Developing Digital Capacity: How and Why Foreign Assistance Shapes Institutions

Harry Oppenheimer,[1]

Last modified: February 8, 2021

Abstract

Internet and cybersecurity issues touch nearly every part of modern government. They are simultaneously security and cooperation issues relevant to militaries and foreign policy bureaucracies, regulatory issues important for technical bureaucrats, and economic issues relevant to development and commerce. This paper analyzes an original dataset built from a corpus of policy documents that map bureaucratic delegation and policy priorities for cybersecurity strategies across over 100 states since the year 2000. The cross-national patterns and evolution of policies demonstrate how developed states and transnational actors impact developing states' cybersecurity policies through networking with sub-state actors. I argue that under conditions of interdependence cybersecurity capacity is necessary to limit negative policy externalities, but assistance shapes institutions to increase the bureaucratic autonomy of technical institutions. This paper broadens our understanding of cybersecurity by demonstrating its importance beyond military uses and capabilities, and offers an important case where interdependence creates incentives to cooperate through state-building with targeted developmental assistance.

[1]PhD Candidate, Harvard University. 1737 Cambridge St, Cambridge MA 02138. Email: hoppenheimer@g.harvard.edu Web: https://scholar.harvard.edu/hoppenheimer.

1 Introduction

It is difficult to overstate the importance of the internet for modern governments and individuals. In 2018 in the United States, the internet sector contributed $2.1 trillion to GDP, created or supported 8.7% of total employment, and became the fourth largest sector in the U.S. economy.[2] 42% of Americans get their news through the internet,[3] 71% of them regularly use online banking, [4] and 28% of them say they are online almost constantly.[5] As a result, cybersecurity capacity - ensuring the safe storage, access, and transfer of digital data - has become a priority for government actors, and the transnational nature of the internet has created new incentives to diffuse that capacity.

While the empirical literature on cybersecurity focuses primarily on military applications, cyber threats affect all internet users and are relevant to a variety of government bureaucracies.[6] National telecommunications operators manage the digital infrastructure where these threats occur, financial and business interests rely on secure digital communications to run, internal security groups attempt to stop criminal efforts online, foreign affairs bureaucracies attempt to organize cooperation on digital issues, and military and national security groups try to protect nations from foreign threat. Over the past twenty years, most countries have develop doctrine and strategy that institutionalizes cybersecurity functions and expresses their understanding of the government's role in the digital space.

This process has been shaped by the involvement of external experts. Technical expertise is its own form of power in international relations (Adler and Haas, 1992; Haas, 1992). Many states that lack the capacity to develop strategy have engaged with external experts to educate themselves about cybersecurity issues. For instance, Trinidad and Tobago, hailed for being the first Caribbean state with a national cybersecurity strategy, did so with the direct assistance of the Organization of American States. A wide cross-section of actors has supported cybersecurity capacity by building on an evaluative framework developed in the United Kingdom. The includes the Republic of Korea, the Netherlands, the World Bank, the Organization of American States, International Telecommunication Union, the Commonwealth Telecommunications Organisation, NRD Cyber Security, the Norwegian Institute of International Affairs (NUPI), and the Oceania Cyber Security Centre (OCSC).

Despite fears of constant conflict in cyberspace these actors invested in capacity building. I argue that cybersecurity presents a challenge for interstate-relations — globally-integrated digital infrastructures

[2] https://internetassociation.org/publications/measuring-us-internet-sector-2019
[3] https://www.journalism.org/2020/07/30/americans-who-mainly-get-their-news-on-social-media-are-less-engaged-less-knowledgeab
[4] https://www.valuepenguin.com/banking/statistics-and-trends
[5] https://www.pewresearch.org/fact-tank/2019/07/25/americans-going-online-almost-constantly/
[6] The literature on cybersecurity and international affairs is growing rapidly. For recent research on the geopolitical implications of cybersecurity, see Borghard and Lonergan (2017); Buchanan (2017); Gartzke (2013); Kostyuk et al. (2018); Valeriano et al. (2018).

expose states to negative policy externalities and shared threat (Oppenheimer, 2020). Externalities create incentives to develop capacity in interdependent states (Bermeo, 2018). However, cybersecurity capacity is highly fluid between offensive and defensive capabilities (Slayton, 2016), and capacity plays a role in both regulatory and coercive means. In this paper, I argue that external engagement is not simply designed to increase cybersecurity capacity and organization, but is also designed to enforce the technical bureaucracies, resulting in autonomous policy-making that is most likely to emphasize the technical dimensions of the policy area (Carpenter, 2001).

I tests two mechanisms of policy diffusion - learning through security and economic partners and teaching through engagement with experts. Learning occurs as sovereign states interact in international forums and observe the policies of others. Teaching occurs when more knowledgeable actors directly engage in the policy-making process of states. States have developed cybersecurity strategy through both mechanisms. However, direct engagement with external experts exerts pressure on state institutions. I find that both engagement with outside experts and the policies of economic and security partners significantly increases policy adoption. However, engagement with external experts only affects adoption for policies owned by technical bureaucracies, while the policies of economic and security partners only affects adoption for policies owned by security and economic bureaucracies.

This paper continues as follows. First, it outlines the multitude of actors in the digital space and their interests therein. Afterward, it discusses two different ways of conceptualizing threats, and the range of viewpoints on cybersecurity and the importance of cybersecurity strategies in expressing a nation's positions on these issues. After explaining the incentives to build up capacity in developing states, it shows how external actors provide information to developing states on cybersecurity. Finally, this paper carries out two empirical tests. First, it leverages hazard models to determine whether policy adoption is more likely after external engagement with experts, and if this is driven primarily by adoption from independent ICT bureaucracies or independent bureaucracies focused on security issues. The paper then demonstrates how policies adopted by independent technical bureaucracies are more likely to emphasize the non-coercive aspects of cyber capacity.

2 Interests in the Digital Space

Since the internet is an information exchange system it can be leveraged for many purposes and faces a multitude of security threats. The process of securing this system relies on two main security concepts, information security and cybersecurity, which are both grounded in the security properties of confidentiality, integrity, and availability. Confidentiality ensures only authorized individuals can view certain information,

integrity ensures that information is not altered, and availability ensures that we can get information when we need it. Information security is an older concept concerned primarily with the individual actors within the system, confidentiality, and protecting private information from being stolen. Cybersecurity is more concerned with the internet architecture, and therefore places more emphasis on integrity and availability (Nieles et al., 2017; Wamala, 2011).

A cyberattack is an attempt, through digital infrastructure, to access, steal, or corrupt information. Different flavors of attacks are also associated with different security principles. A zero-day exploit of a security flaw is used to break confidentiality, and can be used to affect integrity and availability. A distributed denial-of-service attack is used to affect the availability of information. Any individual or organization that uses ICTs can be targeted via ICTs. The extent of that damage depends on what they are relying on ICTs for, and the implications of them losing access, confidentiality, or integrity of that information. Related, one can imagine that an attack designed to destroy information would have different implications from one which was designed to simply deny access to information.

By understanding the technical characteristics of cybersecurity can we move forward to understand which applications have been studied and which have been overlooked. Cyberwarfare is a specific application of cyber capabilities to damage another organization's information networks. Cyber espionage is the use of cyber tools to obtain secrets without the owner's permission. Economic espionage targets is a corporation, military espionage targets the military, or political parties, or intelligence agencies, and so on. Actors use cyberspace to threaten systems because they value the information they can gain, deny access to, or destroy. Organized crime can sell information or use it to extract rents. Hacktivists organizations can expose information to a broad public. Intelligence services can gain insights into adversaries. Governments can use cyberattacks to disrupt adversaries, control their populations, or impose costs on firms. Corporations can steal information from competitors.

Governments can assert control over the internet to identify criminals, ensure data standards, or shut down malicious sites and malware hosts. Such policies resulted in less internet freedom such as in North Korea (where there is no access to the internet) and China (where sections of the internet are blocked). Countries pass legislation to provide a regulatory and legal framework for dealing with cybersecurity issues. This can impact how data is stored, how consumers are informed about breaches, or what defines sensitive information and how it can be accessed or used.[7] Criminal laws in different jurisdictions define what a computer crime is and how individuals can be punished.[8] They can create mechanisms for organizations to

[7] For example see California Security Breach Information Act (SB-1386), European Union General Data Protection Regulation (GDPR), U.K. Data Protection Act

[8] For example see U.S. Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030 (as amended), U.S. Economic Espionage Act of 1996, The Computer Misuse Act 1990 (U.K.)

report cyber attacks and thefts, and levy fines on groups that do not protect data. These approaches are outlined the publicized through national cybersecurity strategies and doctrines.

Bureaucracies have significant incentives to gain control over the cybersecurity policy portfolio. Global Spending on information technology will reach $3.9 trillion in 2020,[9] and global spending on cybersecurity is expected to reacy $170 billion by 2022.[10] The United States Department of Homeland Security, which is responsible for cybersecurity in the public sector, received $1.9 billion in cybersecurity funding for FY2020.[11] The United Kingdom National Cyber Security Centre was allocated £1.3 billion to carry out the UK National Cybersecurity Strategy.[12] Botswana's 2019 *National Cybersecurity Strategy* proposed spending 0.3% of the annual government budget to enact its recommendations and create a national CERT. The World Economic Forum *Global Risks Report 2019*, which surveyed nearly 1,000 decision-makers, listed cyberattacks resulting in the disruption of operations and infrastructure as more likely than a water crisis and more impactful than the spread of infectious diseases.[13]

There has been no "one size fits all" model of bureaucratic delegation in cyberspace. Varying institutions have been delegated the cybersecurity portfolio across different national contexts. Public Safety Canada publishes the Canadian national cybersecurity strategy, the Ministry of Finance published a Danish cybersecurity strategy, and the Communications Ministry publishes the Ghanaian cybersecurity strategy. The Netherlands and United States have cybersecurity strategies independently developed by their defense bureaucracy. This paper seeks to understand when countries delegate cybersecurity to different bureaucracies, and how ownership over the cybersecurity issue area results in policies that reflect distinct understandings of the underlying issues?

3 Models of Cyber Threat

Authors discuss cybersecurity threats primarily as a tool of national power. States can use cyber tools to coerce one another and increase their power. This class of cyber threats are highly specific and targeted. However, the broader set of cybersecurity threats affect millions of computer users and are designed to be as non-specific as possible.

Model 1: Threat Due to Coercive Capacity

States seeking to maximize their security in an anarchic world will invest in capabilities that allow them to ensure their survival and increase their power (Waltz, 1979). In cyberspace these capabilities are very

[9] https://www.gartner.com/en/newsroom/press-releases/2020-01-15-gartner-says-global-it-spending-to-reach-3point9-trillion-in-
[10] https://www.gartner.com/document/3889055
[11] https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf
[12] https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf
[13] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

specific and typically target military systems of adversaries. An example of such attack would be Stuxnet, which was designed to deliver a payload to a Siemens SCADA system using four zero-day exploits and was designed to be inert after a specific date and spread from one system to no more than three others. If the program detected a specific input known to be used on Iranian centrifuges it interfered with the signal to overhead the system.

