Transnational Governance of Cybersecurity:

policy challenges and global inequalities in cyber capacity building[1]

Dr Andrea Calderaro

Cardiff University
CalderaroA@Cardiff.ac.uk

Anthony J S Craig

Cardiff University
CraigAJ@cardiff.ac.uk

Abstract

Connectivity infrastructure is constantly expanding, increasing internet access across countries, regions and socio-political contexts. Given the fast changing geography of the internet, there is a growing demand to strengthen cyber capacity beyond national frameworks, in order to develop a transnationally coherent and coordinated governance approach to cybersecurity. In this context, cyber capacity building initiatives are increasingly central in international debates, with the ambition to support countries in the global south in fostering their cybersecurity strategy from technical and policy perspectives. This article discusses the key factors explaining states' efforts to enhance their cyber capacity. Based on a cross-national quantitative research approach, the findings contradict IR derived approaches to cybersecurity, which assume that countries develop their cyber capacity according to external security threats, domestic politics, or norms. In line with existing research on the role that science play in policymaking processes more broadly, our results suggest instead that a country's science and technical knowledge is the most robust explanation for states' cyber capacity levels. These findings emphasise the need for policymakers to support countries in the global south in developing their cyber capacity beyond national security paradigms by further strengthen education and technical skills in contexts lacking in this resource.

Keywords: *Cybersecurity, Global South, Cyber Capacity Building, Transnational Governance, Scientific Knowledge, Digital Divide*

[1] Article published as: Calderaro, Andrea, and Anthony J. S. Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." *Third World Quarterly* 41(6): 917–38.

Introduction

The expansion of internet connectivity globally has increased the dependence of societies on cyberspace and consequently given rise to a host of vulnerabilities and threats. In this context, one of the most pressing questions is how to build the necessary cybersecurity capacity to protect societies from digital harms. This task is especially critical in relation to the global south where internet usage is growing fast yet the ability to secure infrastructure is lagging. Given the interconnectedness of cyberspace and the transnational nature of digital threats, enhancing international cooperation in the cyber domain beyond the global north is crucial to develop a coherent and coordinated transnational governance approach to cybersecurity.

Existing efforts to address cybersecurity from an international relations (IR) perspective have not adequately tackled the pressing issue of fostering cyber capacity in the global south. Rather, there has been an emphasis on the concept of deterrence, derived from the nuclear weapons era, as a means of reducing cyber threats. The suggestion is that states can avoid attack by investing in cyber capabilities to signal to rival political actors that aggression will either be met with punishment or will not be worth their efforts. However, there is so far little evidence this approach is helpful in explaining cyber capacity building processes.

We argue that identifying the determinants of cross-national variation in cybersecurity is crucial to inform international policy initiatives aiming at supporting cyber capacity building among countries in the global south. In this context, this article empirically examines the factors influencing the level of cybersecurity readiness across countries with the aim of better understanding how policy initiatives should support countries' efforts in developing cyber capacity. Multivariate regression analysis is used to test the effect of a broad range of explanatory variables on a country's level of cyber capacity using three existing measures: the 2014 and 2017 versions of the Global Cybersecurity Index by the UN International Telecommunication Union (ITU) and the National Cyber Security Index developed by the Estonian e-Governance Academy Foundation.

The key findings are that IR theory-driven approaches to cybersecurity inspired by military and deterrence paradigms have little observable impact on a country's cyber capacity. Specifically, countries do not appear to be motivated by the need to deter against international rivals or cyber-attacks. This suggests the misplacement of these approaches in this context. In contrast, the production of science and technical (S&T) knowledge in the country appears to be a key driver of

cyber capacity, which leads to a clear recommendation that policymakers should further their efforts to enhance scientific and technical knowledge in newly connected countries.

The transnational nature of Cybersecurity in a fast-changing Digital Geography

The geography of the internet is rapidly changing, generating new challenges in ensuring an open, neutral, and sustainable global connectivity infrastructure (Calderaro 2014; Ebert and Maurer 2013; Kshetri 2010). In 2003 only 10 per cent of the worldwide population had access to the internet and most of its users were concentrated in North America and Western Europe.[2] Today, almost 50 per cent of the worldwide population is connected to the internet, most of which live outside these regions. As illustrated in figure 1, 50 per cent of the internet population in 2017 lives in Asia. In contrast, North America and Europe now only represent 8 per cent and 20 per cent of the internet population respectively. The global distribution of internet connectivity is clearly shifting away from its original concentration in the global north.

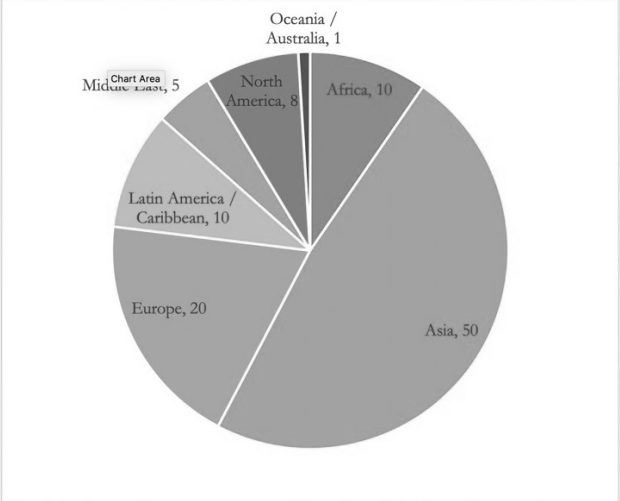

Figure 1 - Distribution of Internet Users Worldwide (%), 2017

Focusing on the group of countries categorized by the UN (2019) as Least Developed Countries (LDCs), referring to low-income countries confronting severe structural impediments to

[2] ITU defines as "internet users" individuals that have accessed the internet from any devices within the last 12 months. ITU Statistics "Global ICT developments 2001-2017", available at: http://www.itu.int/ict/statistics

sustainable development,[3] LDCs have made substantial strides in connectivity in recent years. Table 1 demonstrates that although higher income countries have much greater rates of internet usage (82.43 per cent in 2017) it is in the global south that we see larger increases in internet penetration. In 2010 only 4 per cent of the population in LDCs used the internet compared with 72 per cent among higher income countries. In 2017 however this had increased to almost 18 per cent among LDCs reflecting an increase in 13.65 percentage points. By comparison, internet penetration in higher income countries over the same period had increased by 10.3 percentage points. If these trends continue, it is estimated that by 2025 almost 5 billion of the worldwide population will be connected to the internet, and 75 per cent of them will live in the global south (Kleiner, Nicholas, and Sullivan 2014).

Table 1. Internet penetration among Developed Countries and LDCs

	2010	2017	Difference
Developed Countries	72.13%	82.43%	+10.30
LDCs	4.13%	17.78%	+13.65

Technology traditionally evolves quicker than our capacity to foresee its impact on our political, social, and economic systems. As a consequence, the implementation of regulations, norms, and governance processes aiming at making this impact sustainable is often slower than the technological developments. This is particularly pressing in the global south, where the expansion of connectivity is developing considerably quicker than the ability of governments, industries and civil society to develop the technical and policy capacity to reap the benefits of connectivity, while limiting their exposure to threats emerging from digital infrastructure.

