank Trade index. It compiled four separate databases in World Bank into four indicators: Trade (% of GDP), Exports (% of GDP), Imports (% of GDP), and Net Trade (US Dollars). 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 [44,79]. 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 the e-government development of its Member states [57]. UN experts and volunteer researchers assess e-government maturity across three dimensions: 1) the online service reflecting the scope and quality of online services; 2) the telecommunication connectivity reflecting the development status of the telecommunication infrastructure; and 3) the inherent human capital indicating the aggregate level of education. The e-government development index, EGDI, is considered as the widely adopted indicator for e-government maturity, which will be used in this study.

For the national cybersecurity capability, we use the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU). The International Telecommunication Union, has drafted reports on three versions of the global cybersecurity survey for 2014, 2017, and 2018. These reports were created as part of the ITU's Global Cybersecurity Agenda (GCA), a framework which aims to "*enhance confidence and security in the information society*"[11]. The GCI reference assesses each nation's commitment to cybersecurity across five pillars (legal, technical, organizational, capacity building and cooperation) based on 25 sub-indicators. Using online questionnaires sent to ITU member states and consultations with a group of experts, an overall GCI score is generated to evaluate each nation'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). The tracker lists all publicly known instances of significant and state-sponsored cyber attacks since 2005. The tracker's purpose is to identify incidents where states conduct cyber operations in order to pursuit foreign policy interests. Based on the collected data, the experienced cyber incidents index was calculated as the aggregate number of incidents that had occurred for each country up through the specified year.

4.2 Descriptive Statistics

Table 2 reports the descriptive statistics for each variable within our dataset. In this study, we use the 2017 data for analysis. This decision was made 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. This indicates that the datasets we are handling are significant, non-normal and thus PLS-SEM analysis technology is a suitable method for this study.

Table 2: 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 so that we will not include ARG into this study, resulting into 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

As shown in Table 3, the digital trade restriction level is significantly correlated to the general restriction, trade dependence, economic development, E-government maturity and cybersecurity capability. The mediation variable -- E-government maturity, has significant high correlation with all three independent variables: general service trade restriction, economic development and cybersecurity capability; cybersecurity capability

has significant high correlation with both economic development and cyber threats. These observations enable us to perform further path analysis.

Table 3: Pearlson Correlations

	D_STRI	STRI	TRD	GNI	EGDI	GCI	CC
Digital Restriction (D_STRI)	1.000						
General Service Trade Restriction (STRI)	**0.603*****	1.000					
Trade Dependency (TRD)	**-0.393****	**-0.332***	1.000				
Economic Development (GNI)	**-0.645*****	**-0.496****	**0.401****	1.000			
E-government Maturity (EGDI)	**-0.615*****	**-0.596*****	0.114	**0.820*****	1.000		
Cybersecurity Capability (GCI)	**-0.252**‡	-0.204	-0.130	**0.407****	**0.585*****	1.000	
Experienced Cyber Incidents (CC)	0.020	0.165	**-0.305***	0.085	0.137	**0.470****	1.000

*** p<0.001 ** p<0.01 * p<0.05 ‡ p<0.1

4.3 Research Method

To examine the conceptual model developed above, this study employs the path analysis technique. 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, management information system, operations management, and human resource management [80–82]. 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 a number of single-item constructs as PLS allows for “unrestricted use of single item constructs” and (3) involves non-normal data [80,81,83]. As we are developing a new nation cyber trade behavior model to investigate relationships among digital trading, E-government maturity and cybersecurity capability, PLS-SEM is the most suitable analysis approach. In this study, we used SmartPLS 3.0 to implement the PLS-SEM method and analyze the dataset we created.

5 Result

Consistent with prior studies using PLS-SEM models [83], we analyzed our model in three stages: the first stage focuses on the assessment of the measurement model, the second stage reports the assessment of the developed structural model, and the third stage

evaluates the developed hypothesized relationships.