The existing literature on cybersecurity focuses almost exclusively on this subset - military applications of cyber capabilities. For example, whether cyberspace is a new field for conflict between nations, or if it fails to live up to its kinetic counterparts (Arquilla and Ronfeldt, 1993; Clarke and Knake, 2012; Dogrul et al., 2011; Farwell and Rohozinski, 2011; Gartzke, 2013; Lindsay, 2013; Rid, 2013; Valeriano and Maness, 2015). How states deter the use of cyber weapons, or leverage cyberspace to coerce one another (Borghard and Lonergan, 2017; Goodman, 2010; Iasiello, 2014; Libicki, 2009; Sharma, 2010; Valeriano et al., 2018). Is cyberspace a domain where escalation is especially likely, and is this related to its offense-defense characteristics (Buchanan, 2017; Kostyuk et al., 2018; Libicki, 2012; Lin, 2012; Slayton, 2016)? However, it is not clear from this research how, or even whether, cybersecurity is relevant outside of the military context.

Model 2: Threat Due to a Lack of Capacity and Cooperation

State and non-state actors have incentives to increase their welfare, and therefore seek to enact policies and strategies necessary to ensure the safe exchange of information under threat by 30 million cyberattacks per year. The internet has become a vital part of the market infrastructure in both developed and developing economies, effecting wages (Krueger, 1993; Acemoglu and Autor, 2010; Benavente et al., 2011), growth (Thompson and Garbacz, 2007; Choi and Hoon Yi, 2009), skills gaps (Guillén and Suárez, 2005; van Deursen and van Dijk, 2011), trade (Freund and Weinhold, 2002; Choi, 2010), and poverty (Norris, 2001; Kenny, 2002). The internet economy was worth $4.2 trillion to the G20 economies alone, and in the U.S. two-thirds of jobs require some digital skills (Fefer et al., 2019).

Often, an organization's security relies on its ability to get others to adopt and enforce laws and policies that act in their interests. Oppenheimer (2020) demonstrates how transnational integration of digital infrastructures leads to increases in negative policy externalities among digital neighbors. The ILOVEYOU virus demonstrates the ramifications of legal loopholes in different jurisdictions. The alleged creator of the crime was a 24-year-old college dropout from the Philippines named Onel A. de Guzman. The individual was caught and arrested soon after the attack was traced to his apartment complex. However, there were no laws outlawing writing malware in the Philippines at the time and de Guzman was released without charges after writing one of the most destructive and expensive programs in history.

4 Cyber and Information Security Doctrines

What do states think about cybersecurity? While there is some existing research on the range of viewpoints on cybersecurity issues, there is limited understanding of where countries fall within that range. Arguments usually characterize a US-China axis of cybersecurity understanding. Farrell (2015) argues that, "the United States defined its preferred cyberspace norms as internet openness, security, liberty, free speech, and with minimal government oversight and surveillance in its 2011 International Strategy for Cyberspace." The document itself states, "while offline challenges of crime and aggression have made their way to the digital world, we will confront them consistent with the principles we hold dear: free speech and association, privacy, and the free flow of information" ([The White House], 2011).

China's cybersecurity doctrine draws on two distinct concepts - cyber sovereignty and critical information infrastructure (CII). Historically China has been reluctant to specifically defined what counts as "critical information infrastructure" or how it this different from the American "critical infrastructure." However, operators of CII have to follow specific security procedures, store certain amounts of their data within China, and go through a security review when purchasing network equipment (Triolo et al., 2017). In 2017 they provided more detail to CII as, "public communication and information services, power, traffic, water resources, finance, public service, and e-government" (Wagner, 2017).

In March 2017, China released its own cybersecurity norms document in English and Chinese, titled *International Strategy of Cooperation on Cyberspace*. The document contains four chapters, including ones titled "Basic Principles," "Strategic Goals," and "Plan of Action." Sovereignty again plays a significant role in the principles section, stating "countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing." The strategy chapter also contains the headline "safeguarding sovereignty and security".

International organizations have produced policy templates which emphasize many different issue areas. The International Telecommunications Union lists "defense of homeland," "economic well-being," "favourable world order," and "promotion of values" as the strategic considerations for cybersecurity strategy (Wamala, 2011, p. 40). The guide lists legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation as the five priorities of any cybersecurity strategy and national program (p. 8-9). The Commonwealth also produced a national strategy guide, emphasizing economic development, cybercrime, human rights, raising awareness, and developing national and international partnerships ([Commonwealth Technology Organisation], 2015, p. 10-11) Guidelines produced by NATO lists critical infrastructure protection, education, organizational measures, and international obliga-

tions among the lines of action for cybersecurity strategies (Osula and Kaska, 2013, p. 3). Cybersecurity strategies touch on issue areas across government, and emphasize norms that speak to the core of internet issues in the 21st century.

Publishing a cybersecurity strategy often serves as a new benchmark for state views about the internet and society. After publishing a new strategy in 2020, the Australian Home Affairs minister was criticized as "drab and inward-looking" and "vague and unambitious."[14] The EU's 2013 cybersecurity strategy was criticized for failing to provide enough protection for personal data.[15] The United States 2018 strategy signaled a change to a new posture to address online threat, which some viewed as inviting threats rather than deterring them.[16] At the same time, lacking a cybersecurity strategy is viewed as a national issue and a barrier to government coordination.[17]

5 Cyber Capacity Building

5.1 Benefits of Capacity Building

The policy diffusion literature assumes that states have the capacity to enact policy, but in cyberspace many countries require assistance to develop their cybersecurity capacity and publish strategy. Donors can engage in targeted development as an efficient strategy in an increasingly globalized world (Bermeo, 2018). It is not always clear whether the donor's intentions are based on recipient need or strategic considerations (Alesina and Dollar, 2000; Easterly and Pfutze, 2008; Easterly and Williamson, 2011). However, in cyberspace the need-based and strategic-based considerations are linked. In cyberspace, capacity is necessary to minimize the likelihood that the internet users in one country will become a risk source for the existing internet users.

Policy externalities are central to theories of cooperation and conflict within international relations, especially in a world of increasing interdependence (Keohane and Nye, 1973; Keohane, 1982; Raustiala, 2002; Slaughter, 2003). While powerful states may weaponize interdependence (Farrell and Newman, 2019), internet integration also has the potential to expose countries to threats from others. However, assisting states develop the ability to manage individuals is valuable since negative policy externalities can result from transnational gaps in enforcement. States must have both the ability and willingness to ensure cybersecurity standards and regulations limit the spread of digital threats to adjacent countries.

There are multiple benefits for developing states to accept assistance in cybersecurity capacity building. They may seek part of the estimated $800 billion in global digital trade, and perceive the capacity frameworks

[14] https://www.zdnet.com/article/the-disappointment-of-australias-new-cybersecurity-strategy/
[15] https://nakedsecurity.sophos.com/2013/06/19/eus-cybersecurity-strategy-gets-harsh-criticism-from-data-protection-advocate/
[16] https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html
[17] https://www.thenewsminute.com/article/why-india-needs-national-cybersecurity-strategy-130815, https://www.orben.com/en/reasons-why-mexico-needs-a-national-cybersecurity-agency/

pushed by wealthy states and private corporations as appropriate (Meyer et al., 1997). Since these frameworks are pushed by the most technologically sophisticated states, they may also perceive the advice as the "best" policy (Haveman, 1993; McNamara, 1998). Individual bureaucrats within these governments may benefit if they believe they will be able to own the issue area when doctrine is developed.

5.2 Risks of Capacity Building

All this might lead us to think of cybersecurity capacity assistance as cost-less for technically capable actors. If capacity helps to limit negative externalities, why attempt to shape capacity development in any particular way? The dual-use nature of the cybersecurity regulatory capacity means that states gain the technical ability to harm others. The same capabilities that make a state an effective regulator can be used to develop offensive cyber capabilities and limit the freedom of the web because the same expertise is required for both. Development actors often lack the ability to enforce rules once the aid has been given. The literature details how foreign aid can lead to corruption, rent-seeking, and weakening political institutions and rights protection instead of improving governance (de Mesquita and Smith, 2009; Burnside and Dollar, 2000; Morrison, 2007; Remmer, 2004).

Slayton (2016) argues that "skills are particularly important (in cyberspace) because cyberweapons, unlike physical weapons, are readily defeated once they are revealed as weapons" (p. 86). Alan Paller, the founder of SANS Institute,[18] states that in cyberspace " the skills are the weapon."[19] Most sophisticated cyber weapons, especially weapons designed to target one specific system, can only be used once (Gartzke, 2013). Creating a new weapon requires a skilled programmer writing new code or altering an existing program. These skills are diffused across society, although states may be the most sophisticated actors writing these programs. Computer skills are also not differentiable in the same way that nuclear fission expertise is, but to regulate cyberspace and ensure cybersecurity the government needs the underlying expertise (Drew and Shane, 2013; Lu, 2015; Schulze, 2018).

Who do external actors desire to have the cybersecurity portfolio? I argue that outside actors desire technical bodies free from political or military influence, which increases the cost of weaponizing the internet and widens the information gap between the political and technical sides. As a result of developing ICT capacity, the donor will enforce the independence of technical bureaucracies to limit the opportunities of the government to interfere in ICT regulation for political or military ends. Bureaucrats in these governments benefit because they gain specialized knowledge to control and maintain a valuable policy portfolio. Within American politics, Carpenter (2001) demonstrated how bureaucrats network to increase their autonomy and

[18] SANS Institute is one of the world's largest ICT security training companies, and contracts for the U.S. Department of Defense

[19] Mulrine (2013)

form policy independently from elected officials, here I study a similar phenomena.

Due to the technical nature of the policy area, countries may delegate policy-making to bureaucracies with more specialized knowledge. However, this paper hypothesizes that, in developing states, bureaucracies which network with external actors will be more likely to develop policy autonomously. So, do states that engage with outside develop cybersecurity strategy within distinct bureaucracies, and do these types of institutions emphasize the technical side of cybersecurity capacity?

5.3 Investment in Capacity Building

Who invests in cybersecurity capacity building assistance? The Global Centre for Cyber Security and Capacity Building is an organization with a unique hybrid mission. It is housed at the University of Oxford, but its primary funding source is the United Kingdom Foreign & Commonwealth Office. According to the organization's mission statement "We are working with a wide range of global partners, including governments, international organisations and the private sector. The Centre will ensure that [cyber state capacity] becomes a global resource"[20]. The Foreign Secretary William Hague stated while announcing funding for the GCSCC,

> The new Global Centre for Cyber Security and Capacity Building in Oxford University's Martin School will coordinate global work on cyber threats and cyber policies which will help protect the UK's security. We are dedicating £500,000 per year to this centre to be a beacon of expertise and put the UK at the forefront of cyber policy development.[21]

Martin Borrett, the Director of the IBM Institute for Advanced Security Europe stated the "initiative is an exceptionally timely and important contribution to the activities of the global community seeking to secure cyberspace. The IBM Institute for Advanced Security Europe and our international operations look forward to working with Oxford and their partners to ensure a safe and sustainable cyberspace for all." This was followed up with headlines such as "Industry applauds new Oxford Cyber Security Centre."[22]

Since 2014, 57 countries have gained cybersecurity assistance through the capacity review process designed by the University of Oxford Global Cybersecurity Capacity Centre. A myriad of different actors adopt the Oxford model for cybersecurity capacity evaluation, including the World Bank, the Organization of American States, International Telecommunication Union, the Commonwealth Telecommunications Organisation, NRD Cyber Security, the Norwegian Institute of International Affairs (NUPI), and the Oceania Cyber Security Centre (OCSC).