Given the fast-changing geography of the internet, there is an increasing need to enhance international cooperation beyond the global north with the goal of developing a transnational governance approach to cybersecurity where newly connected countries are expected to be increasingly influential in consolidating the security of connectivity as a whole. Building cyber capacity in the global south is crucial not only to protect potentially vulnerable political, economic, and social institutions from digital treats, but also to protect other countries against malicious cyber

[3] According to the UN, "The assignment of countries or areas to specific groupings is for statistical convenience and does not imply any assumption regarding political or other affiliation of countries or territories by the United Nations" (United Nations Statistics Division 2019).

activity that often originates in the countries that lack adequate infrastructure and governance (Pawlak 2016; Schia 2018). In addition to fostering domestic capacity, the implementation of cyber capacity building strategies should also support countries in the global south to increase their potential as active players in the transnational governance approach to cybersecurity, by developing diplomatic capacity to negotiate norms and transnational agreements in international fora.

In this context, we refer to cyber capacity building as the diffusion of technical, governance and diplomatic skills among relevant stakeholders, including government, industry and civil society actors, in order to ensure the development of sustainable connectivity.

To help inform these debates, some key questions must be investigated: what are the determining factors of existing cybersecurity capacity worldwide? Are existing theoretical perspectives so far adopted to explain cybersecurity challenges useful to understand cyber capacity building inequalities worldwide? What should international policymakers prioritize in their efforts of developing cyber capabilities in the global south?

Cyber Capacity Building as an emerging ambition for international diplomacy

Despite the increasing awareness of the potential implications of cybersecurity, we still lack a clear understanding of what developing cybersecurity capacity actually means. This can be explained by the fact that since internet connectivity affects most aspects of the economy, human security, and global politics, cybersecurity takes different meanings depending on the community addressing the issue. From a technical perspective, cybersecurity usually refers to all initiatives taken to protect connectivity infrastructure and digital services from disruption. This is a perspective adopted by the UN's agency International Telecommunication Union (ITU) and the International Standardisation Organization (ISO) which approach cybersecurity as the threats relating to Information Communication Technologies (ISO 2012). The Organization for Economic Cooperation and Development (OECD) approaches the concept as "Digital Security Risk Management" (OECD 2015) when they refer to economic risks associated with digital disruptions. Finally, and entirely in line with their mandate of targeting criminal activities, Europol associates the concept of cybersecurity with cybercrime (European Union Agency for Law Enforcement Cooperation, 2018).

The rich body of scholarly literature in the field offers the same variegated approach in addressing cybersecurity. A significant distinction in the academic community exists between scholars conceptualising cybersecurity from a human security perspective (Deibert 2013; Mueller 2017; Dunn-Cavelty 2008) and those interested in the role of cyber threats in the context of state security (Demchak and Dombrowski 2011; Rid 2013; Singer and Friedman 2014). The former focuses on cybersecurity as a set of strategies, law enforcement and technical solutions aiming at protecting society in their daily public use of digital services. From this perspective, security in digital environments concerns the protection of digital rights, namely the right to privacy and online freedom of expression. On the other hand, the latter is interested in understanding how cyber threats might target and disrupt state sovereignty, which involves looking at cybersecurity as a military concern.

The approach to cybersecurity as a national security concern should be combined with the call for efforts to develop a transnational approach to cybersecurity. The coexistence of, on the one hand, the transnational nature of the internet infrastructure, including the routing of data and the adoption of protocols beyond state borders, and, on the other hand, governments' claim to digital sovereignty, has existed since the early negotiations addressing the management of the Domain Name System, which has given rise to ICANN (Mueller 2019). More recently, this clash has become particularly relevant given the increased security concerns related to digital infrastructure. Despite its transnational nature, the internet is made up of hardware that is physically distributed within national borders, enabling countries to claim their sovereignty over the functioning, governance, and safety of these segments of the transnational infrastructure. This state-centric perspective is justified given that cyber threats are traditionally considered to target states' sovereignty, pushing the discussion about cybersecurity toward the domain of national state security (Mueller 2017). However, in line with other areas of security, where the distinction between internal and external security is increasingly blurred, national security in the cyber domain may be reinforced with a national strategy and expertise but it also requires the proper functioning of the infrastructure as a whole. As a result, safety and sustainability of connectivity must rely on both national strategy and a transnational governance approach to cybersecurity. The need to implement such a complementary approach is in line with most of the contemporary challenges animating different debates in the domain of transnational governance, such as, for example, climate changes, human rights and several other issues (Scholte 2005; Zürn 2018).

The need to promote cyber capacity globally is evident in various initiatives undertaken at the international, regional, and national levels. For instance, the UN Group of Government Experts (UN GGE) recognised in its 2015 report that "different levels of capacity for ICT security among states can increase vulnerability in an interconnected world" (United Nations 2015, 7) and has called for increased international cooperation to assist countries in developing cyber capacity (United Nations 2015). With the recently launched United Nations Open Ended Working Group (OEWG) the UN has launched the first ever multistakeholder consultation on cybersecurity stability, complementary to the UN GGE. This is a relevant example where newly connected countries are called on to play a role in an emerging transnational approach to cybersecurity. In this context, a call for developing not only national technical skills necessary to reinforce cybersecurity solutions from an enginering perspective, but also to improve the capacity to engage with transnational governance processes in the domain of cybersecurity has emerged as a critical priority during the three day meeting of the UN OEWG at the UN headquarter in December 2019.[4]

With the "Operational Guidance for EU's International Cooperation in Cyber Capacity Building" (European Commission 2018), the EU sets out a pragmatic plan to assess and develop sustainable cybersecurity strategies, to be used not only by EU institutions but also by countries aiming at improving their cyber capacity (Council of the European Union 2018). Similarly, the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford has developed the "National Cybersecurity Capacity Building Model", offering a tool to assess national capacity building (Dutton et al. 2017). Furthermore, the United Kingdom has established a dedicated Cybersecurity Capacity Building program within its Foreign and Commonwealth Office (FCO), and it is one of the principal promoters of the Global Forum on Cyber Expertise (GFCE). The GFCE is an initiative originally launched by the Dutch Ministry of Foreign Affairs, in partnership with a high number of Foreign Ministries worldwide (now counting 38 State members worldwide). This initiative aims to create a global platform for states, international organizations, and private companies to coordinate on best practices in the field of cyber capacity building.

[4] More details about the "2019 UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security" are available: http://papersmart.unmeetings.org/ga/oewg-on-icts/2019-intersessional-meeting-with-industry-partners,-ngos-academia/statements

Theoretical Approaches to Cyber Capacity Building

All the initiatives aimed at supporting cyber capacity building strategies addressed so far have identified similar pathways to secure critical infrastructure against threats to defend national and economic security while ensuring respect for human rights. There is general agreement that cyber capacity is about achieving resilience against internet-based threats through a broad range of policies which include the creation of national cybersecurity strategies, Computer Security Incident Response Teams (CSIRT), the strengthening of cybercrime laws, the promotion of public-private partnerships, and improved education and awareness. Despite this, we know very little about the determinants of cybersecurity capacity across countries.

