Determinants of Cyber Readiness

Christos Andreas Makridis[a] and Max Smeets[b*]

*[a] Sloan School of Management, Massachusetts Institute of Technology, Cambridge, United States;[b]Center for International Security and Cooperation, Stanford University, Stanford, United States; *MwSmeets@stanford.edu*

Abstract

Why are some countries better prepared against cyber attacks than others? Whilst previous studies have revealed discrepancies in countries' cyber readiness, there has not been any rigorous analysis which attempts to explain this variation. Based upon a new dataset (Country Capability Dataset), this article therefore seeks to explain why some countries have a higher cyber security readiness compared to others. We develop three theoretical frameworks to explain variation in countries' cyber readiness: i) 'institutional threat', ii) 'institutional returns', and iii) 'institutional capacity'. We find that countries facing a more threatening security environment are more likely to have a high level of cyber readiness. Also, the analysis indicates that countries which are highly dependent on cyberspace are more likely to have a high level of cyber readiness. Yet, surprisingly, we do not find a statistically significant association between our measures of institutional capacity (including real GDP) and cyber readiness. In other words, states which have more resources available to allocate towards developing a reliable and frontier technology infrastructure are not at a systematic advantage in their cyber security investments.

Keywords: cyber security, cyber readiness, information technology, productivity.

JEL: E23, H42, H56

Determinants of Cyber Readiness

I. Introduction

The dramatic increase in cyber-attacks - and awareness of its consequences - has led countries to marshal their resources to strengthen their cyber security capabilities. In numerous countries, the cyber threat has been elevated to national priority.[1] Over the last two decades, national and international security communities have established new policies, partnerships, laws and institutions to effectively prevent and respond to significant cyber incidents. For example, many countries periodically prepare a National Cyber Security Strategy (NCSS)—an outline of a government's plan to enhance the security and resilience of its national critical infrastructure—followed by a significant allocation of resources.[2]

However, differences exist across countries when it comes to their readiness against (potential) cyber-attacks.[3] Whereas some countries, such as the United States, Estonia, and the Netherlands, are viewed as ahead of the curve, other countries are failing to coordinate new initiatives in response to the growing cyber threats. While there is a broad recognition that these discrepancies exist, and there has been some descriptive evidence about these differences, there is not yet any formal evidence that explains why some countries have much more "cyber (security) readiness"

[1] In the United States, President Barack Obama began making cyber security a priority. For example, the US Army established the US Cyber Command in 2010 and the US Department of Defense published a new cyber security strategy in 2011 (updated in 2015). Two years later, in March 2013 US officials stated that the cyber threat has now replaced terrorism as the greatest threat to national security (Boulanin, 2013). For popular press and policy accounts, respectively, see (Dilanian 2013; the Secretary of Defense, 2015)

[2] Many states have also developed offensive cyber attack capabilities (i.e., military cyber warfare organizations), including: Argentina, Brazil, Canada, China, the Democratic People's Republic of Korea, Denmark, Germany, India, Iran, the Republic of Korea, Switzerland and the United States (Lewis and Timlin, 2011).

[3] The variation in policy responses across countries has been discussed by many academics and policy makers. Melissa Hathaway (2013), for example, described the maturity and commitment of 35 countries to protecting their investment in various areas. Hathaway observes great differences between countries as for adopting appropriate legislation, fostering international co-operation and investing opportunities in private-public information sharing exchanges. She has also been the lead investigator of a new project from Potomac Institute for Policy Studies (Hathaway, 2015).

than others.[4] The primary contribution of this paper is to provide empirical evidence behind the factors that explain dispersion in cyber readiness across over 200 countries.

“Cyber readiness” refers to a country’s state of preparedness or ability to act against cyber-attacks. While the concept of “readiness” is often used in relation to military preparation (i.e. combat readiness), referring to the state of the armed forces and their related units to perform during military operations or other activities, we use the term more inclusively to refer to a country's economic and socio-political conditions that might affect its ability to respond to a cyber attack (Betts, 1995).[5] However, “cyber readiness” should not be confused with the concept of “cyber power”, often defined as “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power” (Kuehl, 2009). Whereas cyber readiness emphasizes defense capabilities, cyber power inherently focuses on both defense and offensive capabilities.

Since cyberspace is often said to be a borderless space, one might question whether discussing the level of readiness between different countries is a futile exercise (Betz and Stevens, 2012). What does national defense mean in a borderless context? Yet, cyberspace is a complex, multi-layered phenomenon with both non-physical and physical properties: “both networked infrastructure (computers, routers, hubs, switches, and firewalls) and the information assets (critical data on which an organization depends to carry out its mission)” (Saydjari, 2002;

[4] For several examples of cyber security indices, see RSA (2015), Booz Allen Hamilton and The Economist Intelligence Unit (2011), United Nations Institute for Disarmament Research (2013)

[5] After all, it is widely acknowledged that cyber security is a multifaceted problem requiring range of actions to keep pace with the technology. For example, Alan Marcus, Senior director, head of IT and telecommunication industries for the US’s World Economic Forum, “[c]ybersecurity is an issue that no one organization can resolve by itself.” This point was already acknowledged in Presidential Decision Directive 63 (PDD-63), the first presidential directive released in May 1998 by President Clinton calling for a range of actions intended to improve the nation’s ability to protect “critical infrastructure” from physical and cyber attacks. See: The White House, “Protecting America’s Critical Infrastructures: PDD 63,“ Critical Infrastructure Assurance Office, (May 22, 1998) Quoted in: Hathaway 2013 p. 9.

Libicki, 2009; Ebert and Maurer, 2013). States, therefore, attempt to turn this 'space' in a domain with sovereign control of portions over it (Deibert, 2012).

The results of this paper are both relevant for (academic) research and policy. First, most existing research on cyber capability, though insightful, focuses on particular states as a way to explain capability development, rather than systematically testing propositions across space. The result is that these small N case studies are not always externally valid and do not shed light on broader patterns that can be useful for policymakers. Both the academic (Inkster, 2010; Blank, 2013; Segal, 2014) and think-tank (Tkacik, 2008; Subramanian, 2013; Chang, 2014) cyber literature generally focuses on great powers, - such as the United States, China and Russia - which almost without exception (Burton, 2013; Ebert and Maurer, 2013) do not consider how the conclusions can be generalized to other countries too.

Second, identifying the main drivers behind differences in cyber readiness is a necessary step towards better national and international cyber policies. For example, knowing the factors that contribute to readiness allows us to provide recommendations over the types of investments that might be more effective than others at strengthening cyber capabilities.

One of our main findings is that countries face a more threatening security environment are more likely to have a high level of cyber readiness. Also, we note that countries that are highly dependent on cyberspace are more likely to have a high level of cyber readiness. More specifically, a country's level of ICT exports is one of the most robust and important predictors of cyber readiness.

Yet, surprisingly, we do not find a statistically significant association between our measures of institutional capacity and cyber readiness. In other words, states which have more resources available to allocate towards developing a reliable and frontier technology infrastructure do not seem actually make sufficient use of these assets to invest in cyber readiness. This suggests that economic development might be a necessary but not sufficient condition for realizing improvements in a country's cyber infrastructure.