5.1 Assessment of the Measurement Model

To evaluate the reliability and validity of the construct measures in the model, we consider the following three criteria: First, for each latent variable, we only use one reflective indicator, and all the outer loadings are 1.000. Second, the composite reliability indivators, Cronbach's Alpha, rbo_A and average variance extracted (AVE), are all 1.000. The Discriminant Validity based on the Fornell-Larcker test shows that the square root of its AVE exceeds all correlations between each factor and every other construct. Hence, the developed model contains strong psychometric properties.

5.2 Assessment of the Structural Model

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 cross-validated predictive relevance of the developed path model. Finally, we use the PLSpredict procedure to assess the model's out-of-sample predictive power.

As reported in Table 4, 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 an acceptable explanatory power of the developed model. The Q^2 values are all larger than zero, indicating a good predictive accuracy. Using the 10-fold cross-validation setting in PLSpredict, the results shows that comparing with the naïve LM (linear regression model) benchmark, the RMSE (root mean squared error) and MAE (mean absolute error) in the PLS-SEM analysis are both significantly lower. Though the model fit criteria (SRMR, NFI, d_ULS, d_G and Chi_square) for PLS-SEM are in an early stage and often not useful for PLS-SEM, we report these key criteria in this study. It shows that the SRME (the standardized root mean square residual) is closed to the threshold 0.100 and the NFI (Normed Fit Index) is close to the threshold value 0.90. Considering the fact that these explications are difficult to comprehend for the applied subject, the developed model has a high overall model fit based on these criteria. Therefore, we can conclude that the developed structural model has a high predictive power and is satisfactory.

Table 4 Structural Model Assessment[#]

Key Variable	Outer VIF	R^2 Adjusted##	Q^2	PLS		LM	
				RMSE	MAE	RMSE	MAE
Cybersecurity Capability (GCI)	1	**0.253** (0.103)**	**0.234**	**0.133**	**0.105**	0.541	0.510
E-government Maturity (EGDI)	1	**0.777*** (0.064)**	**0.696**	**0.068**	**0.051**	0.882	0.877
Digital Trade Restriction (D_STRI)	1	**0.484*** (0.109)**	**0.439**	**0.082**	**0.062**	1.452	1.448
General Service Trade Restriction (STRI)	1	0.087 (0.061)	**0.110**	**0.087**	**0.064**	1.070	1.062
Trade Dependency (TRD)	1	**0.142* (0.074)**	**0.150**	**64.943**	**46.453**	483.760	470.934
Model Fit	**SRMR: 0.147 d_ULS: 0.605 d_G: 0.182 Chi-square: 35.827 NFI: 0.784**						

The algorithmic options include: a) the consistent PLS algorithm which connect all LVs for initial calculation is used. The path weighting scheme is applied and pairwise deletion algorithm is used to handle the missing data. b) the consistent PLS bootstrapping with 5000 subsamples, no sign change option, two-tailed test, 0.1 significance level is used. We use both Percentile Bootstrap and Bias-Corrected and Accelerated (BCa) Bootstrap as confidence interval method. c) for the Stone-Geisser test, the omission distance is set as 7. d) for the PLSpredict, we set both No. of Repetitions and Number of Folds as 10.
##: The standard deviation is reported in parentheses; *** p<0.001 ** p<0.01 * p<0.05

5.3 Assessment of the Hypothesized Relationships

Figure 2 reports the path analysis result. We can see that the developed hypotheses, with the exception of the impact of cyber threat on governmental digitization (H5a) and the impact of general restriction on digital restriction (H2), are significantly supported. The experienced cyber incidents actually has a positive, though not significant, direct impact on E-government maturity. This indicates that the previous cyber incidents do not deter nations from e-government adoption. The general service trade restriction does have a positive, though not significant, direct impact on the digital trade restriction adoption.