[20] https://www.oxfordmartin.ox.ac.uk/cybersecurity/
[21] https://www.gov.uk/government/news/oxford-will-host-cyber-security-capacity-building-centre
[22] https://www.itproportal.com/2013/04/11/industry-applauds-new-oxford-cyber-security-centre/

Each engagement is carried out with an in-country partner that hosts the outside agency to conduct the review. For instance, the 2016 review in Senegal was undertaken by the invitation of the Ministry of Post and Telecommunications. The group was funded "through collaboration with the Dutch Government under the auspices of the Global Forum on Cyber Expertise" and undertaken by the GCSCC. Over three days the group met with stakeholders from across the government, including the armed forces and economic agencies of the government. After meeting with these stakeholders, the group authored the report which was then delivered to the government. The Senegalese government, which owned the report, then released it to the public.

The report's four authors were research fellows associated with Oxford with experience in government cybersecurity policy. One of these authors subsequently worked for the U.S. Office of Management and Budget, where he managed cybersecurity policy. Another left Oxford to become the head of digital standards at the U.K. Department of Digital, Culture, Media and Sport. A third continues to work as a consultant for cybersecurity policy, and the fourth works as a professor.

These reviews often lead directly to policy development and institutional changes in target countries. In November 2017, Senegal published a detailed national cybersecurity strategy with many similarities to documents published by GCSCC. According to GCSCC, "The recommendations that were provided with the review report allow the Senegalese government to prioritize the areas of capacity in which Senegal could invest strategically."[23] The document itself was published through the Ministry of Communication, Telecommunications, Posts and the Digital Economy, which also invited the cybersecurity strategy. Furthermore, document metadata reveals that the strategy was drafted by Fargani Tambeayuk, a program officer at the Commonwealth Technology Organisation, which works closely with the GCSCC and is also funded by the United Kingdom.

Appendix Table 3 contains the reviews which occurred in person along with the institution that carried out the review and any additional information regarding the review funding source. Each review is confidential for the contracting state, although several of these organizations encourage partner states to publish the results of the reviews.

Of the 59 countries that gained outside assistance in the form of a capacity review, 21 had already published a cybersecurity policy or strategy. Of those 21, Albania, Columbia, Lithuania, and Montenegro published new strategies after the review process. Overall, 21 countries published new cybersecurity documents after the review process. The group that invited and hosted the cybersecurity review was re-

[23] https://www.thegfce.com/initiatives/p/progressing-cybersecurity-in-senegal-and-west-africa

sponsible for publishing the eventual national cybersecurity strategy in Gambia,[24] Macedonia,[25] Senegal,[26] Sierra Leone,[27] and Brazil.[28] The host organization was also involved in the doctrine drafting process in Kyrgyzstan.[29] The host institution in Montenegro was later dissolved, but the policy area was delegated to an independent bureaucracy responsibility for public sector reform. Three countries - Albania, Armenia, and Thailand - did not own or co-develop the cybersecurity strategy that their country eventually published.

Of the 8 countries with no public information regarding the host organization, several recognized the influence of international experts in developing policy or developed policy using technical bureaucracies. The Colombian national digital security policy recognized the assistance of the OAS, which carried out the previous cybersecurity capacity review.[30] The Minister of Information, Communciations Technology and Civic Education in Malawi announced that the Commonwealth, which carried out its cybersecurity capacity review, assisted with their strategy.[31]

Cybersecurity capacity reviews often become a cornerstone of cybersecurity strategies. Gambia's cybersecurity capacity review was carried out in late 2018 by the GCSC in collaboration with the World Bank. It was undertaken at the invitation of the Ministry of Information and Communication Infrastructure (MOICI) of Gambia. The 2020 *Gambia National Cyber Security Policy, Strategies and Action Plan* states that it leveraged "recommendations advanced by the Cybersecurity Capacity Review the Gambia Maturity Model (CMM) framework undertaken by Oxford University" (p. 11) and that "'The National Cyber Security strategy is a product of consultations and workshops conducted by MOICI-PURA in collaboration with different consultants (Bird & Bird – Civipol and Expertise France, cybersecurity maturity assessment by CMM Oxford)." (p. 25). Brazil, which received a capacity review in 2018, lists the cybersecurity maturity model as part of the methodology for its 2020 national cybersecurity strategy.

A more extreme version of this occurred in Bermuda. In March 2018, the Commonwealth Telecommunications Organisation (CTO) carried out a cybersecurity capacity review in Bermuda, hosted by the Department of ICT Policy & Innovation. The review has its own section in the *Bermuda Cybersecurity Strategy 2018-2022*, which was published only five months after the engagement. It outlined each of the rec-

[24] The Ministry of Information and Communication Infrastructure
[25] The Ministry of Information Society and Administration
[26] Ministry of Post and Telecommunications
[27] Ministry of Information and Communications
[28] Office of Institutional Security of the Presidency of the Republic of Brazil
[29] Drafted by the State Committee on Information Technology and Communications in cooperation with the Security Council. https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2018/12/31/feature-01#:~:text=Technology-,Kyrgyzstan's%20new%20cybersecurity%20strategy%20aims%20to%20protect%20state%2C%20personal%20data,from%20hackers%20and%20cyber%20espionage.
[30] The team of high-level experts included the participation of members of the ministries that make up the commission, colCERT, CCOC, CCP, cybernetic units of the Military Forces, and the public and private sector. The international team had the support of the OAS, and was attended by experts from the governments of Canada, Spain, the United States, Estonia, South Korea, Israel, the United Kingdom, the Dominican Republic and Uruguay, as well as members of the Forum Economic World, the OECD, the Council of Europe and INTERPOL.
[31] https://www.dataguidance.com/news/malawi-ict-minister-announces-development-national-cybersecurity-strategy

ommendations that the review made for Bermuda. While the Minister of National Security was responsible for the strategy, he revealed in a Ministerial Statement to Parliament that the Ministry of ICT Policy & Innovation was drafting the strategy independently with assistance from the CTO.[32]

Wealthy governments, including the United Kingdom, Finland, South Korea, Japan, Australia, and the United States, have invested in cybersecurity capacity building projects through the framework developed by Oxford University. These engagements are carried out directly in recipient countries with experts linked with these wealthy countries, and these engagements often become a integral part of cybersecurity doctrine. Is this a general rule - that cybersecurity assistance promotes policy diffusion, and does this exert pressure on institutionalization?

6 Hypotheses and Mechanisms

This paper focuses on learning in two forms - through observation of communication in international forums, and through direct engagement with outside experts. The chief argument of this paper is that direct engagement in the policy process exerts pressure on institutionalization and leads to greater technical bureaucratic independence.

The policy diffusion literature proposes that the availability of information regarding diffusion can be a significant driver of policy adoption (Rogers, 2003; Axelrod, 1997). Actors learn or are convinced about the value of adopting practices through information networks such as international institutions (Haas, 1992; Johnston, 2008). I hypothesize that STRATEGY ADOPTION BY PTA MEMBERS or STRATEGY ADOPTION BY EIA MEMBERS may provide information to countries regarding the importance of national cybersecurity strategy. Within the security realm, STRATEGY ADOPTION BY SECURITY AGREEMENT PARTIES may provide information through a distinct channel from economic agreements.

Information exchange mechanisms provide new information to actors, but outside institutions themselves may provide assistance in developing and shaping strategy. These are distinct mechanisms. In the first mechanism, actors learn about policies through interacting outside of the national policy process. When considering alternative ways to address health issues, states could learn about the optimal policy through the World Health Organization. In the second mechanism, actors learn about policies by inviting external actors into the national policy process. In health issues, a country might invite the World Health Organization to conduct an analysis of their national health system and recommend a new practice or policy. This variable, CYBER REVIEW, or engagement with outside technical experts, may explain why some countries adopt strategies and not others.

[32] http://parliament.bm/admin/uploads/ministerials/b193941dfc7f95d419973111e16448c1.pdf

The policy diffusion literature usually assumes that all strategies are created the same, and that, even if they are not the same, they were developed independently without *direct* involvement with outside actors. Part of the goal of this paper is to demonstrate that not all strategies are created the same, that this matters for the content of the policy, and that this is related to engagement with the larger epistemic community.

Alternative explanations in this paper include demand and supply factors. First is DOMESTIC DEMAND FOR CYBERSECURITY STRATEGY, measured by the proportion of a country's population with access to the internet. All else equal, countries with more individuals using the internet will benefit more from adopting policies to secure the exchange of data. This data is provided by the World Bank.

That said, there may be barriers to creating policies. For instance, if a country lacks sufficient domestic technical expertise they may not be able to develop a national level strategy even if the benefits for doing so are significant. Domestic expertise may explain why some countries develop cybersecurity doctrines sooner than others. I measure the DOMESTIC SUPPLY OF CYBERSECURITY EXPERTISE through the number of individuals with a professional cybersecurity certification per capita. I use the Certified Information Systems Security Professional (CISSP) certification, which has existed since 2004. I consider the main cybersecurity professional certification, the Certified Information Systems Security Professional (CISSP) which is administered by the International Information System Security Certification Consortium (known as $(ISC)^2$). The organization publishes contemporary data regarding the number of members by country, and I leverage the internet archive to view previously cached versions of the data for 2006, 2007, and 2012 through 2020.

The idea that states adopt new practices in response to their security environment is at the center of state-building theories (Tilly, 1985). States must modernize in response to external threat or risk being conquered or overthrown. Cyberspace represents a new area of conflict, and reliance on digital systems increases a country's exposure to the potential destructive threats from cyberspace (Craig and Valeriano, 2016; Rid and Buchanan, 2015). If cybersecurity strategies are thought of as an extension of traditional security policy, the PRESENCE OF EXTERNAL THREAT in the form of rivals states should increase the likelihood of adopting strategy.

While states may adopt strategies for a myriad of reasons, the central argument for this paper is that *who* develops strategy is as important as whether a strategy is developed at all, and this may be shaped by external engagement in the policy process. Each of the previous hypotheses concerns the incentives to develop strategy, but not whether the strategy should be developed in one part of the bureaucracy or another. Do the same explanations that hold for doctrine development hold equally for all actors, or does doctrine diffusion differ by the type of bureaucracy that controls the issue area? Later, this paper addresses the significance of issue ownership in cyberspace - doctrines produced by different bureaucracies represent

distinct viewpoints.

For each of the hypotheses in this paper, strategy adoption by different bureaucracies may be explained by different information channels. For instance, STRATEGY ADOPTION BY SECURITY AGREEMENT PARTIES or PRESENCE OF EXTERNAL THREAT may only explain strategy adoption by bureaucracies such as ministries of defense or justice, but not technical ones such as ICTs and communications. Alternatively, DOMESTIC DEMAND FOR CYBERSECURITY STRATEGY could explain adoption by technical bodies, but not others. The main argument of this paper is that ENGAGEMENT WITH OUTSIDE TECHNICAL EXPERTS, which themselves have an interest in promoting bureaucratic autonomy of technical institutions, should only explain policy adoption among technical bureaucracies.