The structure of the paper is as follows. Section 2 establishes a theoretical framework for thinking about cyber readiness and its theoretical determinants. Section 3 introduces the data and measurement of readiness. Section 4 documents descriptive evidence about the cross-section of cyber readiness and estimates how these different determinants affect country scores. Section 5 concludes.

II. Theoretical Frameworks

Unlike some questions in political science or public policy, there is no carved out space in the academic literature providing tailored-made theoretical explanations on why certain states are in a higher state of readiness compared to others. We therefore draw on various disciplines in proposing three broad sets of factors that might explain variation in cyber readiness: (i) institutional threat environment, (ii) institutional returns, (iii) institutional capacity. We use the term “institutional” to refer to a constellation of allied organizations, rather than a specific entity in government. After all, even in the most centralized governments, the cyber issue is cut up and parcelled out to various organizations.[6] The three factors are not mutually exclusive and all build upon the rational choice literature in which a nation or its representatives perform those actions

[6] See for example Russia’s policy (Russian Federation, 2013)

that have been selected as the value-maximizing means for achieving the actor's objectives (Allison and Zelikow, 1999).[7]

Raymond Cohen (1978, p.93) opens his article stating that "[t]hreat perception is the decisive intervening variable between action and reaction in international crisis." Indeed, history is rife with examples of states establishing defensive measures to cope with an ongoing or looming perceived threat. The Spanish authorities started to build the Valdivian Fort System in 1645 along the Chilean coast after the Dutch expedition to the area two years before.[8] The British authorities constructed the chain of 'Martello Towers' in the early 19th century against a possible French invasion. And, perhaps most famously, the Great Wall of China served as a means to prevent nomads into the Empire (though its effectiveness remains disputed).

Following this line of reasoning, the conventional and cyber threat environment seems to provide an obvious motive for cyber readiness. The notion is that a government is more likely to implement various political, legal and social measures if it believes there is an impending (cyber) threat. The 'cyber threat' is said to have become a truly global concern with both nation state and non-state actors becoming more active and sophisticated in this space. According to a report from risk modeling firm Cyence and Lloyd's of London a major cyber attack could lead to over $53 Trillion in economic losses - a figure on par with some of the most severe natural disasters (Barlyn, 2017). Although no country is said to be immune from cyber attacks, the threat is however not spread equally across the world. Certain countries rely more heavily on cyberspace and suffer from more attacks.

[7] Although from a rational-choice perspective all actors are value-maximizing, it does not mean that actors are expected to respond in the same manner against a security threat. Readiness against a security threat will vary from one country to another and from one historical context to another, depending on differences between actors' i) values and objectives, ii) estimates of consequences of different courses of action, and iii) net valuation of each set of consequences.

[8] The extensive fortification system was constructed to prevent similar intrusions from happening again.

It also indicates that the importance of cyber readiness depends on a country's exposure to sectors or infrastructure that is more vulnerable to cyber attacks—for example, the financial or information technology sector. Countries with greater exposure to these types of sectors will require greater cyber readiness since the downside of being fully exposed is larger.

Finally, as David Baldwin (1997) notes in his classic article, security inherently comes at a cost: it is one of the many important policy objectives competing for scarce resources and subject to the law of diminishing returns.[9] From this perspective, countries that have greater resources at their disposal might have an easier time allocating more towards cyber policies. Also, investments in conventional technologies might spillover into the "cyber sector". For example, blockchain technology is important for not only fending off cyber attacks, but also promoting a brand of secure servers and privacy for clients who potentially confide in a company with sensitive information (e.g., health records or credit card numbers).

Overall, this leads us to develop three hypotheses:

H1 (Institutional Threat Environment)*: Countries which are positioned in a more threatening security environment are more likely to have a high level of cyber readiness.*

H2 (Institutional Returns): *Countries that are highly dependent on cyberspace are more likely to have a high level of cyber readiness.*

H3 (Institutional Capacity): *Countries with greater economic productivity and resources are more likely to have a high level of cyber readiness.*

[9] Ibid

Research Design

III.I Data and Measurement

A new dataset was built, the Country Cyber Capability (CCC) data set, that aggregates earlier datasets and operationalizes additional variables on countries' cyber readiness and a wide range of country economic and institutional characteristics.[10]

Our main dependent variable is Cyber Security Readiness. Our primary data comes from a cyber security ranking - the Global Cybersecurity Index (GCI) - implemented by the International Telecommunication Union (ITU) associated with the United Nations (UN). The ITU is a public-private partnership consisting of 193 member states and regulator bodies, 750 sector members (companies, business associations, and NGOs), and academic partners. The first iteration of GCI was in 2014, a second took place in 2017. As shown in table 1, both the GCI 2014 and 2017 are based on five pillars: legal measures, technical measures, organizational measures, capacity building and cooperation.

Table 1: Main Pillars and issue areas GCI

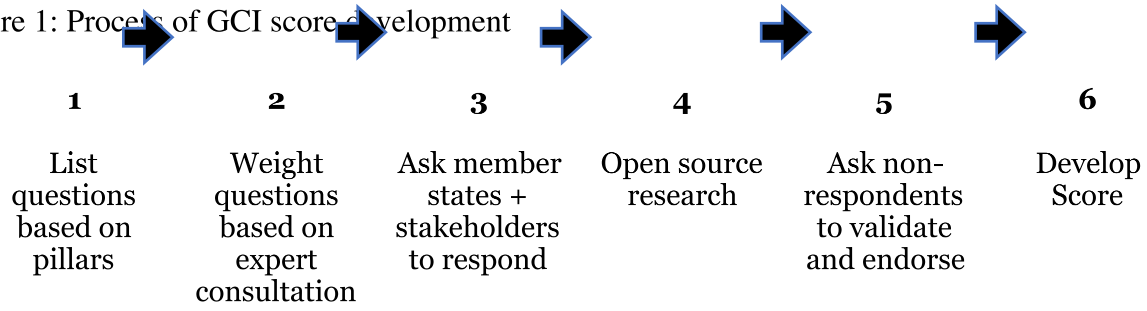
Legal	**Organizational**	**Technical**	**Capacity Building**	**Cooperation**
• Cybercrime Law	• Strategy	• National CIRT	• Standardization Bodies	• Billateral
• Cyber Regulation	• Responsible Agency	• Government CIRT	• Cybersecurity good practices	• Multilateral
• Cyber Training	• Cybersecurity Metrics	• Sectoral CIRT	• R&D Programmes	• International
		• Standards for Organizations	• Public Awareness campaigns	• Public-Private
		• Standards for Professionals	• Professional trainings	• Interagency
		• COP	• Education Programmes	

[10] This is the first study to make use of the dataset. It currently includes 120+ variables on cyber capacity.

Legal	Organizational	Technical	Capacity Building	Cooperation
			• Incentive Mechanism • Home-grown Industry	

The GCI is primarily based on survey data send out to member states and relevant stakeholders. The process in which the score are developed each country can be found in Figure 2. During the second iteration there was a broader involvement of other (industry) stakeholders and also more secondary data was used to construct the scores.