Scholars focusing on cybersecurity from an international relations perspective have mostly approached the issue in terms if the application of internet technology in international conflict. For instance, some have developed the concept of cyber weapons (Herr 2014; Rid and McBurney 2012) and military computer network operations (Buchanan 2016), investigated the impact of cyber capabilities on traditional power dynamics in the international system (Gartzke 2013; Kello 2017; Liff 2012; Lindsay 2013; Valeriano, Jensen, and Maness 2018), or questioned whether cyber capabilities can deter conflict (Liff 2012, Brantley 2017, Nye 2017). Beyond the intellectual efforts to identify the more suitable theoretical framework explaining cybersecurity challenges, these distinctive approaches to cybersecurity have practical implications on how to design cybersecurity governance strategies.

Most IR theories adopted to react to emerging cybersecurity challenges are inspired by approaches traditionally associating security with military initiatives. As a result of this, digital tools are often referred to so-called cyber weapons, and cyber capabilities are thought of as a tool to build deterrence strategies with the goal to protect National Security from cyber threats. However, this approach is misleading, given that digital tools are immaterial as such and are difficult to compare with traditional arms, cyberattacks are rarely tangible and, most importantly, attribution of cyberattacks is still challenging. In this context, the reaction of governments to cyberattacks could be triggered by uncertain attributions, with the risk to undermine geopolitical order instead than fostering stability. This raises many problems when applying the rich literature in the field of "deterrence" to the cyber domain (Clarke and Knake 2010), turning the narrative built around cybersecurity as an emerging challenge for military strategy worldwide inspired by "cold war" times not fully justified (Nye 2017). In other words, even if cybersecurity narratives are often derived

from defence strategies, such as cyberweapons, cyberwar, and cyber command, we have little empirical evidence that these military-inspired approaches are entirely justified and therefore reflect countries' efforts to develop their cyber capacity. If so, we should not expect countries developing cyber capacity in line with the so-called 'cyber arms race' narrative (Taddeo and Floridi 2018), describing countries' efforts worldwide to develop cyber capacity in order to reinforce national military power.

Although there is intense debate about the effect of cyber capabilities on international security, little research has been done on why some states are better prepared for cybersecurity than others. Several indices of national cyber capacity have been published in recent years by independent institutes and international organisations,[5] but there is little academic analysis to explain this process. Some research has addressed the application of cybersecurity norms already in the early stages of countries' connectivity building processes in order to understand how these adapt to the national context (Calderaro 2015), and other research is underway to quantify and explain the proliferation of cyber capabilities from the perspective of military operations (Craig 2018). Makridis and Smeets (2019) quanitatively assess the determinants of cyber capacity and suggest that a country's international threat environment provides the best explanation for increased cyber capacity while finding that domestic resources are less important. Their indicator of threat environment – Correlates of War CINC score – is a well-established measure of material capabilities based on population, raw materials, and military power, however it says little about the security threats facing a state.

Other scholars have examined the impact of national initiatives on cybersecurity outcomes at the technical level. Of particular relevance, Ashgari et al (2015), find the factors that are most correlated with botnet infection rates are a country's rate of pirated software use and its ICT development. Their findings suggest that lower income countries where authors argue that the use of unlicenced software is widespread and where the population lacks ICT infrastructure, skills, and education are the most vulnerable in cybersecurity, which contrasts with the common belief that the higher income countries are the most vulnerable in cyberspace given their greater internet dependence (Clarke and Knake 2010).

[5] For an overview of these efforts see the Index of Indices, available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/2017_Index_of_Indices.pdf

We build on this body of research by explaining variation in cyber capacity by relying on the aforementioned cyber capacity indices that gauge the institutional, technical, organizational, and legal efforts countries have engaged in to improve cybersecurity. Since previous research offered little evidence about the drivers of cyber capacity so far, we use a broad explanatory framework drawn from a range of IR perspectives. We do not assess the impact of these perspectives on actual cybersecurity outcomes (i.e. reduced infection rates from computer viruses) but on the general level of preparedness reflected in national level initiatives taken to build cyber capacity.

Based on the outcome of this study, we argue that countries' initiatives aimed at promoting cyber capacity are not moved by military and security paradigms, but by a country's access to science and technical knowledge. Despite the rhetoric that cybersecurity is a military domain, this research will suggest that the way forward is for policy makers to focus their efforts on developing the domestic capacity to improve cybersecurity through the insititutional development of skills and knowledge.

The drivers of cyber capacity from an IR perspective

In order to identify the drivers of cyber capacity and explain the divide between the global north and south, we draw on multiple IR perspectives relevant for explaining national capabilities. This helps both structure our analysis and provides an opportunity to evaluate their utility in explaining the relatively novel area of cyber capacity. In this section we set out our empirical expectations based on arguments derived from the realist emphasis on external threat environment, the liberal focus on domestic politics, and constructivist interest in inter-governmental organizations (IGOs) and power status. Moreover, we draw on arguments that the development of capabilities depends on the country's resources to develop capacity, independent of its political motivations.

The first set of explanatory factors is informed by Realist IR theory which is founded on the idea that states operating in the self-help, anarchical international system are responsive to security threats from other countries and seek to deter aggression and ensure their survival through military build-ups (Jervis 1978; Waltz 1979). Capacity building in the cyber domain may also be motivated by a need to deter threats. The ability of states to infiltrate one another's computer networks for strategic gain creates a cybersecurity dilemma, according to Buchanan (2016), which as realists argue drive a mutual build up of capabilities to restore security (Jervis 1978). The threat posed by the cyber activity of rival actors could promote the development of cyber capacity in preparation for an attack and to build a deterrent capability either through denial or punishment (Nye 2017).

If states develop cyber capacity to reduce digital threats from their rivals, it follows that states facing more substantial threats or more rivalry should be more interested in building cyber capacity. Security threats can be conceptualised in terms of conventional threats and cyber-based threats. In this analysis, we can assess the effects of both on cyber readiness.

Alternatively, one can look to domestic politics to explain cyber capacity. Liberal IR theory suggests that due to the structural constraints on the executive in democracies (Maoz and Russett 1993), democratically elected governments are more responsive to the demands of their populations than authoritarian states. Cyber threats may not actually be more significant in democracies, but democratic governments may have higher pressure to invest in cyber capacity to avoid suffering negative audience costs. Moreover, regime type may capture the effects of the so called 'cyber-industrial complex' (Carr 2016; Deibert 2011) whereby vested economic and political interests push for increased investment in cyber capacity, partly through cyber threat inflation and 'cyber doom scenarios' (Dunn-Cavelty 2008; Lawson 2013). This phenomenon may be more likely in a democracy due to societal openness giving interest groups more influence in the political decision-making process. On the other hand, authoritarian states could have higher capacity because of greater efficiency whereas relatively new democracies, especially in the global south, may lack the stability to build cyber capacity.

A second domestic political factor is the level of stability in a country. Scholars have shown that civil war has an enormous negative impact on a country's economy (Collier 1999; Stewart, Huang, and Wang 2000). Civil war creates instability and may reduce the capacity of governments to invest in cybersecurity because resources are being focused on restoring stability. Therefore, one might expect a negative relationship between civil war severity and cyber capacity development. Civil war is more prevalent in lower income countries which could be an impediment to their cybersecurity development.