7 Data

7.1 Dependent Variable: Cybersecurity Strategy and Doctrine

The main source for data is a corpus of all national cybersecurity strategy documents. This corpus was collected by combining resources from the Center for Strategic and International Studies (CSIS),[33] International Telecommunications Union,[34] Universita' Roma,[35] and the NATO Cooperative Cyber Defence Centre of Excellence.[36] This corpus includes documents that explicitly deal with cybersecurity or "information security." This excludes documents that have a cybersecurity component but are not cybersecurity focused, such as national security strategies[37] or ICT strategies[38] with statements about cybersecurity, but do not focus on cybersecurity.

This corpus includes national-level cybersecurity strategy or policy documents for 109 different nations or territories. Some non-sovereign territories have developed separate cybersecurity strategies such as Jersey (2017), Guernsey (2017), and the Isle of Man (2018) within the United Kingdom. I include all of these documents and collect separate control variable data for non-sovereign territories. These territories have their own Top-Level Domain (TLD), are allocated IP-address blocks, and have cybersecurity regulatory institutions.[39]

[33] https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index

[34] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

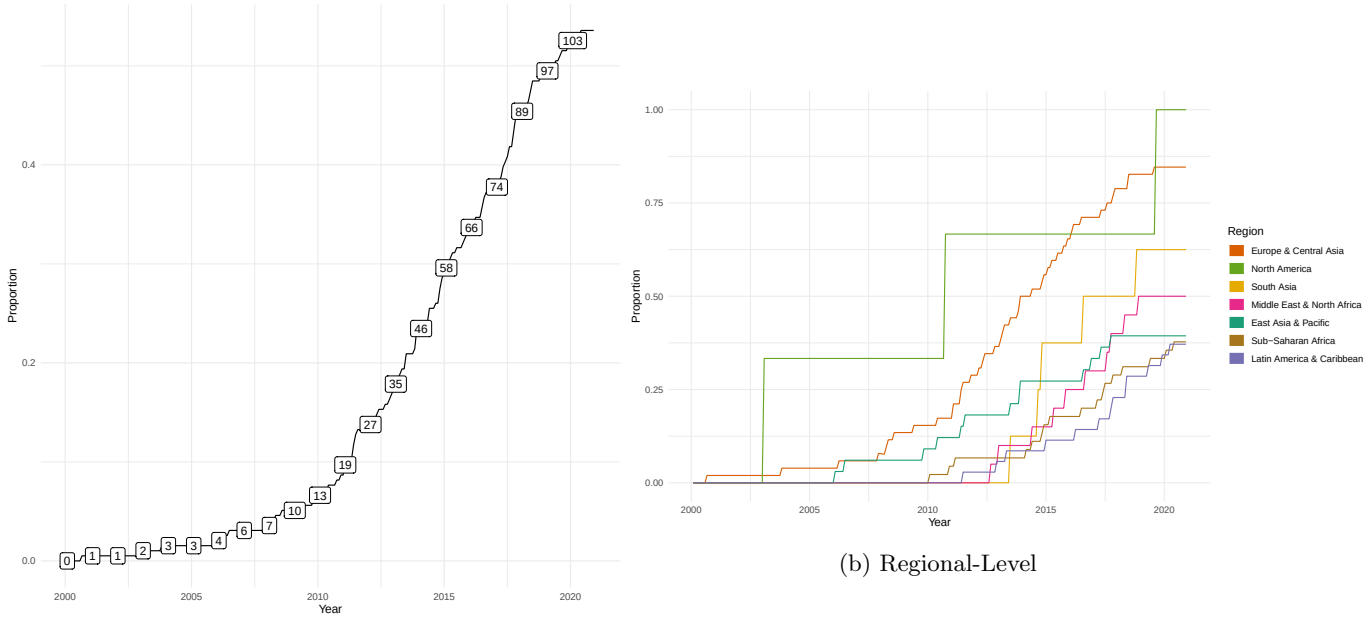
[35] http://www.sicurezzacibernetica.it/en/db_int_ncss.php

[36] https://ccdcoe.org/research/incyder/

[37] Roughly forty countries have military or national security strategies that mention cybersecurity

[38] For instance, Brazil's 2013 "Information Technology Strategy", Ethiopia's 2009 "National ICT Policy and Strategy", or Rwanda's 2010 "National ICT Strategy and Plan".

[39] There is a long-standing debate between technological determinists and sociological construction of technology proponents regarding the relationship between technology and society. This case may demonstrate a case of technological determinism, as territories with limited sovereignty deepen their state institutions as a result of technological pressures. While Guernsey may not fit in traditional international relations frameworks, it is home to thousands of computers and is networked into the international internet backbone.



(a) Global-Level

(b) Regional-Level

Figure 1: Proportion of Countries with Cybersecurity Doctrine or Policy

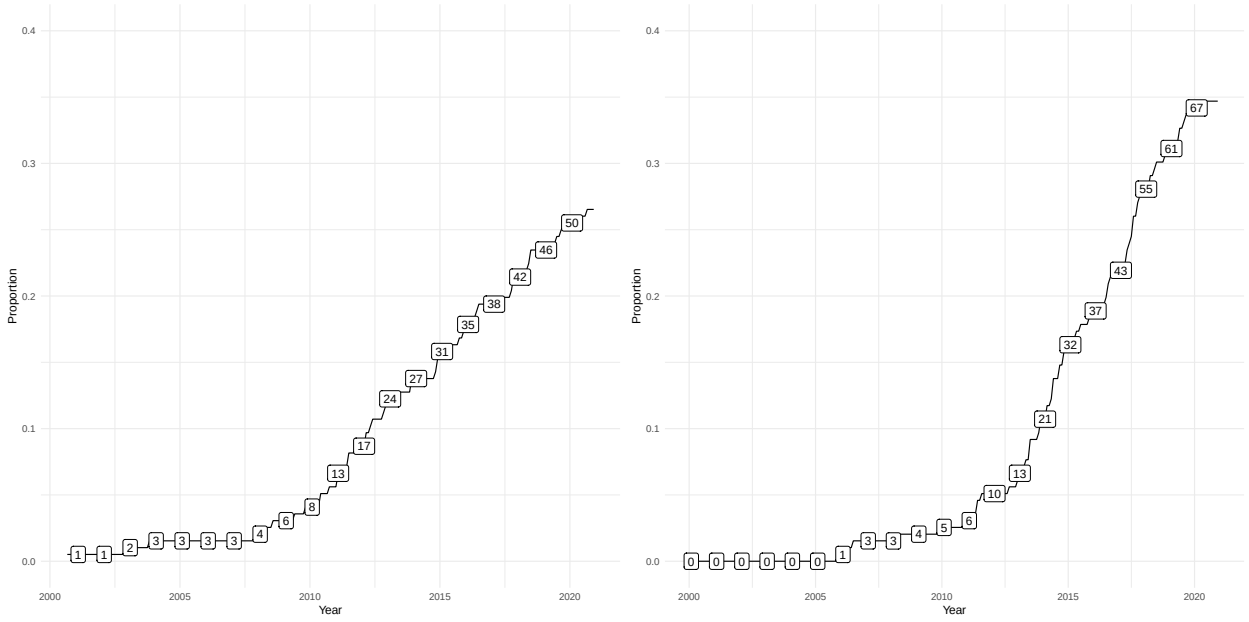
In total there are 185 separate documents. I include all documents that are national-level plans regarding the confidentiality, integrity, or availability of data exchange within and across the country's borders. This includes national cybersecurity strategies, cybersecurity plans and masterplans, information security strategies, cyber defense strategies, and international cyber strategies. This analysis does not include action plans, which often accompany strategy documents and outline the steps to achieve the plans.

Figure 1a presents the proportion of countries with a national cybersecurity document, and1b presents this as a proportion by region.[40] The first strategy was the *Information Security Doctrine of the Russian Federation*, published in 2000. As of 2020, 45% of countries or territories (104 of 233) have cybersecurity documents. The global trend follows the traditional "S-curve" of norm diffusion that is prevalent in the constructivist literature on diffusion (Finnemore and Sikkink, 2001). The proportion is the highest in North America and Europe, and lowest in Latin America and the Caribbean. The "S-curve" shape appears to be driven primarily by adoption in Europe & Central Asia, and the Middle East & North Africa. Policy adoption has occurred more linearly in the other regions.

For each document I code the type of organization that developed the document. These broadly fall into technical bureaucracies,[41] internal security bureaucracies,[42] external security bureaucracies,[43] foreign affairs bureaucracies, and multi-bureaucratic coalitions. I also code for whether the document was created solely

[40] Region is taken from the World Bank.
[41] For instance, Computer Emergency Response Teams, Ministries of Communication and ICTs, standards bodies
[42] For instance, Ministries of Justice, Homeland Security, Home Affairs, Interior
[43] For instance, Intelligence agencies, Ministries of Defense, National Security Councils

by a single bureaucracy, or if one bureaucracy held primary responsibility for the policy but cooperated with others to draft the document. For the analysis I exclude multi-bureaucratic coalitions and consider strategies developed by either technical bureaucracies or non-technical bureaucracies. One country can have different authors for documents at different times. For instance, Denmark's 2014 information security strategy was created by an intergovernmental group headed by the Ministry of Defense, while its 2018 document was created by the Ministry of Finance.



(a) Non-technical Bureaucracy

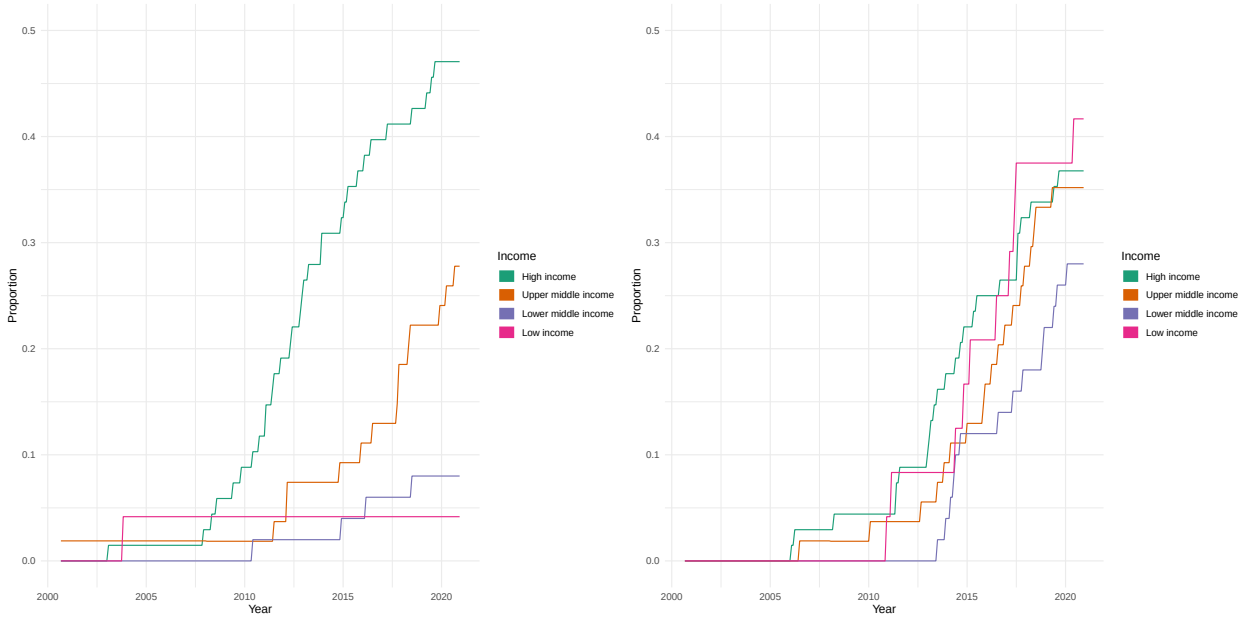
(b) Technical Bureaucracy

Figure 2: Proportion of Countries with Cybersecurity Doctrine or Policy by Bureaucracy

Figure 2a presents the adoption rates by non-technical bureaucracies, while 2b presents adoption rate by technical bureaucracies. Countries can feature in both graphs if they have an active cybersecurity document published by two different types of bureaucracies. Security bureaucracies includes those responsible for internal or external security. Technical bureaucracies include Ministries of ICT or Communications, along with national standards organizations and groups created specifically for cybersecurity.