Figure 1: Process of GCI score development


1
List questions based on pillars
2
Weight questions based on expert consultation
3
Ask member states + stakeholders to respond
4
Open source research
5
Ask non-respondents to validate and endorse
6
Develop Score

Source: ITU (2018)

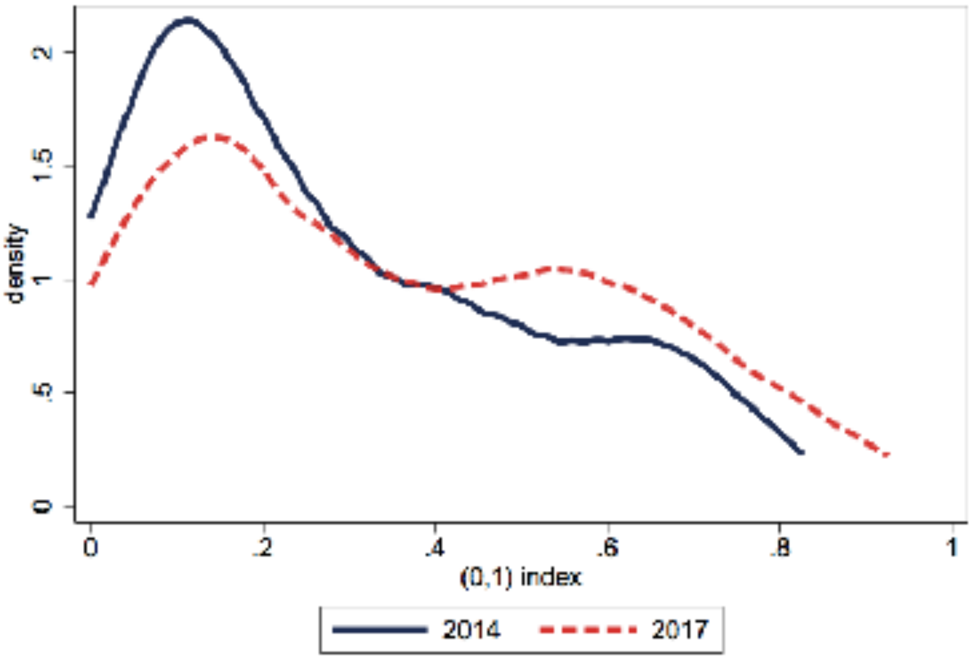
The index has several advantages over others that have been introduced in recent years.[11] First, most studies attempt to gather quantitative evidence to measure a country's 'cyber power' instead of 'cyber-attack readiness'. Second, the developed index of UN ITU recognizes that cyber security is a multi-dimensional concept cutting across many industries and organizations - hence, using five categories. Third, unlike other similar indices, its data collection is extensive as it has a cyber-country profile of almost all countries.[12]

[11] For an overview of other indices see: Index of Cybersecurity indices 2017, ITU

[12] The cyber readiness index developed by Melissa Hathaway, for example, only examines thirty-five countries that have embraced ICT and the Internet. Hathaway, "Cyber Readiness Index 1.0."

Figure 1 provides a glimpse of the variation at our disposal by plotting the distribution of cyber security readiness scores in 2014 and 2017 across countries. We have slightly more countries in 2014 (219) than in 2017 (195). The mean of the readiness score has improved—growing from 0.28 to 0.36, a change of 28%, suggesting that countries might be taking increasing cyber vulnerabilities more seriously. We also observe a slight increase in the standard deviation of scores from 0.23 to 0.25, suggesting that some countries have improved much more than others.

Figure 2: Distribution of Cyber Readiness in 2014 and 2017



mean and s.d. in 2014 (2017) = 0.28 and 0.23 (0.36 and 0.25)

Sources: United Nations International Telecommunication Union (ITU), 2014 and 2017. The figure shows significant dispersion in cyber readiness scores across space, as well as a reasonable amount of within-country variation in these scores within the span of three years.

Examining the data in closer detail indicates that some countries have indeed become considerably better than others over the course of the three years. For example, the United States' score grew from 0.824 to 0.919 (a growth of 11.5%), whereas Germany's score only grew from

0.679 to 0.706 (a growth of 3.9%). The fact that there is such large dispersion in these measures points towards considerable differences in the capabilities of some countries to deal with cyber attacks in comparison to others. These differences beg the obvious question: what are the determinants of readiness across countries?

Our first set of independent variables of interest is *Institutional Threat Environment*. To measure the difference in threat environment between different countries, two indicators are incorporated in the analysis.

First, we measure general country threats using the Composite Index of National Capability (CINC). The index from Singer, Bremer, and Stuckey (1972) aggregates six individually measured components of national material capabilities into a single value per country and year, reflecting an unweighted average of a country's capabilities in each of the areas. The score ranges from zero to unity and reflects a country's capacity along demographic, economic, and military lines, including a country's total population, urban population, iron and steel production, primary energy consumption, military expenditure, and military personnel. While the data has been updated only to 2012, we match the series with our cyber security data by assigning the CINC value from 2012 to 2017. Although there is a mismatch in years, the 2012 value is a sufficiently good proxy for the level that the country would theoretically have in 2017.[13] The main limitation of the assumption is that it prevents us from also including 2017 data on readiness since we would not have a comparable measure of national capabilities for 2017.

Second, to measure the difference in level of cyber threat between different countries, three indicators are incorporated in the analysis. First, we have taken malware data from Kaspersky

[13] To gauge the plausibility of our claim, we estimate an AR(1) regression with the CINC index and find an autoregressive coefficient of 0.993 (p-value = 0.00), consistent with our view that national capabilities are very persistent.

Labs, which leverages their global presence to calculate how often their users encounter detection verdicts on their machines from each country. The measure contains attacks by malicious programs, but does include web anti-virus module detections that would cover certain unwanted programs. Second, we have taken a measure of the overall level of malicious activity from Gartner's Malwarebytes. The company uses data on nearly a billion malware detections and incidents to track Ransomware, ad fraud malware, Android malware, botnets, banking Trojans, and adware.

Our second set of independent variables is *Institutional Returns*. We primarily draw on measures of information and communications technology (ICT) service exports as a share of total service exports and the amount of high technology exports. The former primarily includes computer and communications services (telecommunications, postal and courier services) and information services (computer data and news transactions); the latter measures the dollar value of exported products with high research and development (R&D) intensity, such as aerospace, computers, pharmaceuticals, scientific instruments, and electrical machinery, which are classifications created by the OECD. Both of these measures are intended to capture the relative gains that a country has for investing in its cyber infrastructure and preparedness, manifested through greater dependence on technology in a country's economy. One limitation of this measurement strategy is that not all countries have reliable data on these variables. For example, roughly 31% of the sample of countries is missing data on high technology exports. However, since we still cover 145 countries, we still view our dataset as an externally valid sample.