The third set of factors relate to constructivist-based arguments regarding norms and status. Constructivist IR scholars argue that inter-governmental organisations (IGOs) can help shape state behaviour through the development of norms that define the parameters of acceptable behaviour internationally (Finnemore and Sikkink 1998). The concept of cyber-norms and the institutions that could promote them in areas such as technological export controls, the non-proliferation of cyber weapons, and restraint from cyber conflict have already been discussed by scholars (Finnemore and Hollis 2016; Nye 2014). Greater membership in IGOs reflects a stronger

willingness by a state to engage with global governance efforts and abide by the norms of the international community. Assuming the international community is currently promoting the norm of cyber capacity building, one might expect there to be a greater tendency towards cyber capacity building amongst countries that are in general more cooperative and engaged internationally, in contrast with pariah states such as North Korea that are detached from global governance efforts and less influenced by norms.

Another constructivist-based concept is that of status and prestige. Prior research suggests that states seek military capabilities, including nuclear weapons, as a status symbol (Buzan and Herring 1998; Sagan 1996), and a similar dynamic may exist in the cyber domain. Countries that consider themselves as significant players in international politics may pursue cyber capacity because it befits a state of their status and confers prestige. Major or regional powers, most of which lie in the global north, may therefore be expected to possess greater levels of cyber capacity.

An important condition for the build-up of cyber capacity is whether the country possesses adequate resources to achieve its desired cybersecurity goals. This argument derives from the theory of Opportunity and Willingness (Most and Starr 1989), which suggests that states require both opportunity (capacity) and willingness (interest) to act in a given area. This framework has been employed for explaining a wide range of state activity from international conflict, arms production, or military technology adoption (Early 2014; Fuhrmann and Horowitz 2017; Jo and Gartzke 2007; Kinsella 2000; Siverson and Starr 1991). The final set of factors, therefore, relate to the opportunity to develop cyber capacity, which is determined by its access to resources. Resources should be critical for explaining the cyber capacity divide between the global north and south given the historical inequalities in terms of economic development, industrialisation, and knowledge production.

Arguments can be made as to the importance of several types of resources for developing cyber capacity. For instance, financial resources should be essential to fund national cybersecurity policies, organisations, and hire personnel, industrial capacity should allow a state to draw expertise and technology from the private sector, while a society's level of knowledge and skills should be essential for developing secure technologies and having access to trained IT professionals. In the cybersecurity and IR literature, scholars have argued that skill (applied knowledge) should be a particularly critical factor for maintaining the capability to create malware (Slayton 2017) or for carrying out sophisticated cyber operations (Lindsay 2013). In the development literature on cyber

capacity, scholars have argued that the gap in skills and knowledge is one of the key reasons behind different levels of cyber capacity between the global north and global south (Pawlak and Barmpaliou 2017; Schia 2018). Yet the importance of scientific knowledge as a driver of cybersecurity capacity has not yet been validated empirically using a large sample of countries.

Research Design

We use Ordinary Least Squares (OLS) regression on a cross-sectional dataset of 193 UN member states to explain country-level variation in cyber capacity globally. This method of regression is suitable because of the continuous nature of the dependent variables. To build robustness for our findings, we use three dependent variables which we draw from pre-existing indices of cyber capacity. Below we explain each in turn and then set out our choice of explanatory variables which are used to test the IR-based theories we have applied to cyber capacity building. For consistency, the independent variables are taken from the year 2014 where possible and unless otherwise stated, which is also the year the first ITU index was published.

Dependent variables

Numerous cyber capacity indices have been published recently, although they vary in terms of country coverage and methodology.[6] Some include too few countries for a valid statistical analysis, while others only offer a qualitative assessment of capacity. For this reason, only three of these indices are suitable for the quantitative nature of this article.

The first dependent variable is a country's cyber capacity score according to the 2014 Global Cybersecurity Index (GCI) from the International Telecommunications Union. This index assesses "the existence of national structures in place to implement and promote cybersecurity" in 194 UN member states. The index ranges from 0 to 1 and gauges a country's cyber readiness across five categories - legal, technical, organisational, capacity building, and cooperation – via surveys and secondary research of each country. Points are allocated to each country according to its level of development in each area (none, partial, full), which are then standardised and combined into an index used to rank countries. The legal component assesses whether the state has enacted legislation regarding cybercrime, data protection, incident response, and certifications or standards.

[6] A list of cyber capacity indices is available at:
https://www.itu.int/en/ITUD/Cybersecurity/Documents/2017_Index_of_Indices.pdf

The technical component assesses whether the country has a Computer Security Incident Response Team (CSIRT) and has implemented standards and certification. The organisational component assesses whether the country has a national cybersecurity strategy or policy, a national agency, and benchmarking. The capacity building component incorporates cybersecurity research projects, education and training programmes, numbers of certified professionals, and accredited agencies. Finally, the cooperation component examines intrastate, intra-agency, and public-private partnerships, as well as participation in international organisations.

The second dependent variable is the 2017 version of the GCI which uses an updated methodology, specifically through the use of a binary rather than three-level coding strategy of cyber capacity developments, additional survey questions to member states, and improved facilities for member states to provde evidence to the ITU.

The third dependent variable is the National Cyber Security Index by the think tank "e-Governance Academy", based in Estonia. The NCSI is aimed at gauging a state's defence and resilience against cyber threats and creates an index based on a country's cybersecurity legislation, organizations, policies, and education among other factors. The NCSI arrives at an index through an alternative mathematical formula to the GCI.

Given that our main focus is on cybersecurity governance capacity, our outcome variables mostly reflect national-level cybersecurity rather than cybersecurity capacity in terms of technical standards, software vulnerabilities, encryption technologies, the practices of ISPs, or infection rates, for example. Nevertheless, the indices we use should correlate with technical cyber security capacity given that countries with stronger institutional development evidently have greater resources and willingness to improve cybersecurity at the technical level. Moreover, conducting the study using national level indicators allows us to highlight the deficieny of particular explanatory factors or the importance of others.

We explain variation in these indicators in three separate regression models, since their divergent methodologies means they cannot be aggregated into one dependent variable. Nevertheless, together they offer a test for robustness in our findings, especially if a given explanatory factor has a consistent effect across each model. To first test the similarity of these indices we obtain the correlation coefficients between them.

Table 2. Correlations between cyber capacity building indices

	GCI 2014	GCI 2017	NCSI
GCI 2014	1.000		
GCI 2017	0.849	1.000	
NCSI	0.656	0.707	1.000

As illustrated in Table 2, the two GCI measures are very highly correlated (0.849), reflecting the fact they are published by the same organisation and adopt similar methods. The correlations between the NCSI and GCI 2014 (0.656) and the GCI 2017 (0.707) are also strong, suggesting that both organisations are capturing a broadly similar concept despite divergent methods.

Explanatory variables

Our explanatory variables are drawn from our previous discussion of IR theories as they apply to cybersecurity capacity building. Table 3 provides a summary of these variables, grouped according to the theoretical perspective from which they are derived, their measurement, and their data source. These are then explained more fully in the next section.