As of 2020, around 15% of countries have a national cybersecurity document produced autonomously by a non-ICT bureaucracy, while 28% of countries have a national cybersecurity document produced autonomously by an ICT bureaucracy. The source of the "s-curve" has been adoption by technical bureaucracies. Adoption by security bureaucracies appears somewhat more linear since 2008, when the Slovak National Security Authority published the *National Strategy for Information Security* and the Estonian Defense Ministry produced their *Cyber Security Strategy.*

Figure 5 contains the proportion of countries with active cybersecurity documents by income and by



(a) Non-ICT Bureaucracy by Income

(b) ICT Bureaucracy by Income

Figure 3: Proportion of Countries with Cybersecurity Doctrine or Policy by Bureaucracy and by Income Level (World Bank)

bureaucracy. Subfigure 5a presents this number for non-ICT bureaucracies, while Subrigure 5b presents this number for ICT bureaucracies. There are distinct differences across income levels regarding these numbers. Firstly, independent policy from security bureaucracies is almost entirely limited to wealthy countries, largely in North America and Europe & Central Asia. All cybersecurity strategies in South Asia were created by separate technical bureaucracies. Furthermore, policy adoption in the low and lower-middle income countries is almost entirely driven by ICT bureaucracies.

7.2 Independent Variables

The geographic measures for spatial splines come from the *Dynamic Gravity Dataset*, which provides annual data for countries and country-pairs for 285 countries and territories (Gurevich and Herman, 2018). I also use this dataset for economic integration agreements between states, which the dataset defines according to Article V of GATS. For this analysis I assume that none of the values change from 2016-2020.I use the *Design of Trade Agreements (DESTA)* dataset Version 2.0 for the preferential trade agreement weights (Dür et al., 2014). For security alliances, I use the *Alliance Treaty Obligations and Provisions Project (ATOP)* data on military agreements (Leeds et al., 2002). Version 4.0 of the dataset covers all alliances formed between 1815 and December 31, 2016. I use the data from 2000 to 2016, and carry the 2016 values through 2020.

To understand the influence of security threats on strategy adoption, I use the *Peace Data* on rivalries

(Diehl et al., 2019). Version 2 of the dataset covers rivalries through 2015. It codes adversarial relationships between states on a scale of "severe rivalry," "lesser rivalry," and "negative peace." For each country, I measure the number of countries with "severe rivalry" in each year. These are relationships "in which the sates see one another as enemies and competitors," and includes relationships such as India-Pakistan and US-Iran.

I control for other conditions including the size, wealth, and type of government for each country. For government type I use the World Bank *Worldwide Governance Indicators*, which includes 215 countries and territories (Kaufmann et al., 2010). Most governance indicators, including Polity and Varieties of Democracy, do not have as wide a geographical scope. I use the "Voice and Accountability" index, which measures the extent to which a country's citizens are able to participate in government, media freedom, freedom of association, and freedom of expression. Data on wealth and population also come from the World Bank.

7.3 Methods

I construct adjacency matrices for N countries of size $N * N$ for each of the spatial control variables. For time-varying adjacencies, such as the number of preferential trade agreements between two countries, I construct an array of matrices for length year T for N countries which is $N * N * T$. The spatial weights are the matrix product of the adjacency matrix and the vector y_t, representing the countries which have an available cybersecurity document at time t. The weights for one period are commonly expressed as $[W_{yi}] = \sum_{j=1}^{n} w_{ij} y_i$.

I estimate Cox Proportional Hazard Models for adoption for three different of survival functions, which model the amount of time until a certain event occurs (Cox, 1972). This class of models is the most frequently used within policy adoption and diffusion studies (Box-Steffensmeier and Jones, 1997; Simmons and Elkins, 2004; Simmons et al., 2018). Covariates in hazard models provide the increased risk of a change in states occurring, given that the event has not occurred previously. Following the advice of others, I fit the model using semi-parametric splines for all continuous variables (Simmons et al., 2018; Therneau and Grambsch, 2000)

Each country series is measured as the number of months from August 2000 (when the first document was produced) until the country's first document was published, censored at 2020. This is then subset to consider the number of months until a document was published by an ICT bureaucracy and the number of months until a document was published by a non-ICT bureaucracy. To leverage month and year-level time-varying covariates I use interval censoring. In Cox Proportional-Hazards models negative coefficients

represent increases in survival, or in this case increases in the amount of time between the beginning of the window and when a document was produced.

8 Doctrine Adoption

The central findings are that 1) the explanations for policy diffusion are different depending on the institution that is delegated the policy, and 2) engagement with external experts increases the diffusion of cybersecurity policies and strategies for independent technical bureaucracies, but has no effect on security or executive bureaucracies. These findings are summarized in Table 1, which contains the hazard ratio coefficients for each of the variables in the analysis.

Among all strategies, CYBER REVIEW increases the chances by approximately 2.2 times that a country will publish a strategy, and among strategies adopted by independent technical bureaucracies it increases the chances by approximately 1.8 times. However, there is no effect of engagement with outside experts on the chances of adoption by a non-technical bureaucracies.[44] This supports the theory that technical assistance not only promotes cybersecurity doctrine development, but that this promotion is driven by organizations with a technical focus. This is surprising given that the entire government has access to this report and these engagements work with a cross-section of government bureaucracies. Other actors should be able to take the insights and develop their own strategy, and yet engagement with outside experts has no effect on diffusion outside of independent technical bureaucracies.

STRATEGY ADOPTION BY SECURITY AGREEMENTS PARTNERS and by STRATEGY ADOPTION BY ECONOMIC INTEGRATION AGREEMENTMEMBERS did have a significant and positive effect on adoption rates when considering all strategies or strategies developed by non-technical bureaucracies such as ministries of defense, national security councils, ministries of justice, or national police. Each additional EIA member with a cybersecurity strategy increased the probability of any diffusion by approximately 3.5%, and each ally with a cybersecurity strategy increased the probability of diffusion by approximately 1.8%. Adoption by PTA members did not have a significant effect on the rate of adoption for any subset of strategies.[45] Future research can address why adoption by economic integration partners, but not preferential trade partners, is associated with diffusion.

The only learning mechanism that explained policy diffusion among non-technical bureaucracies was adoption by allies, which increased the probability of diffusion by approximately 1.8%. This suggests that

[44] As a robustness check, I run this analysis for 2014 to the present, when cybersecurity capacity reviews began. This removes all countries which published documents before 2014. The coefficient for CYBER REVIEW changes from 3.23 to 3.71 for all strategies, and from 2.89 to 2.59 for technical bureaucracy strategies. The significance of the coefficients does not change.

[45] This result holds if limited to PTA's with an e-commerce component. It also holds if the regression removes the economic integration term.

Table 1: Cybersecurity Strategy Adoption

	All Strategies	Technical Bureaucracies	Non-technical Bureaucracies
Cyber Review	3.24169*	2.87508*	1.66968
	(0.00056)	(0.00642)	(0.40512)
PTA Adoption (ws)	0.99672	0.99342	0.99348+
	(0.25819)	(0.06213)	(0.08021)
EIA Adoption (ws)	1.03581*+	0.9873	1.01981+
	(0.00063)	(0.38769)	(0.19757)
Ally Adoption (ws)	1.01482*	0.99698+	1.01813*+
	(0.00707)	(0.69189)	(0.02074)
Internet Pct (s)	1.01952	1.00454+	1.03684*
	(0.02937)	(0.70657)	(0.00715)
Domestic Expertise (s)	1.09123+	1.44047+	0.91872+
	(0.70869)	(0.28777)	(0.76221)
Number of Rivals (s)	1.34898*+	0.61004*+	1.21824*+
	(0)	(2e-05)	(0.00018)
Gov. Effectiveness (s)	2.34039*	2.41578*+	1.53956+
	(0.00158)	(0.00208)	(0.16606)
GDPpc (log) (s)	0.65081+	0.43345*+	0.60547+
	(0.04185)	(0.00024)	(0.12429)
n	39306	43079	43751
n events	107	69	48
NPH Prop pj.05	0	0	0
Global NPH Prop pj.05	0.9299	0.9015	0.9943

Note: These models all control for population, distance spatial lags, and contiguous state spatial lags. Results are from a Cox-Proportional Hazards Model with standard errors clustered at the country level. The coefficient is for the linear effect of the covariate. The reported values are the hazard ratios.
"*"=linear effect significant at the .025 level.
"+"=nonlinear effect significant at the .025 level.
"s" indicates a spline term, while "ws" indicates a weighted spline term.

this policy area diffuses among non-technical organizations through ally networks such as NATO, ASEAN, or the Shanghai Cooperation Organization (SCO). One explanation for why this effect does not hold for technical bureaucracies may be that these bureaucrats have fewer opportunities to network in these institutions than non-technical bureaucrats, and so information can not pass through these mechanisms.

Many security and economic integration organizations have invested in cybersecurity cooperation in the past fifteen years. NATO includes cybersecurity among its collective defense tasks and accredits an institution that supports cybersecurity education and provides expertise to member states. That institution provides courses on international law and cyber operation and published a manual on international law that is referenced in several country's strategies. The OAS has published a cybersecurity strategy guide and assisted cybersecurity capacity across its member states. The press release on the 13th SCO National Security Council Secretaries in 2018 called "for intensifying practical cooperation in the field of international information security and drafting universal regulations, principles and norms of states' responsible conduct

in the media sector".[46]

The presence of rival states also has a positive effect on strategy adoption, but this too depends on the type of institution. Each additional rival increases the probability of strategy diffusion by approximately 38 percent for all strategies, and by approximately 35 percent when considering only strategies by non-technical bureaucracies. On the otherhand, it decreases the probability of diffusion by technical bureaucracies by approximately 38 percent. The international system may shape state institutions (Gourevitch, 1978), and external threat is central to the consolidation of modern states (Rasler and Thompson, 1985; Tilly, 1985). Valeriano and Maness (2014) argued that few rivals are engaged in cyber conflict, but this analysis demonstrates that the presence of rivals increases the likelihood that a state will adopt a national cybersecurity strategy, and this effect is almost entirely driven by non-technical bureaucracies. This also suggests that external threat does more than promote policy diffusion - it makes diffusion more likely within bureaucracies with an explicit military or policing mandate.