Our third set of independent variables is *Institutional Capacity*. First, we measure a country's logged GDP per capita, which helps capture the aggregate resources a country has at its disposable. Dividing by population helps ensure that we are not simply capturing the fact that one country is larger than another and, therefore, has a larger aggregate GDP when its average citizens are worse off. Second, we measure a country's information technology infrastructure, which we proxy using mobile cell subscriptions and broadband connections. Broadband refers to the number of residents who have access to the public internet at speeds equal or greater than 256 kbit/s, including cable modem, DSL, fiber-to-home/building, and satellite. The rationale underlying this decision is that a country with greater technological know-how will be in a better position to also fend off potential cyber attacks. Third, we measure a country's educational enrollment in primary and secondary schooling, which captures the availability of knowledge workers who are more likely familiar with cyber vulnerabilities. We also validate that countries with greater educational attainment also have greater research and development (R&D) expenditures, consistent with the view that these countries do more R&D.

Note that we consider mobile cell and broadband subscriptions as determinants of institutional capacity rather than returns. While both are proxies for technology adoption, and thus the relative returns a country may face to have a strong cyber defense against incoming attacks, we view both mobile cell subscriptions and broadband are broader indicators of a country's information technology literacy and expansiveness of technology users. The more citizens who are exposed and connected to the internet with basic technological skills, the more able the country might be to train information security workers and/or for the average household to take basic precautions when online.

Our final set of variables are controls that help ensure that our estimates are not confounded by omitted variables that correlate with both cyber readiness and our measures of the institutional threat environment, institutional returns, and institutional capacity. We specifically measure the employment share in the agricultural sector, population growth, and institutional governance scores relating to legal rights and logistical performance.

The strength of legal rights is measured on a 1 to 12 scale, capturing the degree to which collateral and bankruptcy laws protect the rights of borrowers and lenders. One reason these laws are potentially important for cyber readiness is that access to secure credit is essential for not only business investment and expansion, but also a prerequisite to having a robust financial sector. Since the financial sector is often the most exposed to cyber threats, these countries are also tasked with having greater readiness. The data is obtained a through survey to over 9,000 local experts (e.g., lawyers, consultants, accountants) in each country. In addition, the logistics performance index is measured on a 1 to 5 scale, capturing the perceptions of a country's logistics based on the efficiency of customs clearance, quality of trade / transport infrastructure, ease of arranging competitively priced shipments, ability to track and trace consignments, and frequency with which shipments reach the consignee within the scheduled time. One reason logistics is important for cyber readiness is because it provides a glimpse of a country's infrastructure for dealing with uncertainty and, more generally, processing and managing risk. Our index is based on the results from six sub-indices that capture the specific quality of different logistics dimensions. The data is obtained through a survey to private sector establishments with most of the responses coming from small or medium enterprises (roughly 82% of the sample). We work with standardized versions of these two indices (mean zero and standard deviation of one) to ease the interpretation of their regression estimates. Moreover. we use these two indices because they have the best coverage and representative of other indices of institutional governance. Overall, these controls help address the concern that countries with a better labor force and or higher quality institutions will also have better cyber readiness.

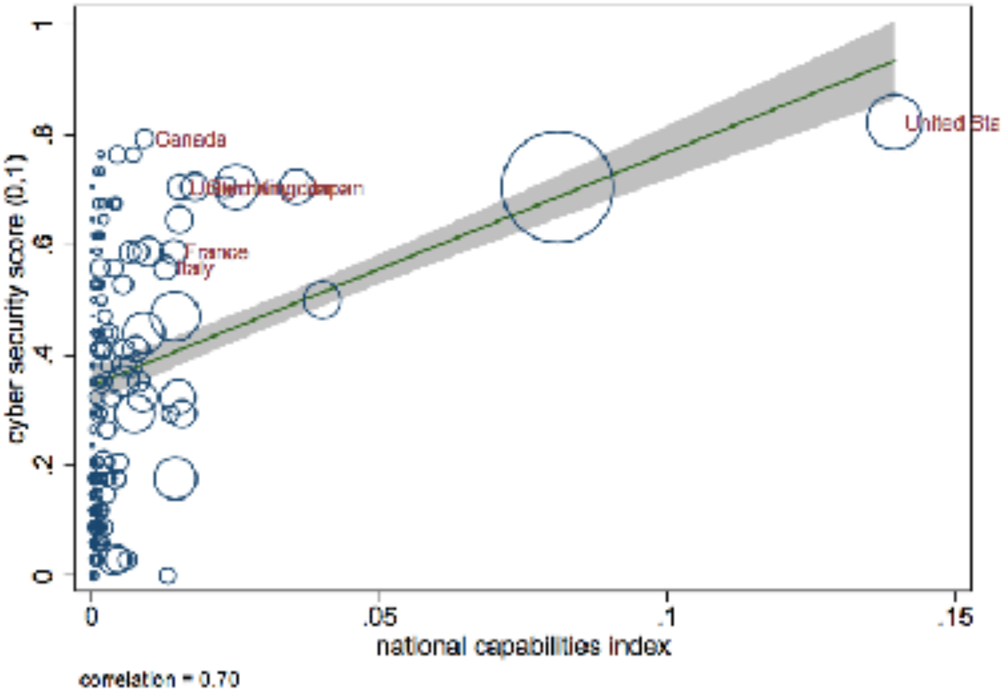
IV. Statistical Evidence

IV.I Descriptive Evidence

Before we present our main multivariate regression results, it is useful to examine the raw data and the correlation between our measure of cyber readiness and its different determinants. As said, we draw on the 2014 cyber readiness index because it is the most comprehensive. All our correlations are weighted by country population, although, as the plots illustrate, these correlations are quite robust to alternative weighting schemes (e.g., unweighted).

We begin with our institutional threat environment measures. Figure {fig:scatter_gci_cinc} plots the composition index of national capabilities (CINC) with the cyber readiness scores. Although there is a strong positive correlation of 0.70, it is interesting that the correlation is driven so heavily by a few countries with high capabilities, namely the United States and India (China ranked with a CINC of 0.21 as an even greater outlier).