Table 3. Overview of explanatory variables

Theoretical perspective	Indicator	Definition	Data source
Realist	Interstate rivalry	Average number of interstate rivals (2004-2013)	Peace scale
	Cyber threat	Average number of cyber incidents over previous 10 years (2005-2014)	Cyber Operations Tracker
Domestic politics	Regime type	Democracy-autocracy score (2014)	Polity IV
	Civil War	Average magnitude of civil conflict (2005-2014)	Major Episodes of Political Violence
Constructivism	IGO membership	Number of IGOs state is a member of as of 2014	Correlates of War
	Power status	Is the state a regional or major power (based on CINC scores, 2014)	Correlates of War
Domestic resources	Financial resources	Log of GDP per capita (constant US dollars, 2014)	World Development Indicators
	IT industry	Log of ICT service exports (current US dollars, 2014)	World Development Indicators
	Scientific and technical knowledge	Log of Scientific and technical journal articles (2014)	World Development Indicators
	Broadband internet penetration	Fixed broadband users per 100 people (2014)	World Development Indicators
	Mobile internet penetration	Mobile internet users per 100 people (2014)	World Development Indicators

Realist derived indicators

External threat environment. The conventional threat is measured by the average number of interstate rivalries a country has been engaged in over the previous 10 years. Rivalry describes a "relationship in which decision makers have singled out other states as distinctive competitors and enemies

posing some actual or potential military threat" (Colaresi, Rasler, and Thompson 2008, 3). A rivalry is characterised by longstanding hostility and competition between a pair of states over issues such as territorial disputes or relative power and influence. As such it is an appropriate method for gauging a state's external security environment. It is generally accepted that the perceived threat and hostility associated with interstate rivalry increases the likelihood of mutual military build-ups (Rider, Findley, and Diehl 2011; Vasquez 2013) and may also drive the build-up of cyber capacity more generally, given the prominence of cyber conflict between rival states (Valeriano and Maness 2015). The data comes from the Goertz, Diehl, and Balas (2016) peace scale dataset.

Cyber Threat. To assess the hypothesis that countries facing greater levels of cyber threat will have developed higher cyber capacity, we create a variable for the number of cyber incidents that have affected the state over the previous ten years. This information comes from the Cyber Operations Tracker from the Council on Foreign Relations,[7] which records publicly known computer network operations since 2005 and identifies which country was targeted. These include DDoS, espionage, defacement, data destruction, sabotage, and doxing. Caveats to the use of this data include the potential for cyberattacks to go unreported and the relative over-reporting within some countries.

Domestic politics

Regime type. Regime type refers to how democratic or authoritarian a country's government is. The data comes from Polity IV project's autocracy-democracy scores, which places countries on a scale from -10 (most authoritarian) to 10 (most democratic) (Gurr, Jaggers, and Moore 1990).

Civil war. With this indicator we asses potential internal conflict, as a dummy variable to measure internal security concerns. Civil war data comes from the Major Episode of Political Violence dataset (MEPV) and is measured by the average annual magnitude of civil violence and civil war over the previous ten years (2005-2014).

Constructivism derived indicators

Inter-Governmental Organisations membership. Engagement in international organisations is measured by the count of IGOs a country is a member of as of 2014 from the intergovernmental

[7] More information available at: https://www.cfr.org/interactive/cyber-operations

organisations' data set (v3) from the Correlates of War. IGOs are organisations "set up by three or more states to fulfil common purposes or attain common objectives" (Feld, Jordan, and Hurwitz 1994, 10).

Power status. Prestige seeking is indicated by whether the country is a major and/or regional power. Major power status comes from the Correlates of War state system membership data set (version 2016). Additionally, we determine if the state is a regional power if it has at least a third of the material capabilities of the most powerful country in the region, using the CINC scores from the Correlates of War.

Latent resources and infrastructure

S&T knowledge. The level of scientific and technical knowledge (S&T) available in the society is measured by the number of scientific and technical journal articles per million people published from that country. This data comes from the World Development Indicators (WDI) by the World Bank. Endogeneity (reverse causality) should not be a serious issue here since scientific and technical journal articles are mostly exogenous to cybersecurity capacity as it incorporates a much broader array of scientific disciplines than those related directly to cybersecurity.[8]

Economic development. Economic development and financial resources is measured by Gross Domestic Product (GDP) per capita (current US dollars), which we obtain from the WDI.

ICT Industry. The size of the ICT industry is measured by a country's ICT service exports (current US dollars), with data from from the WDI. Services rather than goods are used because data on goods can capture the mass production of physical equipment that does not necessarily reflect the sophistication of industry.

Infrastructure. Internet infrastructure is controlled for by including two variables - the percentage of a country's population with a fixed broadband subscription and the percentage with a mobile subscription, thus taking into account the most prominent methods of internet access. These data are from the WDI.

Data analysis

[8] S&T articles, GDP per capita, and ICT service exports are log transformed to correct for their skew and better model a linear relationship.

Before turning to the multivariate regression results, we present some descriptive data to highlight the cybersecurity divide between the global north and global south. Figure 2 compares the average cyber capacity (using the GCI 2014 and 2017) between LDCs and Developed Countries, as defined by the UN classification. Contrary to the difference in internet growth between global north and south countries shown earlier, cyber capacity appears to have increased more from 2014 to 2017 among Developed Countries as it has among LDCs. It is possible though that this difference is a result of methodological changes between the two indices. Regardless of which version of the GCI used, however, it is clear that Developed Countries are far ahead of LDCs in their level of cyber preparedness.

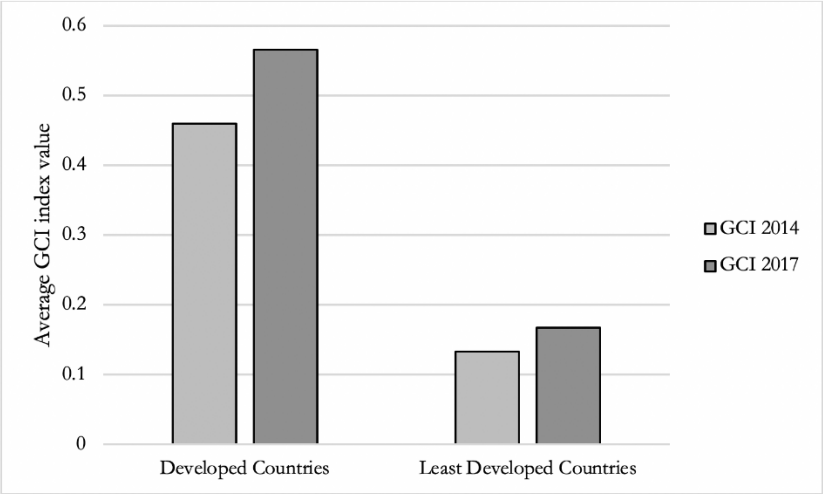

Figure 2 - Cyber Capacity among Developed Countries and LDCs

LDCs are clearly at a disadvantage in cybersecurity capacity, with Developed Countries having on average an index score of between 0.4 and 0.6 and LDCs having a score of between 0.1 and 0.2.