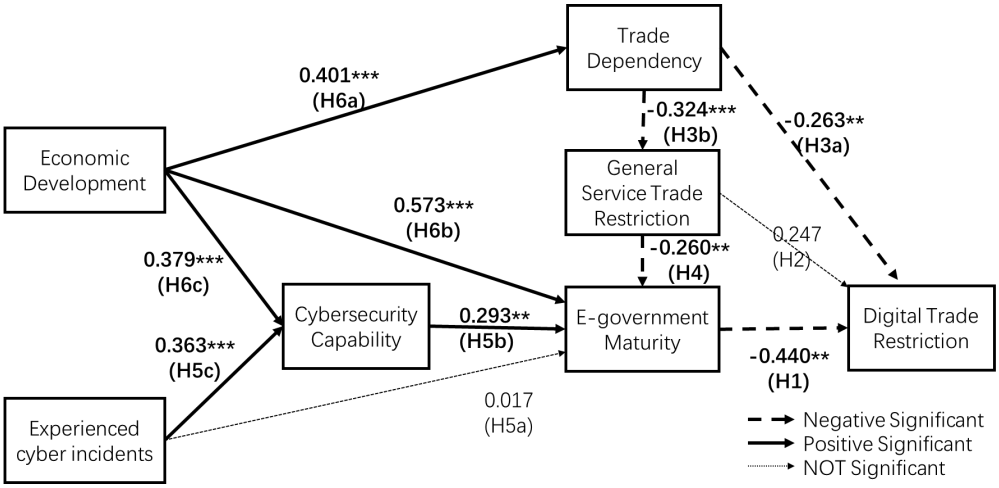

Figure 2: Path Coefficients Result

Table 5 summarizes the direct, indirect and total effect for the predictors on the key outcome variables: digital trade restriction, E-government maturity and cybersecurity capability. The E-government maturity, trade dependency, economic development and cybersecurity capability all have a significant negative impact on digital trade restriction. Though the direct impact of general service trade restriction on digital trade restriction is not significant, we observe a significant indirect impact, resulting into a significant, overall positive effect. This means that there exists a path dependence effect from general trade in service to digital trade. For the e-government maturity, the general service trade restriction has a significant negative impact, indicating that restrictions on service trade indeed limits a government's capability to adopt e-government strategy. The trade dependency, economic development and cybersecurity capability all have significant positive impacts on the governmental digitization procedure. In addition, the economic capability significantly supports the cybersecurity capability building and the experienced cyber incidents does push governments to invest in cybersecurity. Interestingly, the cyber incidents themselves actually do not have a direct significant impact on either the e-government maturity nor the digital trade restriction.

Table 5 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)**
	General Service Trade Restriction	0.247 (0.158)	**0.115‡** **(0.066)**	**0.361**** **(0.131)**
	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)**
	Experienced Cyber Incidents		-0.054 (0.046)	-0.054 (0.046)
E-government Maturity (EGDI)	General Service Trade Restriction	**-0.260*** **(0.110)**		**-0.260*** **(0.110)**
	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)**
	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

To evaluate the mediation effect from E-government maturity and cybersecurity capability, we further report the specific indirect effects in Table 6. 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 strategy for digital trade system. For the effect from experienced cyber incidents to 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 for E-government strategy. This indicates that cybersecurity capability building can turn the economic capability and experienced cyber incidents into motivation of E-government adoption. Considering the impact of cyber incidents on digital trade restriction, the cybersecurity capability and E-government maturity together show a negative mediation effect. This means that 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 6 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	Indirect-Only	**-0.047‡ (0.025)**	-0.104	-0.017	-0.101	-0.016

Restriction						
Economic Development -> Cybersecurity Capability -> E-government maturity -> Digital Trade Restriction	Indirect-Only	**-0.049‡ (0.029)**	-0.117	-0.015	-0.114	-0.015

** p<0.01 * p<0.05 ‡ p<0.1

6 Discussion

6.1 Theoretical implications

This study sought to theoretically develop and empirically test the national cyber trade behavior model to investigate the relationships among cybersecurity commitment and digital trade restrictions. Based on empirical evidences from 46 countries, we confirm that the developed model is satisfactory.