Figure 3: Cyber Readiness Scores & Composite National Index of Capabilities

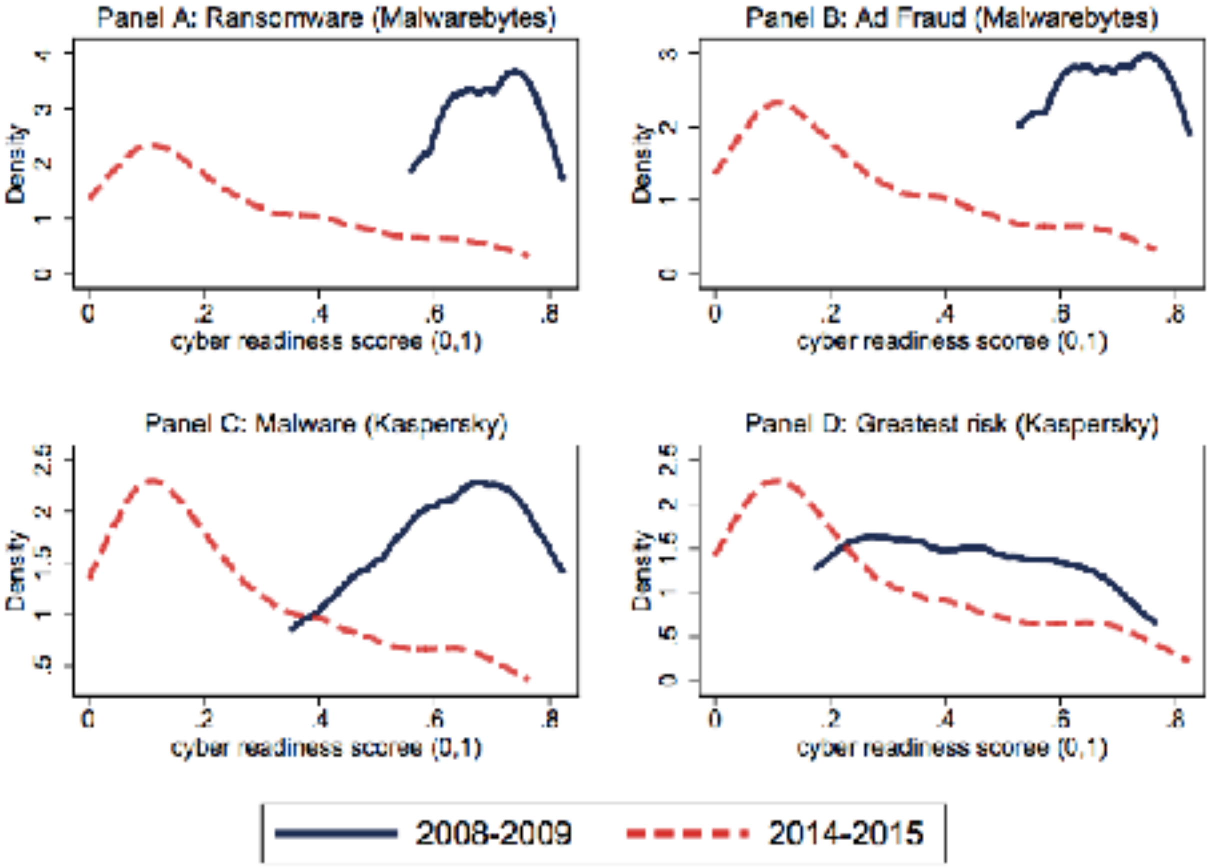


Sources: Correlates of War, United Nations International Telecommunication Union (2014). The figure plots the global cyber- security index (GCI) with the composite index of national capabilities (CINC) from Singer et al. (1972) who measure the aggregate capabilities emerging from economic, demographic, and military features. Observations are weighted by population and an outlier observation with CINC=0.21 is excluded (China). Observations are weighted by population.

While the capabilities index is highly correlated with cyber readiness, we also note that the correlation is driven primarily by population. For example, the correlation between CINC and population is 85%. Moreover, the countries that rank greatest in the capabilities index are China, United States, and India. We, therefore, turn towards a separate measurement strategy of institutional threats (specially, cyber threats) that is less correlated with population. As said, we specifically draw on measures of cyber security threats based on lists from Malwarebytes and Kaspersky classifying the top countries at greatest risk of attack. Since these are binary variables, we plot the distribution of cyber readiness scores for countries that are and are not on the list in Figure 4.

These measures include the top 10 countries for ransomware detections (Malwarebytes), the top 10 countries for ad fraud (Malwarebytes), the top 10 countries where online resources are seeded most with malware (Kaspersky), and the top 20 countries where users face the greatest risk of infection (Kaspersky), which correspond to Panels A, B, C, and D, respectively. Across each measurement approach, we find that countries that are on the list have systematically higher cyber readiness scores. Of course, the positive association between being a greater target and cyber readiness does not imply causality. Indeed, these correlations suffer from a fundamental reverse causality problem: countries with greater cyber readiness scores are also more productive (e.g., higher GDP levels and growth rates), which means they are bigger targets among cyber criminals seeking to commit fraud.

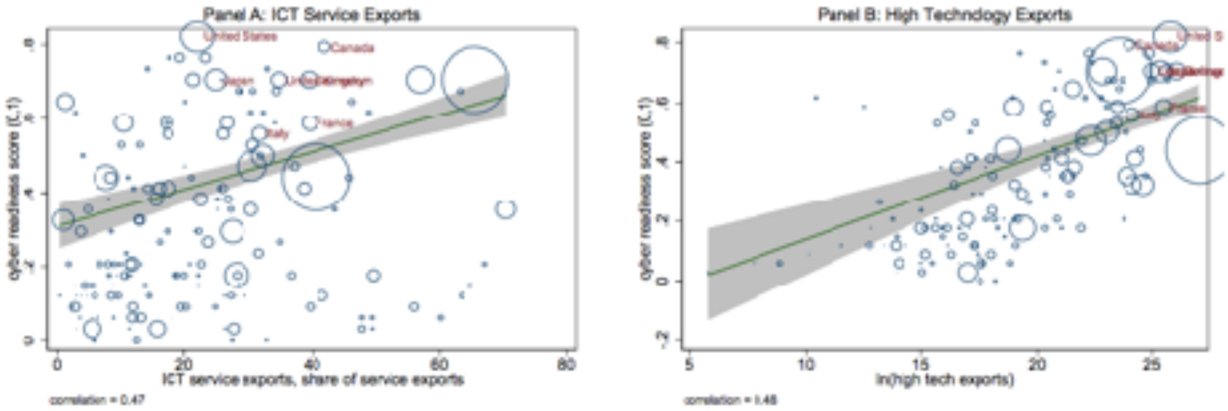
Figure 4: Distribution of Cyber Readiness Scores & Cyber Threat Lists



Sources: United Nations International Telecommunication Union (2014) and Malwarebytes and Kaspersky 2017 annual reports of cyber security. The figure plots the distribution of cyber readiness scores between countries that are versus are not on the lists compiled by Malwarebytes and Kaspersky. Panel A measures the top 10 countries for ransomware detections and Panel B measures the top 10 countries for ad fraud malware both from Malwarebytes. Panel C measures the top 10 countries where online resources are seeded with malware and Panel D measures the top 20 countries where users face the greatest risk of infection. The figure shows that countries with greater cyber threats also have greater readiness scores.

We now turn towards our measures of institutional returns. We find a strong correlation of 0.47 and 0.48 between our measures of ICT service exports and high technology exports with the cyber readiness score, respectively. While there is much greater dispersion and noise in ICT service exports as a share of total service exports, there is still a high correlation. The fact that both series are so correlated with cyber readiness is remarkable in light of the fact that ICT service exports and high technology exports only have a 0.36 correlation, implying that there is a unique and robust relationship between a country's dependence on technology exports and its preparedness against potential cyber attacks. We also tested several other measures, like the ICT goods exports as a share of total exports, but found a weaker relationship in part because most ICT exports are now in the form of services, rather than tangible products.