DEMAND, which in this case is measured by percentage with access to the internet, has a significant and positive effect for all strategies and the subset of strategies adopted by non-technical bureaucracies. A 1 percent increase in the percentage of the population with access to the internet is associated with a roughly 3 percent increase in the probability of adoption for all types and approximately 5 percent increase in the probability of adoption for non-technical bureaucracies. Technical bureaucracies policy adoption is significant at the 90% level.

Domestic expertise, on the other hand, does not have a significant effect across the models. This may mean that, even in countries with low overall levels of cybersecurity expertise, governments can access enough expertise to develop strategies and doctrines. It may also indicate that countries can copy cybersecurity strategy models from other states, or contract cybersecurity strategy out to an external actor such as a international institution or consulting group. The fact that cybersecurity capacity assistance promotes strategy adoption suggests this may be the case.

Government effectiveness, which measures many aspects of state capacity, has a positive and significant effect on policy adoption overall and policy adoption by non-technical bureaucracies. A one standard deviation increase in the government effectiveness score was associated with a 234% increase in the probability of adoption for all strategies, and a 241% increase in the probability of adoption for non-technical bureaucracies.

Wealth decreases the diffusion of strategy diffusion by technical bureaucracies, but not among non-technical bureaucracies. This suggests that wealthier countries are more likely to delegate strategy development to organizations such as a national police or military. Future research can examine why less wealthy countries are less likely to defer cybersecurity strategy development to technical bureaucracies. One expla-

[46] http://eng.sectsco.org/news/20180522/431989.html

nation may be that cybersecurity in wealthy countries covers a different set of issues than in developing ones. An implication of this may be that, as countries become wealthier, they remove the cybersecurity portfolio from technical groups.

8.1 Alternatives

There are several potential challenges to inference with this approach. One is that stronger technical bureaucracies can invite outside experts, and so the engagement is endogenous with bureaucratic independence. The main outcome, policy adoption, is the measure of bureaucratic autonomy, but bureaucratic autonomy and strength may affect the likelihood of inviting reviews. If this is the case, we should see evidence of cybersecurity doctrine development before the review period. Additionally, we should not expect the strategy itself to be shaped by the engagement, since the strategy was developed by a strong and capable bureaucracy.

Senegal and the case of the *Stratégie Nationale de Cybérsecurité du Sénégal*, published in November 2017, demonstrates the limits of this logic. The Ministry of Communication, Telecommunications, Post, and Digital Economy hosted a cybersecurity capacity review in January 2016, which produced a 53-page set of recommendations for February 2016. The review stated that the national Cyber Task Force, which was convened to develop the national strategy, had only met twice in the year since it was created. As of the review, "there are several agencies, ministries and organisations that conduct ad-hoc cybersecurity initiatives." The strategy that was published in 2017 was authored by the Ministry of Communication, Telecommunications, Post, and Digital Economy, and makes no mention of a national task-force.

Mozambique's national cybersecurity strategy reflects the same dynamics. The Commonwealth Telecommunications Organization (CTO) carried out a cybersecurity capacity review in 2016 hosted by the Instituto Nacional das Comunicações de Moçambique (INCM). There was no national cybersecurity strategy at that point, but the introduction to the review " calls on the CTO team to assist the Republic of Mozambique develop a National Cybersecurity Strategy (NCS) for Mozambique." The final version of the national cybersecurity strategy was drafted by the INCM. A nearly identical case occurred in Bermuda, where the group that provided the cybersecurity capacity review and guidance emphasized the need for a national strategy and assisted their host organization in creating one.

However, even if the review is endogenous, the interpretation of these results is no less striking. Instead, more powerful and autonomous technical bureaucracies would be more likely to invite outside experts into the policy process. If this is the case, they may be networking to increase their autonomy, which has been demonstrated at the national level (Carpenter, 2001), but not at the international level. While epistemic communities exist and can shape policy (Adler and Haas, 1992), there is little evidence that they network

to increase one another's power within their respective political environments.

Another potential challenge is that the factors which correlate with inviting outside experts may also explain policy adoption. For instance, countries with higher levels of internet access are more likely to adopt cybersecurity strategies, and higher internet access may also explain why certain countries invite outside experts. Appendix Table 4 contains the results of a survival analysis for cybersecurity capacity reviews, beginning with March 2014.

Government effectiveness did significantly increase the hazard of cybersecurity review, while wealth significantly decreased the hazard of review. This leaves open the possibility that the less developed countries with effective governments are more likely to invite cybersecurity experts and publish doctrines. However, overall there was no relationship between wealth and policy adoption, so while poorer countries were more likely to institutionalize within a technical bureaucracy and invite a capacity review, they were overall not more likely to publish a strategy. Future work will incorporate a measure of technical regulatory power that can help untangle whether this effect is driven by independent bureaucratizes inviting outside experts, if outside experts help increase bureaucratic autonomy, or if this is a networking model where these groups work together to increase autonomy (Carpenter, 2001).

9 Does Policy Ownership Matter?

9.1 Text Methods

Engagement with outside experts may increase the hazard of policy adoption in technical bureaucracies, but is that because these bureaucracies emphasize distinct dimensions of cybersecurity? What is not clear yet is whether ownership over cybersecurity issues actually impacts a country's understanding of the underlying policy issue. One could assume that all cybersecurity strategies produced by ministries of finance are similar, and are more likely to reflect the values of financial interests within a state. Alternatively, ICT regulatory bodies may produce more technocratic policies. However, recent advances in text-as-data methods allow researchers to understand not just whether a policy was created, but how policies relate to one another and the factors that drive them to express different concepts.

The rational choice policy diffusion literature typically focuses on pieces of legislature or practices that can be discretely measured over time. For instance gender quotas within national legislatures (Bush, 2011), women's suffrage (Ramirez and Boli, 1987), the presence of election monitors (Hyde, 2011; Kelley, 2011), government spending levels, or criminalizing human trafficking (Simmons et al., 2018). Thus far, the analysis has demonstrated that diffusion among different bureaucracies follows different logics, explains how technical bureaucratic independence is a desirable outcome for developed states, and shows that technical bureaucracies

benefit from engagement with external actors.

Text methods have already produced compelling research on the behaviors of political actors. In one of the earliest applications of text-as-data researchers were able to extract economic and social policy positions of politicians in Britain and Ireland (Laver et al., 2003). Since then other researchers have used text to understand the policy positions of political actors from debate records (Budge, 2001; Catalinac, 2014). Stewart and Zhukov (2009) successfully applied a supervised content analysis to 8000 public statements made by Russia's elites to understand preferences over the use of force. They were able to conclude that while military elites are more activist in considering the use of force, they were more hesitant to embrace intervention. Baturo and Mikhaylov (2013) demonstrated how constituents pick up on informational messages from leaders in the Russian elites. Miller (2013) used text analysis to show how the long-term impact of colonization manifests itself in speech patterns at the United Nations. Schonhardt-Bailey (2006) utilized text clustering to analyze political debates on trade over time.

Beginning with the whole cybersecurity corpus, I convert frequent cybersecurity terms to a common format to increase the comparability of the texts.[47] This data is then tokenized[48] and organized by document. I parse this text with a universal-dependencies algorithm using the `udpipe` package in $\mathbb{R}$. This process tags each term with a part of speech and converts each term into a lemma.[49] From here I implement a keyword algorithm, specifically the Rapid Automatic Keyword Extraction (RAKE) algorithm, to identify terms that should be considered as one (Rose et al., 2010). For instance, some text methods might consider "United Nations" as three terms, one for "United", one for "Nations" and the third "United Nations." One submission that uses United Nations and another that uses the word national might then be incorrectly assumed to be related. Implementing a keyword algorithm helps limit this risk. I then apply structural topic models to the corpus with prevalence covariates to estimate the topics and the factors that influence documents' placement into topics (Roberts et al., 2019).

9.2 Doctrine Content

Do technical bureaucracies, which are often provided support from outside expert networks, represent distinct viewpoints in the strategies that they eventually adopt? After selecting the optimal value of k (the number of topics) I estimate the topic model for doctrine content. I include prevalence covariates for whether the policy was created by a technical organization and year splines. Table 2 contains the sixteen topics listed by γ, the prevalence of the topic within the corpus. The terms listed have the highest FREX values, a metric

[47] For example, cyber crime and cyber-crime are converted to cybercrime, cyber security and cyber-security are converted to cybersecurity, etc.

[48] Split into separate terms from one block of text.

[49] A lemma is the most basic part of speech. For instance, "growing" becomes "grow."

that ranks items by their frequency and exclusivity (Bischof and Airoldi, 2012; Airoldi and Bischof, 2016; Roberts et al., 2019). These terms are relatively exclusive to the topic, but also frequent within the corpus itself. Figure 4 contains the regression results for technical bureaucracy authorship for topic prevalence.

Table 2: Topic FREX Terms

Topic	γ	Concept	FREX
T5	0.12	CERTs & Child Protection	cii, specific object, national cybersecur, framework, national cybersecurity strategi, csirt, child, ict, critical information infrastructur, month, cert, address
T13	0.11	Cybercrime	deliv, prosper, onlin, cybercrimin, advic, harm, deter, drive, exploit, malici, resili, success
T12	0.10	Cooperation & Defense	compet, cybersecurity strategi, situat, nato, ict secur, cooper, sustain, phase, crisi, ict, cyber def, crise
T2	0.09	Sovereignty	adapt, digital secur, anssi, digit, fight, sovereignti, personal data, cyberthreat, cyberspac, axi, reinforc, essenti
T16	0.09	Budget & Admin	institut, annex, task, approv, budget, public administr, republ, council, ict system, interior, action plan, alloc
T8	0.06	Multi-stakeholder	digital secur, decre, digital environ, cybernet, retriev, articl, multiple stakehold, countri, commiss, latin, novemb, percent
T10	0.06	Critical infrastructure	ncsc, workforc, pillar, critical national infrastructur, cyber resili, communiti, recognis, malicious cyber act, essential servic, engag, wide, partnership
T6	0.05	Military & Defense	cyber defens, defens, dod, command, nato, militari, mission, defend, weapon, alli, armi, armed forc
T3	0.05	Standards & management	information secur, chapter, information security polici, information societi, entiti, information security manag, standard, matur, national inform, section, information security issu, national information secur
T4	0.05	Talent & Government	government ag, agenc, talent, facilit, public organ, complet, unit, national cybersecur, offic, mechan, cultiv, cybersecurity industri
T1	0.05	Business	digital domain, digit, author, business commun, polic, parti, supplier, knowledg, public author, societ, authoriti, supervis
T7	0.04	Information sphere	state polici, information spher, information spac, sphere, feder, republ, state author, information resourc, information protect, informat, format, telecommunication system
T9	0.04	Risk management	federal govern, cyber risk, feder, ncs, critical infrastructur, prioriti, depart, vulner, national strategi, secretari, reduc, secure cyberspac
T15	0.03	Technical	electronic commun, internet, traffic, internet infrastructur, internet secur, name, bill, exampl, other th, server, cybersecurity effort, protocol
T11	0.03	Standards	iec, password, physical secur, mandat, information asset, log, access, record, business continu, asset, backup, access control
T14	0.03	Information sharing	ci oper, cybersecurity measur, cybersecurity polici, nisc, util, iot, cip, governmental bodi, share, cross, information shar, outag

The most frequent topic in the corpus is differentiated by other topics by its focus on Computer Emergency Response Teams (CERTs) and internet issues such as child protection. Capacity development and cybercrime were also frequently present in this topic, but appear frequently in other topics as well. This topic was significantly more prevalent in the documents produced by technical bureaucracies. CERT groups respond to cybersecurity issues, serve as a resource for cybersecurity best practices, and share information with other CERTs in international forums and through bilateral agreements. These teams are viewed as a

necessary part of cybersecurity capacity building. For instance, the International Telecommunications Union (ITU) includes CERT development in its targetted development portfolio, writing that these groups could "identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level."[50]. Israel agreed to establish a national CERT in Honduras in 2017,[51] and CERTS exchange information between China and Australia.