Our first objective was to understand the relation between the cybersecurity capability building and the digital trade restrictions. This study shows that there exists no significant direct, but indirect impact which is mediated by E-government maturity, from cybersecurity capability building to digital trade restriction. In another word, the E-government strategy will affect the impact from cybersecurity capability building to digital trade restrictions. If the policy for cybersecurity capability building can support the e-government strategy, it can eventually motivate a less restrictive digital trade system. However, the cybersecurity capability building practices that counteract the e-government adoption may result into more restrictive digital trade system. This provides elaborates to the debates about the impact of cybersecurity on digital trade restriction, thereby satisfying our original objective.

Secondly, our work contextualizes information security behavior theories into national policy adoption context, focusing on cybersecurity capability building and digital trade restriction implementation. Considering "*building cybersecurity capability*" as taking a protective action and "*digital restriction implementation*" as an avoidance action, this study empirically show that within the context of national cyber trade behavior, the perceived cyber threat can motivate the protective action by building cybersecurity capability, which is consistent with many studies on individual and organizational behavior [22,25]. However, there is no significant, direct relationship between the experienced cyber incidents and the e-government maturity nor the digital trade restriction implementation. This means that unlike individual security behavior [19,20], the perceived cyber threat will not trigger avoidance behavior for nations. Conversely, mediated by the

protective behavior--the coping capability building, cyber incidents actually motivate a society to invest in cybersecurity, improve e-government maturity, and eventually foster a more open digital trade system. This provides empirical evidence to support the argument that cyber-attack itself actually has negative, if not none, impact on raising tensions in digital trade. This is consistent with the cyber restraint theory arguing that cyber operations have limited strategic value as a foreign policy tool, and that cyber incidents will not lead to conflictual foreign policy responses [72,84].

The third contribution from this study is to extend the previous research scope [16,51,55] for e-government studies and reveal the importance role of e-government maturity for a more secure, open digital trade system. E-government strategy can not only encourage less restrictive digital trade policies, but also mediate the impact from cybersecurity capability building, economic development and general service trade restrictions to digital trade restrictions. On the other hand, 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 [30,31,53,54]. Beyond these factors, this study confirms that the access to international resources through international trade and the capability to handle cyber threat by cybersecurity capability building both can significantly impact the E-government maturity.

6.2 Practical implications

This study offers a holistic model to understand digital policies within digital trade context, focusing on the relations between cybersecurity capability policy, e-government maturity and digital trade restrictions. This provides a governance framework to manage the increasing cybersecurity concerns within digital trade systems. Governmental digitization can reverse the potential concerns that cyber threats or cybersecurity regulations may create restrictions for digital trade. To develop practical norms supporting a cyber-secure and open digital innovations, the international community -- including nation states, industry, non-state-entities, and civil society, should allocate resources and efforts to promote the global e-government development. More specifically, the practices from those nations which have high cybersecurity capability building, high e-government maturity and low digital trade restrictions can provide good insights for international

community to develop practical guidance to effectively manage cybersecurity issues within digital trade system. From this perspective, given the significant commitment to cybersecurity, the world's best digital governmental capabilities and the national strategy to build the global digital supply chain hub, Singapore is best positioned to coordinate the development of the cybersecurity governance framework for digital trade system.

Furthermore, this study suggests that a nation with high trade dependency, high cybersecurity commitment, advantage e-government maturity and low general trade restriction would have a low digital trade restriction, resulting in a more friendly environment for cross-border digital innovations. More specifically, if the implementation for a cybersecurity capability building policy cannot support the e-government strategy, or create barriers for e-government adoption, it is possible that such policy will turn out as a digital trade barrier and increase the policy risk for international business. For example, our data shows that Indonesia has the lowest e-government maturity, a low trade dependency, and a low cybersecurity capability. There exists a restrictive digital trade environment within Indonesia. Hence, when implemented the cybersecurity capability building policy, Indonesia needs to pay special attention to avoid introducing more digital trade restrictions. Fortunately, given the significant increase in cybersecurity capability and e-government maturity in 2018, we can expect that the cross-border digital innovation environment within Indonesia can become less restrictive. Therefore, it can be seen that the developed framework provides a baseline for organizations to evaluate the potential consequences from the increasing cybersecurity policies and understand the trend of cross-border digital innovation environments, which can help them to effectively design their global digital strategy.