The next step of the analysis can shed more light on what factors may be driving this inequality, beyond that of economic development. Table 4 shows the results of three linear regression models where the effect of our independent variables on cyber capacity according to three different indices are examined. In models 1 to 3, the dependent variables are the ITU GCI 2014, GCI 2017, and the NCSI. For each independent variable, robust standard errors are displayed in parenthesis below the regression coefficients. The coefficients convey the effect of a one unit increase in each explanatory variable on the cyber capacity value. The level of statistical significance is denoted by the asterixis next to the coefficients according to the system noted at the bottom of the regression table.

Table 4. Multivariate OLS regression of cybersecurity capacity

Theoretical perspective	Indicator	(1) GCI 2014	(2) GCI 2017	(3) NCSI
Realist	Cyber threat	0.00767*	0.00459	-0.224
		(2.02)	(1.58)	(-0.85)
	Interstate rivalry	-0.000763	0.00331	-0.497
		(-0.05)	(0.25)	(-0.48)
Domestic politics	Regime type	-0.00419	-0.00694*	0.0673
		(-1.40)	(-2.43)	(0.27)
	Civil war	0.0265*	0.0207*	-0.0402
		(2.23)	(2.14)	(-0.05)
Constructivism	IGO membership	0.00309**	0.00195	0.0266
		(2.83)	(1.78)	(0.27)
	Power status	0.0502	0.0539	1.135
		(1.06)	(1.34)	(0.27)
Domestic resources	S&T knowledge	0.0461***	0.0515***	4.201***
		(3.58)	(4.42)	(3.47)
	GDP (per capita)	-0.00399	-0.0202	-1.490
		(-0.18)	(-0.89)	(-0.63)
	ICT Serv. Exports	0.00685	0.0211*	2.524**
		(0.69)	(1.99)	(2.93)
Infrastructure	Broadband Subs.	0.00211	0.00368	0.582*
		(0.69)	(1.31)	(2.39)
	Mobile Subs.	0.000378	0.000705	0.0467
		(0.73)	(1.46)	(0.85)
	Constant	-0.236	-0.271	-27.99
		(-1.03)	(-1.10)	(-1.38)
	Observations	142	142	114
	R^2	0.62	0.68	0.73

Notes: t-statistics in parenthesis. Statistical significance denoted by * p<0.05, ** p<0.01, *** p<0.001

The R squared statistic at the lower end of the table allow us to assess the performance of each model as it describes the proportion of variance in cyber capacity indices that are explained by the variables in the model. Model 1 explains 62 per cent of the variance in the dependent variable, model 2 explains 68 per cent, and model 3 explains 73 per cent. This suggests that our set of independent variables are explaining variation in cyber capacity relatively well, although there is still some variance left unexplained.

Turning to the specific results, the findings lend most support to domestic resources as being important determinants of cybersecurity capacity. S&T knowledge, as measured by scientific and

technical journal articles, is the most consistent predictor of cyber capacity across all models, maintaining a positive and highly statistically significant relationship ($p<0.001$) in relation to each dependent variable. A one unit increase in the log of scientific journal articles per million people is associated with a rise in 0.046 in the GCI 2014 score, 0.052 in the GCI 2017 score, and 4.201 in the NCSI score. The more scientific research a country produces, the higher its cyber capacity is likely to be while controlling for other factors, suggesting that S&T knowledge is a crucial resource for developing cybersecurity readiness.

No other factor has a consistent effect in these models. ICT service exports has a significant and positive impact when using the GCI 2017 and the NCSI, but not the GCI 2014. Specifically, a one unit increase in ICT service exports corresponds to a 0.021 increase in the GCI 2014 score and a 2.524 increase in the NCSI score. Internet infrastructure does not appear to have an independent impact on cyber capacity, with only broadband usage being statistically significant in model 3. Results can therefore vary depending on the methods used to create a cyber capacity index. There is no firm evidence that infrastructure and industry are driving cyber capacity, unlike S&T knowledge which has a consistent effect.

Although GDP per capita and the cyber capacity indices are strongly correlated to one another, GDP per capita is not statistically significant in any model when controlling for other factors. This is because S&T knowledge is an intervening variable between economic development and cyber capacity. An intervening variable is one that follows an independent variable and precedes a dependent variable in a causal sequence. It is likely that higher income countries are better able to generate more S&T knowledge which in turn leads to greater cybersecurity capacity. So, it is not that GDP per capita is unimportant. To the contrary, a lack of economic resources is probably an underlying cause of low cyber capacity, but it has its effect via its influence on S&T knowledge. GDP per capita becomes insignificant when controlling for S&T knowledge because S&T knowledge is the more proximate cause.

Interestingly, the results barely support the realist-based arguments linking increased security threats to cyber capacity building. Only model 1 suggests a significant relationship between cyber incidents suffered and increased capacity, while in model 3 the prediction changes to a negative one and is not statistically significant. Moreover, a country's number of international rivals has no significant impact in any model. Cyber capacity building appears not to be driven by a state's

international strategic or threat environment therefore, which casts doubt on the ability for theories based on deterrence to explain cyber capacity efforts.

Domestic politics may have slightly more of an effect on cybersecurity capacity. Civil war is significant in models 1 and 2 where the results suggest surprisingly that increased civil conflict is linked to an increase in cyber capacity. One possible explanation for this is that countries with greater civil discord may be more eager to implement strong cybersecurity policies to crack down on domestic dissent. On the other hand, there is very little evidence that a country's regime type is linked either to higher or lower capacity, and both autocracies and democracies seem equally eager to develop their capacity.

Finally, while IGO membership and power status are associated with an increase in cyber capacity, they are not statistically significant, with the exception of IGO membership in model 1. There is little evidence that either IGO membership or a country's power status are driving states towards greater capacity building efforts.

New approach to cyber capacity building beyond IR Theory: the role of Scientific and Technical Knowledge

In contrast to deterrence-based logic as a potential driver of behaviour in the cyber domain (Nye 2017), this study instead sheds light on the role that the production of S&T knowledge has in explaining the unequal efforts in developing cyber capabilities worldwide. In other words, we argue that approaches to cybersecurity that are inspired by international security and military paradigms are not enough to explain countries' efforts in developing national cyber readiness.

Although this outcome might sound as a surprise, it is in line with a rich body of research addressing the key role of S&T knowledge in influencing national strategies in multiple key security dimensions of society across global north and global south including economic development and wealth (Tödtling, Lehner, and Trippl 2006). In the context of security studies, research has offered empirical evidence on the role that S&T knowledge has in ensuring the dominant military position of countries and their leading role in the field of innovation in the defence domain (Paarlberg 2004). With a specific focus on the global south, knowledge production is also seen as determinant to support resilience capacity of countries for disaster management (Gaillard and Mercer 2013). Moreover, although knowledge is increasingly transnational, research in the field also concludes

that the geographical proximity of authors of scientific and knowledge production is significant to the localization of their influence (Thompson and Fox-Kean 2005). In a broader context, there is also a general agreement about the impact that national S&T knowledge has on countries policy making capacity (Harry and Jones 2012). Traditionally, there is a tight complementary relation between scientific knowledge production and policy making processes. Although, its actual impact might vary depending on the different dimensions of the policy making process.