The prevalence of Topics 13, 12, 2, 16, 8, and 10 is not connected to policy ownership by technical bureaucracies. Topic 13 concerns issues related to cybercrime, while Topic 12 connects to issues around cooperation and defense. Topic 12 is also connected to NATO, which has a robust cybersecurity program. Topic 2 addresses cyber-sovereignty issues, which are most common in Chinese cybersecurity discussions. Topic 16 concerns budget and administrative issues, which should be no more likely in technical than non-technical owned documents. Topic 8 is the multi-stakeholder topic, which also features Latin America. Critical infrastructure issues characterize Topic 10.

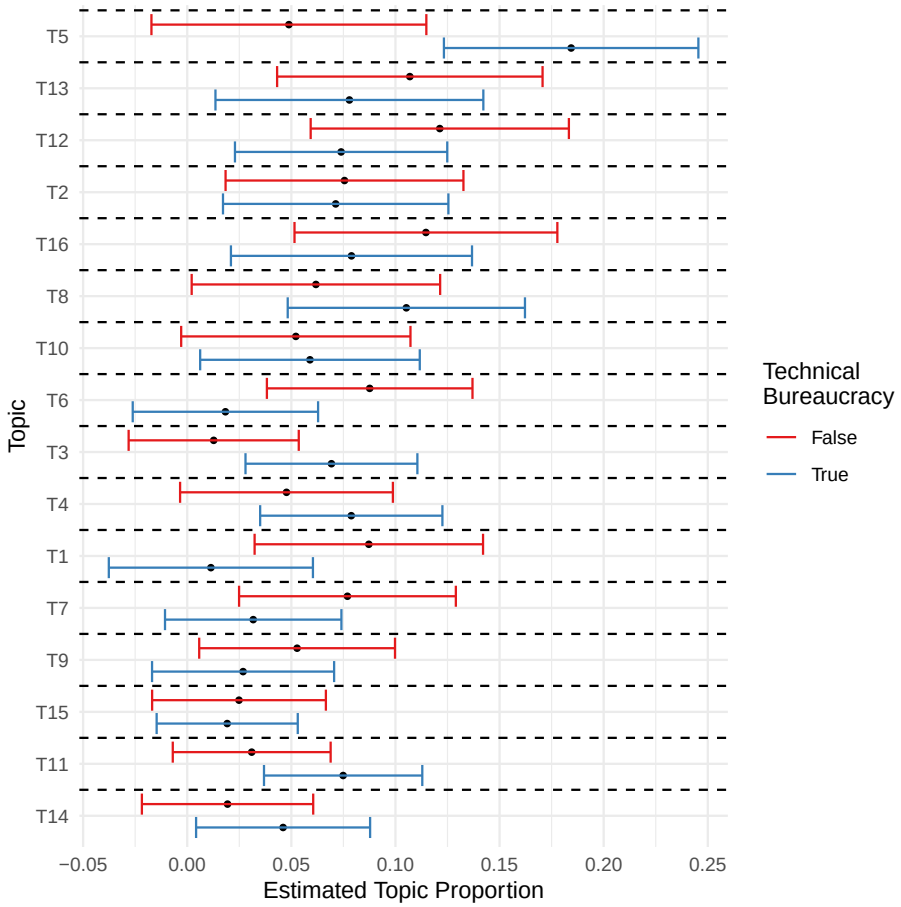
Authorship by technical institutions has a significant impact on Topic 6, which focuses on military and defense applications of cyber technologies. It includes terms such as armies, cyber defense, command, military, and armed forces. This dimension of cybersecurity is the focus of most of the academic literature on "netwar" and deterrence. Technical institutions that own the cybersecurity policy portfolio are significantly less likely to produce documents that emphasize these dimensions of cybersecurity capacity.

Conversely, these strategies are more likely to feature Topic 3, which addresses standards and management of cyberspace. It also features development terms such as "maturity", and information security issues. As Kello (2017) notes, the political science community and technical experts have different images in mind for a concept like "information security." The technical community considers this as data protection methods, while information security sounds more like information control to political scientists. Information security is an older concept than cybersecurity, and is concerned primarily with the individual actors within the ICT system, data confidentiality, and protecting private information from being stolen.

Technical institutions are no more or less likely to address Topic 4 (talent & government), but are less likely to address Topic 1. One potential explanation for this is that technical institutions are more shielded from the business community, perhaps because they are able to access cybersecurity expertise from other sources such as international institutions or foreign governments. Another explanation is that wealthier countries, which are less likely to defer to technical institutions, must do more to address the business community in their nation. None of the other topics, including Topic 7 (information sphere), Topic 9 (risk management), Topic 15 (technical), Topic 11 (standards) and Topic 14 (information sharing) appear more

[50] [International Telecommunications Union] (2010)
[51] http://www.israeldefense.co.il/en/node/28961

Figure 4: Effect of Technical Bureaucratic Author on Expected Topic Prevalence



Note: Difference in expected topic proportion for whether a document was produced by a technical bureaucracy. Topics are ordered from highest to lowest overall proportion in the corpus.

or less frequently in technical bureaucracy-produced documents.[52]

Accordingly, when external actors network with technical institutions and help them maintain the cybersecurity policy portfolio they anticipate strategies that emphasize and de-emphasize specific dimensions of the domain. These policies are more likely than their counterparts produced by security or judicial bureaucracies to address CERTS and child protection, and also standards and management and information security. They are significantly less likely to write about the business community and suppliers, and also the military and defense. This helps explain why technical ownership over the cybersecurity portfolio is advantageous to external actors.

[52] At the 90% level, technical bureaucracy authorship is associated with less prevalence for Topic 7 and more prevalence for Topic 11. However, I do not include these in the discussion.

10 Conclusion

Increasing interdependence and global diffusion of information technologies presents challenges to developed states. On the one hand, the spread of ICTs has the potential to alleviate poverty and encourage the free flow of information. Gaps in cybersecurity capacity have the potential to create negative policy externalities for developed states as they open up information flows with less developed countries. Nevertheless, cybersecurity capacity is fluid and easily re-purposed for coercive ends. This paper argues that this creates an incentive to diffuse expertise and also promote institutionalization within certain parts of host governments.

Bureaucracies and government institutions worldwide are fighting for control over the cybersecurity portfolio, which is a valuable policy area that touches nearly every part of modern governance. Many developing states have worked with outside agencies to assist cybersecurity policy formulation and institutionalization. As a result, states which have networked with outside experts are more likely than their peers to develop cybersecurity startegy, but this effect only holds for technical bureaucracies such as ministries of communications, and not for non-technical bureaucracies such as ministries of justice, national police, or defense bureaucracies. Instead, diffusion in those areas can be explained through traditional interstate communication channels such as security alliances or economic integration agreements.

There are several other areas for future research that will deepen our understanding of how expert networks influence national policy-making. In cyberspace there are certainly cases of external influence in the policy-making process absent cybersecurity capacity reviews. This includes the OAS in Belize (2020)[53], Guatemala (2018),[54] Paraguay (2016),[55] and Costa Rica (2017).[56] The ITU has carried out similar engagements in Nepal (2016)[57] and Mauritania (2019).[58] While there are other ways experts can provide support, cybersecurity capacity reviews are engagements which do not select on the dependent variable of influence in the final product. There is an unknown quantity of cybersecurity assistance missions outside of capacity reviews that did not result in strategy adoption.

Efforts to increase bureaucratic autonomy would be ineffective if policy ownership does not affect strategy content. This paper has demonstrated the cross-national variation in cybersecurity policy content, and how that content is driven by the underlying ownership of the policy area. Technical bureaucracies produce strategies that focus relatively more on computer emergency response teams, child protection, standards,

[53] https://www.oas.org/en/about/offices_events.asp?sCode=BEL

[54] http://www.oas.org/en/sms/cicte/default.asp

[55] "this Plan was produced National with the participation of the various sectors involved in the issue of cybersecurity in Paraguay under the support and facilitation of the Organization of American States (OAS)."

[56] "Cybersecurity requires a holistic vision and multisector attention, therefore, in the process of building this strategy, the Ministry of Science, Technology and Telecommunications (MICITT) had the specialized technical support of the Organization of American States (OAS)"

[57] "The Policy has been developed by Nepal Telecommunication Authority with technical assistance from International Telecommunication Union (ITU)."

[58] The logo for the ITU is featured on the first page of the Mauritanian national cybersecurity strategy.

and information security, and relatively less on the business community and the military. As a result, many developing states exhibit distinct cybersecurity policy views not because of the threat environment they face or their participation in international institutions, but due to the bureaucracy they delegate policy to, which is influenced by engagements with external actors. Future work will explore how outside expert assistance affects the specific wording of cybersecurity strategies, and the other forms of cooperation that may result from increased internet interdependence.

References

Acemoglu, D. and D. Autor (2010, June). Skills, Tasks and Technologies: Implications for Employment and Earnings. Working Paper 16082, National Bureau of Economic Research.

Adler, E. and P. M. Haas (1992). Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program. *International Organization 46*(1), 367–390.

Airoldi, E. M. and J. M. Bischof (2016, October). Improving and Evaluating Topic Models and Other Models of Text. *Journal of the American Statistical Association 111*(516), 1381–1403.

Alesina, A. and D. Dollar (2000, March). Who Gives Foreign Aid to Whom and Why? *Journal of Economic Growth 5*(1), 33–63.

Arquilla, J. and D. Ronfeldt (1993). Cyberwar is Coming! https://www.rand.org/pubs/reprints/RP223.html.

Axelrod, R. (1997, April). The Dissemination of Culture: A Model with Local Convergence and Global Polarization. *Journal of Conflict Resolution 41*(2), 203–226.