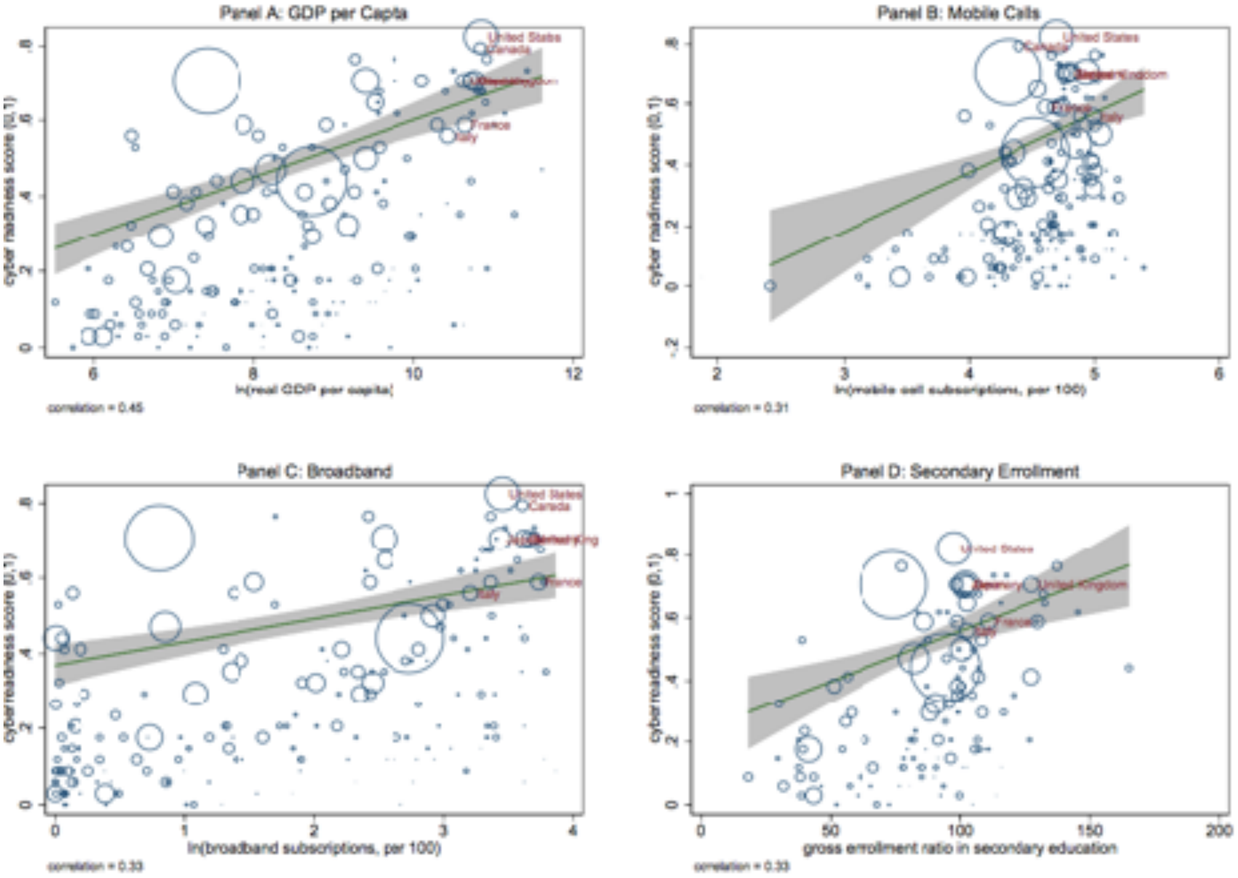
Figure 4: Cyber Readiness Scores & Institutional Returns Characteristics



Sources: United Nations International Telecommunication Union (2014) and World Bank. The figure plots cyber readiness scores against several proxies for institutional returns, including information and communications technology (ICT) service exports as a share of total service exports and logged high technology exports measured in current US dollars. Observations are weighted by population.

We finally turn towards our measures of institutional capacity. We find a positive correlation between cyber readiness and each of these inputs, but the strongest correlation is with real per capita GDP, which has correlation of 0.46. Mobile cell and broadband subscriptions and secondary enrollment all have a correlation of roughly 0.30. In this sense, while we view information technology and education as important determinants of a country's readiness, real GDP per capita captures a wider suite of differences across countries in terms of their productivity and ability to fend off attacks. Not surprisingly, countries with higher GDP per capita also have more cell and broadband subscriptions and educational attainment.

Figure 5: Cyber Readiness Scores & Institutional Capacity Characteristics



Sources: United Nations International Telecommunication Union (2014) and World Bank. The figure plots cyber readiness scores against several proxies for institutional capacity, including real GDP per capita (in constant 2010 US dollars), the logged number of mobile cell subscriptions per 100 people, the logged number of broadband subscriptions per 100 people, and the gross enrollment ratio in secondary education. Observations are weighted by population.

IV.II *Multivariate Regression Analysis*

While our earlier descriptive statistics are useful, they do not have a causal interpretation. For example, countries with stronger legal rights also have higher GDP per capita. Moreover, wealthier countries tend to have more educated workers and these workers might be better suited to reduce vulnerabilities to the country's technology infrastructure. Here, we try to "chip away" at some of these unobserved factors through a series of multivariate regressions:

$$y_{it} = \gamma_{it} + \beta X_{it} + \eta_i + \lambda_t + \epsilon_{it}$$

where y denotes country i's cyber security commitment index from the ITU, TE denotes a vector of “threat environment” characteristics, IR denotes a vector of “institutional return” characteristics, IC denotes a vector of “institutional capacity” characteristics, r denotes a vector of “institutional returns” characteristics, X denotes our control variables, and denote fixed effects on country and year, and denotes the error. We cluster standard errors by country to allow for autocorrelation in the same location over time (Bertrand et al., 2004).

One of the most fundamental concerns associated with estimating Equation 1 is the presence of reverse causality. In particular, increases in cyber readiness might allow countries to better project influence and power internationally, thereby strengthening their position domestically and raising economic activity. While cyber readiness has important consequences for economic development, we are not particularly worried that our estimated coefficients are driven by these types of time-varying shocks because the correlation between GDP growth and the cyber readiness score is zero. In fact, the correlation with ten-year long-differences in GDP growth is only -0.08, suggesting that, if anything, growth in productivity might allow countries to become more prepared for cyber attacks with fewer resources. If that is true, then our estimated coefficients will tend to underestimate the role of our main independent variables of interest, making us overly conservative.

Table 2 documents our results. We begin by sequentially adding in variables—starting with the threat environment, moving to institutional returns, and finishing with institutional capacity. We find a strong positive correlation between both the composite index of national capabilities and indicator for whether the country is in the top 20 at risk of infection and cyber readiness. When we control for both variables, together with our baseline controls, we find that countries ranking in the top 20 have a 0.122 higher readiness index than their counterparts. Moreover, a one unit increase in the CINC is associated with a 1.509 unit increase in readiness. Recognizing that readiness is bounded between zero and one, evaluating CINC at its mean of 0.006 implies that the conditional correlation in column 3 amounts to a 0.009 unit increase in readiness.