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. We can believe that the conclusion from this study is representative enough to describe the relationships between cybersecurity commitment, e-government and digital trade restriction. Additionally, this study employs the PLS-SEM based path analysis method, which can handle relatively

small sample sizes. As we focus on the relationships between measured variables instead of latent variables, the rule of thumb (10 observations per indicators) is not applicable. Hence the empirical results in this study can be acceptable.

We acknowledge that in contrast with the 46 nations used in the study, many of other unobserved countries have significantly different economic development levels, e-government maturities, trade dependencies and cybersecurity commitments. Once the digital trade restriction data for these nations is available, further studies to generalize the developed theory will be valuable.

The study does not consider other possible factors such as the political capacity and national culture. Including more diverse interactions could help in investigating the cross-country effects. However, it is difficult to theoretically model these intricate relationships. Rather, this study sheds light on the critical relationships among cybersecurity capability building, e-government maturity and digital trade restriction, developing a theory to understand the impact of cybersecurity within digital trade system. In the future studies, we will 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 researches [82,85–87] have argued that "*the single-item measures can provide an acceptable balance between practical needs and psychometric concerns*" and that these single-item measures can be high in validity. PLS-SEM is the suitable method when the study uses a number of single-item constructs as PLS-SEM allows for the unrestricted use of single item constructs [83].

Finally, given the availability of data, this study does not consider the evolution of the relationships within the developed theory. We believe that future research should look into the dynamic of this model. More empirical studies to reveal trigger factors for such evolution will be very valuable.

7 Conclusion

Many recent studies already confirm that digital trade restrictions can harm economic growth and organizational digital innovations. However, we are observing the dramatic increase of digital trade restrictions due to cybersecurity issues, including privacy, data protection, intellectual property rights, and security, raising concerns of encouraging

digital protectionism. Organizations need to understand the trend of cybersecurity and digital trade policies to align their global digital strategy.

Based on individual/organizational security behavior theories, the path dependency effect from policy diffusion theory, and the value of the e-government strategy, we develop the first national cyber trade behavior model bridging cybersecurity commitment and trade restrictions for digital innovations. Empirical evidences highlight the mediation effect from cybersecurity capability building and e-government strategy on digital trade restrictions. Specially, e-government maturity, which can be impacted by the cybersecurity capability building, plays a critical role in promoting a more secure and open digital trade system. This provides a governance framework to build a more secure and open digital trade system, and support organizations to evaluate policy risk from cybersecurity policy implementations.

Cybersecurity is becoming a critical cornerstone for global digitization. We hope that our unification research can inspire further studies and discussions to better understand the global digitization trend enabled by information technology, so that business leaders and policy makers can manage cybersecurity risks more effectively.

Reference

1. Lucas HC, Agarwal R, Clemons EK *et al.* Impactful Research on Transformational Information Technology : an Opportunity. *MIS Q* 2013;**37**:371–82.

2. World Trade Organization. *World Trade Statistical Review 2019*., 2019.

3. Mckinsey Global Institute. *Digital Globalization: The New Era of Global Flows*., 2016.

4. Relihan T. These Are the Cyberthreats Lurking in Your Supply Chain. *SSRN Electron J* 2019:1–6.

5. Lowry PB, Dinev T, Willison R. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *Eur J Inf Syst* 2017;**26**:546–63.

6. Gwebu KL, Wang J, Hu MY. Information security policy noncompliance: An integrative social influence model. *Inf Syst J* 2019:1–50.

7. Madnick S, Johnson S, Huang K. What Countries and Companies Can Do When Trade and Cybersecurity Overlap. *Harv Bus Rev* 2019;**January**:1–6.