In the context of cyber capacity building, given that in this study S&T knowledge emerges to be the most robust finding, we explore further its impact on different dimensions of cyber capacity identified by the ITU by disaggregating its 2014 GCI scores and examining their correlation between S&T knowledge and these dimensions.[9] In particular, we are interested in understanding the more influential capacity of countries' S&T knowledge across the ITU identified 4 pillars of cyber capability: Legal, Technical, Organizational, and Capacity Building.

Table 5. Correlation between Scientific & Technical knowledge and GCI 2014 scores

Cybersecurity dimension	Correlation coefficient
Legal	0.618
Technical	0.557
Organizational	0.546
Capacity building	0.544
Cooperation	0.547

The production of Scientific and Technical journal articles evidently has the most significant effect on the legal aspect of a country's cybersecurity policy development with a correlation of 0.618 as shown in table 5. Access and availability of S&T knowledge may be the key factor why LDCs have lower cyber capacity than their Developed counterparts, given the evident existing gap in S&T knowledge production.

[9] In contrast, the ITU does not provide a disaggregated score for the 2017 GCI index

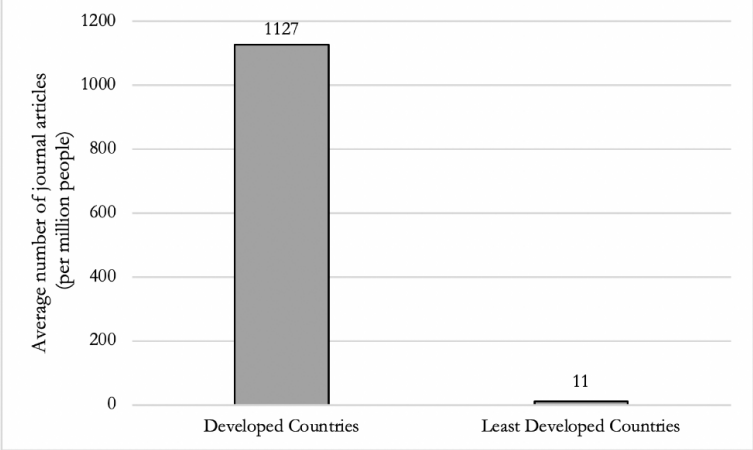

Figure 3 - Scientific and Technical journal articles (per million people) among Developed Countries and LDCs

In figure 3, we compare the average number of scientific and technical journal articles (in the year 2014) between the two groups of countries to illustrate the substantial divide in S&T knowledge production between them. Developed Countries publish on average 1127 journal articles per million people while the average amongst the LDCs is only 11. This research highlights that bridging this gap could support the global south in developing cyber capacity, more than any other factors.

Conclusion

Given the fast-changing nature of internet geography, this article has stressed the importance of defining a transnational governance approach to cybersecurity aiming at bridging the existing gaps across countries worldwide. In particular, we have highlighted how, given the transnational nature of connectivity infrastructure, it is becoming increasingly relevant to approach cybersecurity strategies beyond national borders. We have also provided evidence on how digital geography is fast changing, with the expectations that most internet users will be soon living in the global south. In this context, we have highlighted the emerging call to develop cybersecurity capacity in the global south in order to support local stakeholders to develop their technical and governance skills that would make newly connected countries benefitting from the technological development instead than been harmed from it. Moreover, given the emerging transnational governance approach to cybersecurity, cyber capacity building should also support the development of cyber diplomacy skills in international negotiations, in order to enable newly connected countries to play an active role in such fora. However, despite the various initiatives developed by an increasing number of international actors and countries' foreign policy offices, we have identified a lack of understanding of the driving factors explaining the different national cyber capacities.

To inform such approaches, we have sought identify the potential drivers of cybersecurity capacity globally through a quantitative analysis that is structured according to established international relations perspectives. We have helped to identify robust findings for the determinants of a country's level of cybersecurity preparedness by drawing on on three different measures of national cyber capacity. Interestingly, our research shows that measures based on international security paradigms are less relevant in explaining cyber capacity. We find little empirical evidence that a country's efforts to build capacity is influenced by its external threat environment as indicated by international rivals or cybersecurity incidents. Perspectives derived from domestic political or norms-based arguments have little relevance either. This suggests the need to develop different theoretical perspectives to understand cyber capacity building processes.

Our measure of S&T knowledge, however, is consistently a positive and significant predictor of cyber capacity across all three indices which gives us greater confidence of the importance of this type of resource in explaining cybersecurity variance between the global north and south. Our results suggest that Scientific and Technical knowledge development is of critical importance, above that of political incentives or pressures.

Given the relationship between scientific and technical journal articles and cyber capacity, it may be necessary for international actors and cybersecurity diplomats to focus on S&T knowledge as a means to boost cybersecurity readiness, especially in the global south which often lacks the resources to support education and training in this area to the same extent as countries in the global north.

The analysis also raises some issues about the appropriate method of measuring cyber capacity, given the variation in results according to different dedicated indices. Some variables, for instance, ICT industry, are statistically significant when using some cyber capacity indices but not for others. These differences are likely explained by variation in coding methodologies for cyber capacity indices. It necessitates further research to identify the most appropriate means of gauging cyber readiness. Our findings suggest technical expertise is essential for developing cyber capacity, but the next question is by what processes can states translate this asset into cybersecurity readiness. This can further inform policy decisions on how to build capacity in the global south.

References

Asghari, Hadi, Michael Ciere, and Michel J. G. van Eeten. 2015. "Post-Mortem of a Zombie: Conficker Cleanup After Six Years." Proceedings of the 24th USENIX Conference on Security Symposium,Washington, D.C., August 12–14, (2015), 1–16.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford: Oxford University Press.

Buzan, Barry, and Eric Herring. 1998. *The Arms Dynamic in World Politics*. Boulder, CO: Lynne Rienner.

Calderaro, Andrea. 2014. "Internet Politics Beyond the Digital Divide. A Comparative Perspective on Internet Politics across Political Systems." In *Social Media in Politics*, eds. Bogdan Pătruț and Monica Pătruţ. New York, NY: Springer International Publishing, 3–17.

———. 2015. *Internet Governance Capacity Building in Post-Authoritarian Contexts. Telecom Reform and Human Rights in Myanmar*. Rochester, NY: Social Science Research Network.

Carr, Madeline. 2016. "Public–Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92(1): 43–62.

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: The next Threat to National Security and What to Do about It*. New York, NY: Ecco.

Colaresi, Michael P., Karen Rasler, and William R. Thompson. 2008. *Strategic Rivalries in World Politics: Position, Space and Conflict Escalation*. Cambridge: Cambridge University Press.

Collier, Paul. 1999. "On the Economic Consequences of Civil War." *Oxford Economic Papers* 51(1): 168–83.

Council of the European Union. 2018. 15244/18 *Draft Council Conclusions on Cybersecurity Capability and Cyber Capacity Building in the EU*.

Craig, Anthony. 2018. "Understanding the Proliferation of Cyber Capabilities." *Council on Foreign Relations*. https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities (July 30, 2019).