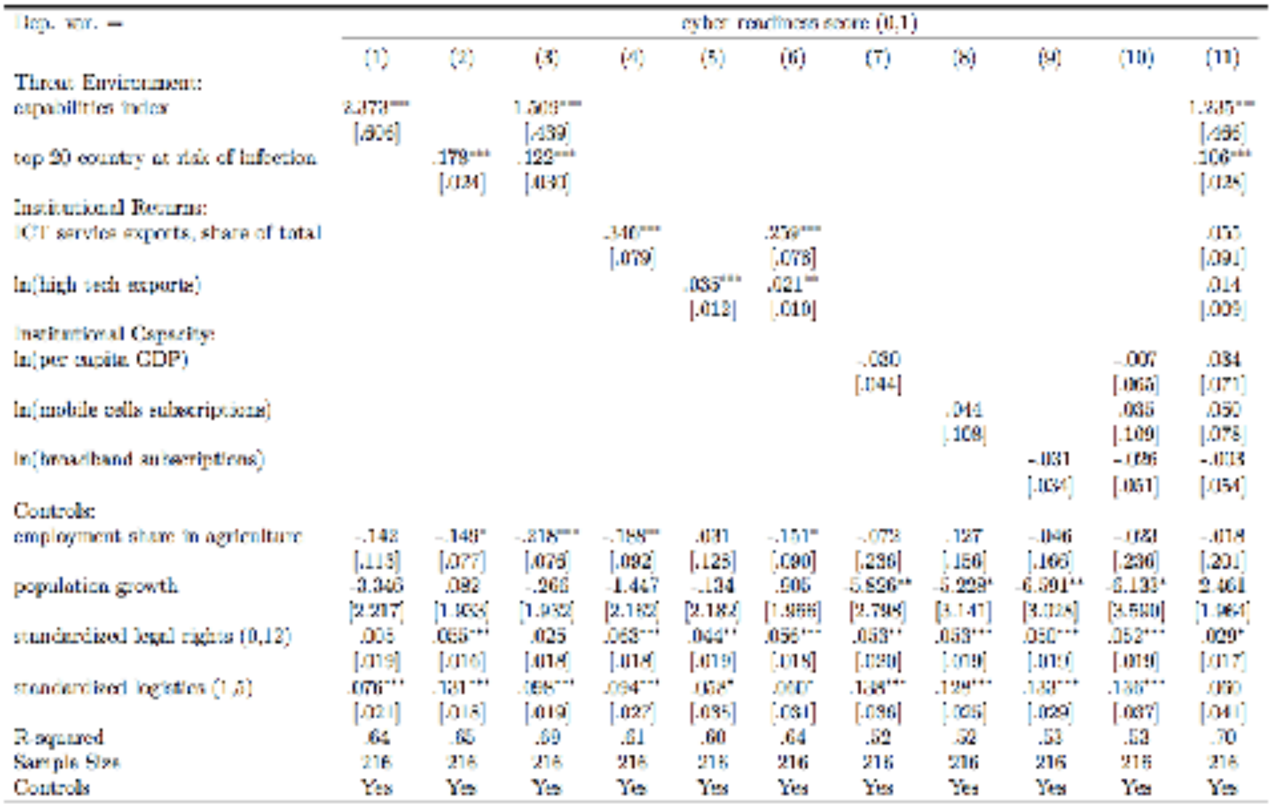
As we emphasized earlier, we do not interpret these as causal effects: increases in threat do not necessarily cause increases in cyber readiness. Rather, the countries that have a higher cyber readiness also face greater threats, which is consistent with a story of reverse causality.

Turning to our measures of institutional returns, we see that both ICT service exports are positively associated with cyber readiness. For example, column 6 shows that a 1 percentage point rise in ICT service exports (as a share of total service exports) is associated with a 0.3 unit increase in the index, which is rather large given the mean is 0.43. Similarly, a 10% rise in high tech exports is associated with a 0.21 unit increase in cyber readiness.

Perhaps surprisingly, however, we do not find a statistically significant association between our measures of institutional capacity and cyber readiness. For example, even real per capita GDP is not statistically associated with increases in readiness—in fact, it is negatively associated with it, if anything. Mobile cell subscriptions have a slight positive association with cyber readiness, whereas broadband subscriptions have a slight negative association. However, we cannot reject the null hypothesis that the two have the same (and potentially null) effect on readiness.

Turning towards our final specification in column 11, which we view as the baseline, we find that the threat indices remain highly statistically and economically associated with cyber readiness. Our measures of institutional returns become statistically and economically insignificant and our estimate of per capita GDP becomes positive, but statistically insignificant. These results are important because they highlight the necessity to control for potentially confounding factors. For example, they suggest that countries thinking of increasing their cyber readiness should not necessarily increase their information technology infrastructure right away—at least viewed in isolation of other policies. Instead, one of the levers countries may have at their disposal might be to simply raise their overall national capabilities and develop strategies for helping domestic users be less susceptible to intrusions from attackers.

Table 2: Baseline Results: Cyber Readiness and Country Characteristics



Dep. var. =	cyber readiness score (0,1)										
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Threat Environment:											
capabilities index	2.473***		1.503***								1.235***
	[.606]		[.439]								[.466]
top 20 country at risk of infection		.179***	.122***								.106***
		[.024]	[.031]								[.028]
Institutional Returns:											
ICT service exports, share of total				.340***		.259***					.055
				[.079]		[.078]					[.091]
ln(high tech exports)					.035***	.021**					.014
					[.012]	[.010]					[.009]
Institutional Capacity:											
ln(per capita GDP)							-.030			-.007	.034
							[.044]			[.065]	[.071]
ln(mobile cells subscriptions)								.044		.035	.050
								[.108]		[.109]	[.075]
ln(broadband subscriptions)									-.031	-.026	-.013
									[.034]	[.051]	[.054]
Controls:											
employment share in agriculture	-.142	-.148*	-.218***	-.188**	.031	-.151*	-.073	.127	-.046	-.021	-.018
	[.113]	[.077]	[.076]	[.092]	[.125]	[.090]	[.236]	[.156]	[.166]	[.236]	[.201]
population growth	-3.346	.092	-.266	-1.447	-.134	.905	-5.826**	-5.229*	-6.591**	-6.133*	2.461
	[2.217]	[1.933]	[1.932]	[2.182]	[2.184]	[1.866]	[2.798]	[3.147]	[3.028]	[3.580]	[1.964]
standardized legal rights (0,12)	.005	.065***	.025	.063***	.044**	.056***	.053**	.053***	.050***	.052***	.029*
	[.019]	[.016]	[.018]	[.018]	[.019]	[.018]	[.020]	[.019]	[.019]	[.019]	[.017]
standardized logistics (1,5)	.076***	.131***	.098***	.094***	.058*	.060*	.138***	.129***	.133***	.136***	.060
	[.021]	[.018]	[.019]	[.027]	[.035]	[.031]	[.036]	[.025]	[.029]	[.037]	[.041]
R-squared	.64	.65	.69	.61	.60	.64	.52	.52	.53	.53	.70
Sample Size	216	216	216	216	216	216	216	216	216	216	216
Controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Sources: World Bank and International Telecommunication Union, 2014. The table reports the coefficients associated with the ITU cyber readiness score (zero to one index) on measures of the threat environment, institutional returns, and institutional capacity, together with other country controls. Threat environment is measured using the composite index of national capabilities (CINC) from Singer et al. (1972) and the top 20 countries at risk of infection as defined by kaspersky. Institutional returns are measured using the ICT services exports (as a share of total service exports) and high tech exports. Institutional capacity is measured using real per capita GDP, mobile cell subscriptions, and broadband interent subscriptions. All regressions include the following controls: the agricultural employment share, population growth, legal rights, and logistics quality. Observations are weighted by country population and standard errors are clustered at the country-level.