8. Aaronson SA. *What Are We Talking About When We Discuss Digital Protectionism?*, 2018.
9. Fefer RF, Akhtar SI, Morrison WM. Digital Trade and U.S. Trade Policy. *Congr Res Serv Rep* 2017:1–43.
10. US White House. Executive Order on Securing the Information and Communications Technology and Services Supply Chain. 2019.
11. International Telecommunication Union. *Global Cybersecurity Index (GCI) 2018*., 2019.
12. WTO. Members debate cyber security and chemicals at technical barriers to trade committee. 2017.
13. Ikenson D. Cybersecurity or Protectionism: Defusing the Most Volatile Issue in the U.S.-China Relationship. *Cato Inst* 2017.
14. West R, Godinho CA, Bohlen LC *et al.* Development of a formal system for representing behaviour-change theories. *Nat Hum Behav* 2019;**3**:526–36.
15. Graham E, Shipan C, Volden C. The Diffusion of Policy Diffusion Research. *Br J Polit Sci* 2013;**43**:673–701.
16. Nam T. Examining the anti-corruption effect of e-government and the moderating effect of national culture: A cross-country study. *Gov Inf Q* 2018;**35**:273–82.
17. Tang T, Ho ATK. A path-dependence perspective on the adoption of Internet of Things: Evidence from early adopters of smart and connected sensors in the United States. *Gov Inf Q* 2019;**36**:321–32.
18. Twizeyimana JD, Andersson A. The public value of E-Government – A literature review. *Gov Inf Q* 2019;**36**:167–78.
19. Chen Y, Zahedi FM. Individuals' Internet Security Perceptions and Behaviors Polycontextual Contrasts Between the united states and china. *MIS Q* 2016;**40**:205–22.
20. Liang H, Xue Y. Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Q* 2009;**33**:71–90.
21. Venkatesh V, Morris MG., Davis GB. *et al.* User Acceptance of Information Technology: Toward a Unified View. *MIS Q* 2003;**27**:425–78.
22. Liang H, Xue Y, Pinsonneault A *et al.* What Users Do Besides Problem-Focused Coping in the IT Security Context: An Emotion-Focused Coping Perspective. *MIS*

Ouarterly 2019;**43**:1–22.
23. Riek M, Bohme R, Moore T. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Trans Dependable Secur Comput* 2016;**13**:261–73.
24. Warkentin M, Johnston AC, Shropshire J *et al.* Continuance of protective security behavior: A longitudinal study. *Decis Support Syst* 2016;**92**.
25. Moody GD, Siponen M, Pahnila S. Toward a Unified Model of Information Security Policy Compliance. *MIS Q* 2018;**42**:285–311.
26. Cram WA, D'Arcy J, Proudfoot JG. Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Q* 2019;**43**:525–54.
27. DePietro R, Wiarda E, Fleischer M. The context for change: Organization, Technology and Environment. *The Process of Technology Innovation*. 1990, 151–232.
28. Benoit O, Rogers EM. Diffusion of Innovations. *Rev Française Sociol* 2006;**5**:216.
29. W.Welch E, K.Feeney M, Park CH. Determinants of data sharing in U.S. city governments. *Gov Inf Q* 2016;**33**:393–403.
30. Thi LS, Lim HE, Al-Zoubi MI. Estimating influence of toe factors on e-government usage: Evidence of jordanian companies. *Int J Bus Soc* 2014;**15**:413–36.
31. Meijer A. E-governance innovation: Barriers and strategies. *Gov Inf Q* 2015;**32**:198–206.
32. Smith S, Winchester D, Bunker D *et al.* Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Q Manag Inf Syst* 2010;**34**:463–86.
33. Goldfarb A, Tucker C. Privacy and Innovation. *Innov Policy Econ* 2012;**12**:65–90.
34. Agrawal A, Gans J, Goldfarb A. AI and International Trade. *The Economics of Artificial Intelligence*. 2019, 463–92.
35. Christensen L, Colciago A, Etro F *et al.* The Impact of the Data Protection Regulation in the EU. *Intertic Policy Pap* 2013.
36. Bauer M, Erixon F, Krol M *et al. The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data,Moving Commerce*. Belgium, 2013.
37. van der Marel E, Bauer M, Lee-Makiyama H *et al.* A methodology to estimate the costs of data regulations. *Int Econ* 2016;**146**:12–39.
38. Ferracane M, Kren J, Marel E van der. Do Data Policy Restrictions Impact the