Deibert, Ronald J. 2011. "Tracking the Emerging Arms Race in Cyberspace." *Bulletin of the Atomic Scientists* 67(1): 1–8.

———. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Steward.

Demchak, Chris C., and Peter Dombrowski. 2011. *Rise of a Cybered Westphalian Age*. Air Univ Maxwell Afb Al Strategic Studies Quarterly.

Dunn-Cavelty, Myriam. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. New York, NY: Routledge.

Dutton, William H. et al. 2017. *Cyber Security Capacity: Does It Matter?* Rochester, NY: Social Science Research Network. SSRN Scholarly Paper.

Early, Bryan R. 2014. "Exploring the Final Frontier: An Empirical Analysis of Global Civil Space Proliferation." *International Studies Quarterly* 58(1): 55–67.

Ebert, Hannes, and Tim Maurer. 2013. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34(6): 1054–74.

European Commission. 2018. "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building."

European Union Agency for Law Enforcement Cooperation. 2018. "Internet Organised Crime Threat Assessment (IOCTA).".

Feld, Werner J., Robert S. Jordan, and Leon Hurwitz. 1994. *International Organizations: A Comparative Approach*. 3rd Edition. Westport, Conn: Praeger Pub.

Finnemore, Martha, and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110(3): 425–79.

Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52(4): 887–917.

Frances Stewart, Cindy Huang, and Michael Wang. 2000. "Internal Wars In Developing Countries: An Empirical Overview of Economic and Social Consequences." In *War and Underdevelopment: Volume 1: The Economic and Social Consequences of Conflict*, eds. Frances Steward and Valpy Fitzgerald. Oxford: Oxford University Press.

Fuhrmann, Matthew, and Michael C. Horowitz. 2017. "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles." *International Organization* 71(2): 397–418.

Gaillard, J.C., and Jessica Mercer. 2013. "From Knowledge to Action: Bridging Gaps in Disaster Risk Reduction." *Progress in Human Geography* 37(1): 93–114.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38(2): 41–73.

Goertz, Gary, Paul F. (Paul Francis) Diehl, and Alexandru Balas. 2016. *The Puzzle of Peace : The Evolution of Peace in the International System*. Oxford: Oxford University Press.

Gurr, Ted Robert, Keith Jaggers, and Will H. Moore. 1990. "The Transformation of the Western State: The Growth of Democracy, Autocracy, and State Power Since 1800." *Studies In Comparative International Development* 25(1): 73–108.

Harry, Jones, and Nicola A. Jones. 2012. *Knowledge, Policy and Power in International Development: A Practical Guide*. Bristol, UK: Policy Press.

ISO. 2012. "ISO/IEC 27032:2012, 'Information Technology - Security Techniques - Guidelines for Cybersecurity.'".

Jervis, Robert. 1978. "Cooperation under the Security Dilemma." *World Politics* 30(2): 167–214.

Jo, Dong-Joon, and Erik Gartzke. 2007. "Determinants of Nuclear Weapons Proliferation." *Journal of Conflict Resolution* 51(1): 167–94.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press.

Kinsella, David. 2000. "Arms Production in the Third Tier: An Analysis of Opportunity and Willingness." *International Interactions* 26(3): 253–86.

Kleiner, Bart D., Paul J. Nicholas, and Kevin Sullivan. 2014. *Cyberspace 2025: Today's Decisions, Tomorrow's Terrain',*. Redmond, WA: Microsoft.

Kshetri, Nir. 2010. "Diffusion and Effects of Cyber-Crime in Developing Economies." *Third World Quarterly* 31(7): 1057–79.

Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10(1): 86–103.

Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35(3): 401–28.

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22(3): 365–404.

Makridis, Christos Andreas, and Max Smeets. 2019. "Determinants of Cyber Readiness." *Journal of Cyber Policy* 4(1): 72–89.

Maoz, Zeev, and Bruce Russett. 1993. "Normative and Structural Causes of Democratic Peace, 1946-1986." *The American Political Science Review* 87(3): 624–38.

Most, Benjamin A., and Harvey Starr. 1989. *Inquiry, Logic, and International Politics*. Columbia: University of South Carolina Press.

Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Cambridge, MA: Polity.

———. 2019. "Against Sovereignty in Cyberspace." *International Studies Review* 0: 1–23.

Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *Centre for International Governance Innovation / Chatham House*.

———. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41(3): 44–71.

OECD. 2015. *Digital Security Risk Management for Economic and Social Prosperity*. Paris: OECD Publications.

Paarlberg, Robert L. 2004. "Knowledge as Power: Science, Military Dominance, and U.S. Security." *International Security* 29(1): 122–51.

Pawlak, Patryk. 2016. "Capacity Building in Cyberspace as an Instrument of Foreign Policy." *Global Policy* 7(1): 83–92.

Pawlak, Patryk, and Panagiota-Nayia Barmpaliou. 2017. "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity." *Journal of Cyber Policy* 2(1): 123–44.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Rid, Thomas, and Peter McBurney. 2012. "Cyber-Weapons." *The RUSI Journal* 157(1): 6–13.

Rider, Toby J, Michael G Findley, and Paul F Diehl. 2011. "Just Part of the Game? Arms Races, Rivalry, and War." *Journal of Peace Research* 48(1): 85–100.

Sagan, Scott D. 1996. "Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb." *International Security* 21(3): 54–86.

Schia, Niels Nagelhus. 2018. "The Cyber Frontier and Digital Pitfalls in the Global South." *Third World Quarterly* 39(5): 821–37.

Scholte, Jan Aart. 2005. *Globalization: A Critical Introduction*. 2Rev Ed edition. New York, NY: Red Globe Press.

Singer, P. W, and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*.

Siverson, Randolph Martin, and Harvey Starr. 1991. *The Diffusion of War: A Study of Opportunity and Willingness*. Ann Arbor: University of Michigan Press.

Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41(3): 72–109.

Taddeo, Mariarosaria, and Luciano Floridi. 2018. "Regulate Artificial Intelligence to Avert Cyber Arms Race." *Nature* 556(7701): 296–98.

Thompson, Peter, and Melanie Fox-Kean. 2005. "Patent Citations and the Geography of Knowledge Spillovers: A Reassessment." *The American Economic Review* 95(1): 450–60.

Tödtling, Franz, Patrick Lehner, and Michaela Trippl. 2006. "Innovation in Knowledge Intensive Industries: The Nature and Geography of Knowledge Links." *European Planning Studies* 14(8): 1035–58.

United Nations. 2015. "Consensus Report from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security."

United Nations Statistics Division. 2019. "Standard Country and Area Codes Classifications (M49).".

Valeriano, Brandon, Benjamin Jensen, and Ryan C Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

Valeriano, Brandon, and Ryan C Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

Vasquez, John A. 2013. *The War Puzzle Revisited*. Cambridge: Cambridge University Press.

Wagner, Ben. 2013. "Governing Internet Expression: How Public and Private Regulation Shape Expression Governance." *Journal of Information Technology & Politics* 10(4): 389–403.

Waltz, Kenneth N. 1979. *Theory of International Politics*. Long Grove, Ill: Waveland Press.

Zürn, Michael. 2018. *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford: Oxford University Press.