V. Conclusion

Cyber security has surged in importance in recent years given the frequency and severity of attacks against countries, companies, and individuals. However, very little is known about the overall preparedness of countries to defend against these attacks. This paper uses new 2014 and 2017 data from the International Telecommunications Union (ITU) to measure the cross-section of cyber security readiness and quantify the main factors that explain its dispersion on a sample of over 200 countries.

Our parsimonious theoretical framework relates a country's cyber readiness with its institutional threat, institutional returns, and institutional capacity. We find that countries which are positioned in a more threatening security environment are more likely to have a high level of cyber readiness. Also, we note that countries that are highly dependent on cyberspace are more likely to have a high level of cyber readiness. More specifically, a country's level of ICT exports is one of the most robust and important predictors of cyber readiness.

Yet, surprisingly, we do not find a statistically significant association between our measures of institutional capacity and cyber readiness. In other words, states which have more resources available to allocate towards developing a reliable and frontier technology infrastructure do not seem actually make sufficient use of these assets to invest in cyber readiness. This suggests that economic development might be a necessary but not sufficient condition for realizing improvements in a country's cyber infrastructure.

Finally, this study remains to have a number of inherent limitations. Future research should consider to not only analyse differences in level of response but also in type of response. For example, whereas some countries have followed very much a legal approach to the issue, others have viewed cyberspace as a military domain to be defended. Analytically distinguishing these policy differences and explaining them would provide a fruitful avenue for future research. In addition. The existing measures of cyber readiness are very coarse. Other studies could try and incorporate more firm-level data to understand what firms and sectors are better prepared. It would be useful to have more measures of readiness over time – instead of merely cross-sectional – given the differences across countries.

References

Akamai, (2014): “The State of the Internet” Retrieved from: https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/index.jsp?WT.ac=soti_banner.

Allison, G. and P. Zelikow (1999): “Essence of decision: Explaining the Cuban Missile Crisis,” Pearson.

Baldwin, D. A. (1997): “The concept of security,” Review of International Studies, 23, 5–26.

Barlyn, S. (2017): “Global cyber attack could spur $53 billion in losses: Lloyd's of London,” Reuters, retrieved from: https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

Bertrand, M., E. Duflo, and S. Mullainathan (2004): “How much should we trust differences-in-differences estimates?” Quarterly Journal of Economics, 119, 249–275.

Betts, R. K. (1995): “Military Readiness: Concepts, Choices, Consequences,” Washington, DC: Brookings Institution Press.

Betz, D. J. and T. Stevens (2012): “Cyberspace and the state: Towards a strategy for cyber-power,” Routledge, Adelphi series.

Burton, J. (2013) “Small states and cyber security: The case of New Zealand,” Political Science, 65:2, 216-238

Blank, S. (2013): “Russia information warfare as domestic counterinsurgency,” American Foreign Policy Interests, 35, 31–44.

Booz Allen Hamilton and The Economist Intelligence Unit, (2011): “Cyber Power Index: Findings and Methodology,” retrieved from: http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

Boulanin, V. (2013): “Cybersecurity and the arms industry,” SIPRI Yearbook.

Burton, J. (2013): “Small states and cyber security: The case of New Zealand,” Political Science, 65, 216–238.

Chang, A. (2014): “Warring state: China’s cybersecurity strategy,” Center for a New American Security

Cohen, R. (1978): “Threat Perception in International Crisis,” *Political Science Quarterly*, 1, (1978)

Dilanian, K. (2013): “Cyber-attacks a bigger threat than Al-Qaeda, officials say”, Los Angeles Times, Retrieved from: http://articles.latimes.com/2013/mar/12/world/la-fg-worldwide-threats-20130313;

Deibert, R. (2012): “The growing dark side of cyberspace (. . . and what to do about it),” Penn State Journal of Law & International Affairs, 1.

Ebert, H. and T. Maurer (2013): “Contested Cyberspace and Rising Powers,” Third World Quarterly, 34,1054–1074.

FireEye, (2013): “Advanced Threat Report: 2013, ” Special Report, Retrieved from: http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2013.pdf

Hathaway, M., (2013): "Cyber Readiness Index 1.0." Presentation, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Hathaway, M., (2015): “Cyber Readiness Index 2.0; A Plan For Cyber Readiness: A Baseline and an Index,” Potomac Institute.
IMPACT, (2015): “Alphabetical List,“ Retrieved from: http://www.impact-alliance.org/countries/alphabetical-list.html

Inkster, N. (2010): “China in cyberspace,” Survival: Global Politics and Strategy, 52, 55–56.

ITU (2018): GCI 2017, retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx/

Kuehl, D. T. (2009): “From cyberspace to cyberpower: Defining the problem,” Washington, DC: Potomac Books.

Lachow, I. (2013): “Active cyber defense: A framework for policymakers,” Center for a New American Security.

Lewis, J. A. and K. Timlin (2011): “Cybersecurity and cyberwarfare,” Center for Strategic and International Studies.

Libicki, M. (2009): “Cyberdeterrence and cyberwar,” RAND Corporation.

Ebert, H and Maurer, T. (2013), “Contested Cyberspace and Rising Powers," Third World Quarterly, 34:6, 1054-1074

Rosenzweig, P. (2013): “International Law and Private Actor Active Cyber Defensive Measures,” Stanford Journal of International Law, 47.

RSA, (2015): “Cybersecurity Poverty Index,” retrieved from: https://www.emc.com/collateral/ebook/rsa-cybersecurity-poverty-index-ebook.pdf

Russian Federation, (2013) “Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020,” Retrieved from: https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf

Saydjari, O. S. (2002): “Defending cyberspace,” Computer, 35, 125–127.

Segal, A. M. (2014): “Cyberspace: The new strategic realm in US-China relations,” Strategic Analysis, 38, 577–581.

Subramanian, A. (2013): “Preserving the open global economic system: A strategic blueprint for China and the

Singer, D. J., S. Bremer, and J. Stuckey. (1972). Capability distribution, uncertainty, and major power war, 1980-1965. In Bruce Russett (ed) Peace, War, and Numbers, Beverly Hills: Sage, 19-48.

Symantec, (2014): “Internet Security Threat Report 2014,” 19, Retrieved from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

United Nations Institute for Disarmament Research, (2013): “The Cyber Index: International Security Trends and Realities,“ United Nations Publications, retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

United States,” Peterson Institute for International Economics.

The Secretary of Defense, (2015): “the Department of Defense Cyber Strategy,” (April 2015), Retrieved from: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Tkacik, J. (2008): “Trojan dragon: China’s cyber threat,” Heritage Foundation.