Productivity Performance of Firms and Industries? *SSRN Electron J* 2019, DOI: 10.2139/ssrn.3384004.
39. Ferracane M. Restrictions on Cross-Border Data Flows: A Taxonomy. *Ssrn* 2017:1–27.
40. Gray V. Innovation in the States: A Diffusion Study. *Am Polit Sci Rev* 1973;**67**:1174–85.
41. Berry FS, Berry WD. State Lottery Adoptions as Policy Innovations: An Event History Analysis. *Am Polit Sci Rev* 1990;**84**:395–415.
42. Gilardi F. Who learns from what in policy diffusion processes? *Am J Pol Sci* 2010;**54**:650–66.
43. Shipan CR. The Mechanisms of Policy Diffusion. *Source Am J Polit Sci* 2018;**52**:840–57.
44. Zhao F, Shen KN, Collier A. Effects of national culture on e-government diffusion - A global study of 55 countries. *Inf Manag* 2014;**51**:1005–16.
45. Zhang Y, Zhu X. Multiple mechanisms of policy diffusion in China. *Public Manag Rev* 2019;**21**:495–514.
46. Arslan A. Cross-Cultural Analysis of European E-Government Adoption. *World Appl Sci J* 2009;**7**:1–14.
47. Iannacci F, Seepma AP, de Blok C *et al.* Reappraising maturity models in e-Government research: The trajectory-turning point theory. *J Strateg Inf Syst* 2019, DOI: 10.1016/j.jsis.2019.02.001.
48. Estermann B. Development paths towards open government – an empirical analysis among heritage institutions. *Gov Inf Q* 2018;**35**:599–612.
49. Khan A, Krishnan S. Conceptualizing the impact of corruption in national institutions and national stakeholder service systems on e-government maturity. *Int J Inf Manage* 2019;**46**:23–36.
50. Andersen KV, Henriksen HZ. E-government maturity models: Extension of the Layne and Lee model. *Gov Inf Q* 2006;**23**:236–48.
51. Porumbescu GA. Comparing the Effects of E-Government and Social Media Use on Trust in Government. *Public Manag Rev* 2016;**18**:1308–34.
52. Lee J, Layne K. Developing fully functional E-government: A four stage model. *Gov*

Inf Q 2001;**18**:122–36.
53. Omar E.M. K. e-Government readiness: Does national culture matter? *Gov Inf Q* 2011;**28**:388–99.
54. Blohm I, Riedl C, Füller J *et al.* Managing Citizens' Uncertainty in E-Government Services: The Mediating and Moderating Roles of Transparency and Trust. *Inf Syst Res* 2016;**27**:87–111.
55. Bertot JC, Jaeger PT, Grimes JM. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Gov Inf Q* 2010;**27**:264–71.
56. United Nations. *Benchmarking E-Government: A Global Perspective*., 2001.
57. United Nations. *United Nations E-Government Survey 2018: Gearing E-Government to Support Transformation towards Sustainable and Resilient Societies*., 2018.
58. Bandura A. Social cognitive theory in cultural context. *Appl Psychol Int Rev* 2002;**51**:269–90.
59. Armstrong CP, Sambamurthy V. Infrastructures Information Firms : The Influence of Senior Leadership and IT Infrastructures. *Inf Syst Res* 1999;**10**:304–27.
60. Preston DS, Chen D, Leidner DE. Examining the antecedents and consequences of CIO strategic decision-making authority: An empirical study. *Decis Sci* 2008;**39**:605–42.
61. Zafar H, Ko MS, Osei-Bryson KM. The value of the CIO in the top management team on performance in the case of information security breaches. *Inf Syst Front* 2016;**18**:1205–15.
62. Boyson S. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation* 2014;**34**:342–53.
63. Mahoney J. Path dependence in historical sociology. *Theory Soc* 2000;**29**:507–48.
64. Pierson P. Increasing Returns, Path Dependence, and the Study of Politics. *Am Polit Sci Rev* 2000;**94**:251–67.
65. Adele R, Fouda N. Protectionism and Free Trade : A Country's Glory or Doom ? *Int J Trade, Econ Financ* 2012;**3**.
66. Costinot A. Jobs, Jobs, Jobs: A "new" perspective. *J Eur Econ Assoc* 2009;**7**:1011–41.
67. Reuveny R, Thompson WR. Explaining protectionism: 17 perspectives and one

common denominator. *Glob Soc* 2001;**15**:229–49.
68. Thompson WR, Reuveny R. Tariffs and trade fluctuations: Does protectionism matter as much as we think? *Int Organ* 1998;**52**:421–40.
69. WTO. *Trade in Services : The Most Dynamic Segment of International Trade*., 2015.
70. Rippetoe PA, Rogers RW. Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping With a Health Threat. *J Pers Soc Psychol* 1987;**52**:596–604.
71. Cavelty MD. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Wenge A, Mauer V (eds.). London and New York: Routledge Journals, Taylor & Francis Ltd, 2008.
72. Maness RC, Valeriano B. The Impact of Cyber Conflict on International Interactions. *Armed Forces Soc* 2016;**42**:301–23.
73. Lindsay JR. Stuxnet and the Limits of Cyber Warfare. *Secur Stud* 2013;**22**:365–404.
74. Czosseck C, Ottis R, Talihärm A-M. Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *Int J Cyber Warf Terror* 2011;**1**:24–34.
75. Siddiqui K. David Ricardo's Comparative Advantage and Developing Countries: Myth and Reality. *Int Crit Thought* 2018;**8**:426–52.
76. Hidalgo CA, Klinger B, Barabási AL *et al.* The product space conditions the development of nations. Science, 317(5837), 482-487. *Science (80-)* 2007;**317**:482–7.
77. Nordas HK, Rouzet D, Benz S *et al. Services Trade Policies and the Global Economy*., 2017.
78. Ferencz J. *The OECD Digital Services Trade Restrictiveness Index*., 2019.
79. Tang L, Koveos PE. A framework to update Hofstede's cultural value indices: Economic dynamics and institutional stability. *J Int Bus Stud* 2008;**39**:1045–63.
80. Ringle CM, Sarstedt M, Straub DW. A Critical Look at the Use of PLS-SEM in MIS Quarterly. *MIS Q* 2012;**36**:19.
81. Ringle CM, Sarstedt M, Mitchell R *et al.* Partial least squares structural equation modeling in HRM research. *Int J Hum Resour Manag* 2018;**5192**:1–27.
82. Sarker S, Ahuja M, Sarker S. Work–Life Conflict of Globally Distributed Software Development Personnel: An Empirical Investigation Using Border Theory. *Inf Syst Res*

2018;**29**:103–26.
83. Hair JF, Risher JJ, Sarstedt M *et al.* When to use and how to report the results of PLS-SEM. *Eur Bus Rev* 2019;**31**:2–24.
84. Gartzke E. The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth. *Int Secur* 2012;**38**:41–73.
85. Robins RW, Hendin HM, Trzesniewski KH. Measuring global self-esteem: Construct validation of a single-item measure and the Rosenberg Self-Esteem Scale. *Personal Soc Psychol Bull* 2001;**27**:151–61.
86. Burisch M. You don't always get what you pay for: Measuring depression with short and simple versus long and sophisticated scales. *J Res Pers* 1984;**18**:81–98.
87. Postmes T, Haslam SA, Jans L. A single-item measure of social identification: Reliability, validity, and utility. *Br J Soc Psychol* 2013;**52**:597–617.