Baturo, A. and S. Mikhaylov (2013, June). Life of Brian Revisited: Assessing Informational and Non-Informational Leadership Tools. *Political Science Research and Methods 1*(01), 139–157.

Benavente, J., D. Bravo, and R. Montero (2011, December). Wages and workplace computer use in Chile. *The Developing Economies 49*, 382–403.

Bermeo, S. B. (2018). *Targeted Development: Industrialized Country Strategy in a Globalizing World*. New York, NY, United States of America: Oxford University Press.

Bischof, J. M. and E. M. Airoldi (2012, June). Summarizing topical content with word frequency and exclusivity. In *Proceedings of the 29th International Coference on International Conference on Machine Learning*, ICML'12, Madison, WI, USA, pp. 9–16. Omnipress.

Borghard, E. D. and S. W. Lonergan (2017, July). The Logic of Coercion in Cyberspace. *Security Studies 26*(3), 452–481.

Box-Steffensmeier, J. M. and B. S. Jones (1997). Time is of the essence: Event history models in political science. *American Journal of Political Science*, 1414–1461.

Buchanan, B. (2017). *Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System.* Oxford University Press.

Budge, I. (Ed.) (2001). *Mapping Policy Preferences: Estimates for Parties, Electors, and Governments, 1945-1998*. Oxford ; New York: Oxford University Press.

Burnside, C. and D. Dollar (2000). Aid, Policies, and Growth. *The American Economic Review 90*(4), 847–868.

Bush, S. S. (2011, January). International Politics and the Spread of Quotas for Women in Legislatures. *International Organization 65*(1), 103–137.

Carpenter, D. P. (2001). *The Forging of Bureaucratic Autonomy: Reputations, Networks, and Policy Innovation in Executive Agencies, 1862-1928*. Princeton, N.J: Princeton University Press.

Catalinac, A. (2014). Quantitative Text Analysis with Asian Languages: Some Problems and Solutions. *Polimetrics I*(1).

Choi, C. (2010, November). The effect of the Internet on service trade. *Economics Letters 109*(2), 102–104.

Choi, C. and M. Hoon Yi (2009, October). The effect of the Internet on economic growth: Evidence from cross-country panel data. *Economics Letters 105*(1), 39–41.

Clarke, R. A. and R. K. Knake (2012). *Cyber War: The Next Threat to National Security and What to Do About It* (1st Ecco pbk. ed ed.). New York: Ecco.

[Commonwealth Technology Organisation] (2015). Commonwealth Approach for Developing National Cybersecurity Strategies. Technical report, Commonwealth of Nations.

Cox, D. R. (1972). Regression Models and Life-Tables. *Journal of the Royal Statistical Society. Series B (Methodological) 34*(2), 187–220.

Craig, A. and B. Valeriano (2016, May). Conceptualising cyber arms races. pp. 141–158.

de Mesquita, B. B. and A. Smith (2009). A Political Economy of Aid. *International Organization 63*(2), 309–340.

Diehl, P. F., G. Goertz, and Y. Gallegos (2019, September). Peace data: Concept, measurement, patterns, and research agenda. *Conflict Management and Peace Science*, 073889421987028.

Dogrul, M., A. Aslan, and E. Celik (2011, June). Developing an international cooperation on cyber defense and deterrence against Cyber terrorism. In *2011 3rd International Conference on Cyber Conflict*, pp. 1–15.

Drew, C. and S. Shane (2013, July). Résumé Shows Snowden Honed Hacking Skills. *The New York Times*.

Dür, A., L. Baccini, and M. Elsig (2014). The design of international trade agreements: Introducing a new dataset. *The Review of International Organizations 9*(3), 353–375.

Easterly, W. and T. Pfutze (2008, June). Where Does the Money Go? Best and Worst Practices in Foreign Aid. *Journal of Economic Perspectives 22*(2), 29–52.

Easterly, W. and C. R. Williamson (2011). Rhetoric versus Reality: The Best and Worst of Aid Agency Practices. *World Development 39*(11), 1930–1949.

Farrell, H. (2015, April). Promoting Norms for Cyberspace. http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358.

Farrell, H. and A. L. Newman (2019, July). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security 44*(1), 42–79.

Farwell, J. P. and R. Rohozinski (2011, February). Stuxnet and the Future of Cyber War. *Survival 53*(1), 23–40.

Fefer, R. F., S. I. Akhtar, and W. M. Morrison (2019, May). Digital Trade and U.S. Trade Policy. pp. 45.

Finnemore, M. and K. Sikkink (2001, June). The Constructivist Research Program in International Relations and Comparative Politics. *Annual Review of Political Science 4*(1), 391–416.

Freund, C. and D. Weinhold (2002, May). The Internet and International Trade in Services. *American Economic Review 92*(2), 236–240.

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

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly 4*(3), 102–135.

Gourevitch, P. (1978). The Second Image Reversed: The International Sources of Domestic Politics. *International Organization 32*(4), 881–912.

Guillén, M. F. and S. L. Suárez (2005, December). Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-National Internet Use. *Social Forces 84*(2), 681–708.

Gurevich, T. and P. Herman (2018). The Dynamic Gravity Dataset: Technical Documentation.

Haas, P. M. (1992). Introduction: Epistemic Communities and International Policy Coordination. *International Organization 46*(1), 1–35.

Haveman, H. A. (1993). Follow the Leader: Mimetic Isomorphism and Entry Into New Markets. *Administrative Science Quarterly 38*(4), 593–627.

Hyde, S. D. (2011). *The Pseudo-Democrat's Dilemma: Why Election Monitoring Became an International Norm*. Cornell University Press.

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security 7*(1), 54–67.

[International Telecommunications Union] (2010, June). Final Report: World Telecommunication Development Conference. Technical report, International Telecommunications Union, Hyderabad, India.

Johnston, A. I. (2008). *Social States: China in International Institutions, 1980-2000*. Princeton Studies in International History and Politics. Princeton, NJ: Princeton Univ. Press.

Kaufmann, D., A. Kraay, and M. Mastruzzi (2010). The Worldwide Governance Indicators: Methodology and Analytical Issues. Technical Report 5430, The World Bank.

Kelley, J. (2011, November). Do International Election Monitors Increase or Decrease Opposition Boycotts? *Comparative Political Studies 44*(11), 1527–1556.

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

Kenny, C. (2002). Information and Communication Technologies for Direct Poverty Alleviation: Costs and Benefits. *Development Policy Review 20*(2), 141–157.

Keohane, R. O. (1982). The demand for international regimes. *International Organization 36*(2), 325–355.

Keohane, R. O. and J. S. Nye (1973, July). Power and interdependence. *Survival 15*(4), 158–165.

Kostyuk, N., S. Powell, and M. Skach (2018). Determinants of the Cyber Escalation Ladder. *The Cyber Defense Review 3*(1), 123–134.

Krueger, A. B. (1993). How Computers Have Changed the Wage Structure: Evidence from Microdata, 1984-1989. *The Quarterly Journal of Economics 108*(1), 33–60.

Laver, M., K. Benoit, and J. Garry (2003, May). Extracting Policy Positions from Political Texts Using Words as Data. *American Political Science Review 97*(02).

Leeds, B. A., J. M. Ritter, S. M. Mitchell, and A. G. Long (2002). Alliance Treaty Obligations and Provisions, 1815-1944. *International Interactions 28*, 237–260.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND.

Libicki, M. C. (2012). Crisis and Escalation in Cyberspace. https://www.rand.org/pubs/monographs/MG1215.html.

Lin, H. (2012). Escalation dynamics and conflict termination in cyberspace. *Strategic Studies Quarterly*, 46–70.

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

Lu, D. (2015, December). When Ethical Hacking Can't Compete. https://www.theatlantic.com/technology/archive/2015/12/white-hat-ethical-hacking-cybersecurity/419355/.

McNamara, K. R. (1998). *The Currency of Ideas: Monetary Politics in the European Union*. Cornell Studies in Political Economy. Ithaca, N.Y: Cornell University Press.

Meyer, J. W., J. Boli, G. M. Thomas, and F. O. Ramirez (1997). World Society and the Nation-State. *American Journal of Sociology 103*(1), 144–181.

Miller, M. C. (2013). *Wronged by Empire: Post-Imperial Ideology and Foreign Policy in India and China*. Studies in Asian Security. Stanford, California: Stanford University Press.

Morrison, K. M. (2007, June). Natural Resources, Aid, and Democratization: A Best-Case Scenario. *Public Choice 131*(3), 365–386.

Mulrine, A. (2013, September). Cyber security: The new arms race for a new front line. *Christian Science Monitor*.

Nieles, M., K. Dempsey, and V. Y. Pillitteri (2017, June). An introduction to information security. Technical Report NIST SP 800-12r1, National Institute of Standards and Technology, Gaithersburg, MD.

Norris, P. (2001, September). *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge University Press.

Oppenheimer, H. (2020). The Diffusion of Cyber Threat: Security in the Network.

Osula, A.-M. and K. Kaska (2013). National Cyber Security Strategy Guidelines. Technical report, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Ramirez, F. O. and J. Boli (1987). The Political Construction of Mass Schooling: European Origins and Worldwide Institutionalization. *Sociology of Education 60*(1), 2–17.

Rasler, K. A. and W. R. Thompson (1985). War Making and State Making: Governmental Expenditures, Tax Revenues, and Global Wars. *The American Political Science Review 79*(2), 491–507.

Raustiala, K. (2002). The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law. *Virginia Journal of International Law 43*.

Remmer, K. L. (2004, January). Does Foreign Aid Promote the Expansion of Government? *American Journal of Political Science 48*(1), 77–92.

Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford ; New York: Oxford University Press.

Rid, T. and B. Buchanan (2015, January). Attributing Cyber Attacks. *Journal of Strategic Studies 38*(1-2), 4–37.

Roberts, M. E., B. M. Stewart, and D. Tingley (2019). **Stm** : An *R* Package for Structural Topic Models. *Journal of Statistical Software 91*(2).

Rogers, E. M. (2003). *Diffusion of Innovations*.

Rose, S., D. Engel, N. Cramer, and W. Cowley (2010, March). Automatic Keyword Extraction from Individual Documents. In M. W. Berry and J. Kogan (Eds.), *Text Mining*, pp. 1–20. Chichester, UK: John Wiley & Sons, Ltd.

Schonhardt-Bailey, C. (2006). *From the Corn Laws to Free Trade: Interests, Ideas, and Institutions in Historical Perspective*. Cambridge, Mass: MIT Press.

Schulze, M. (2018, September). Where Does Cyber Defense Stop and Offense Begin?

Sharma, A. (2010, February). Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis 34*(1), 62–73.

Simmons, B. A. and Z. Elkins (2004, February). The Globalization of Liberalization: Policy Diffusion in the International Political Economy. *American Political Science Review 98*(1), 171–189.

Simmons, B. A., P. Lloyd, and B. M. Stewart (2018). The Global Diffusion of Law: Transnational Crime and the Case of Human Trafficking. *International Organization 72*(2), 249–281.

Slaughter, A.-M. (2003). Global Government Networks, Global Information Agencies, and Disaggregated Democracy. *Michigan Journal of International Law 24*(4).

Slayton, R. (2016). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. *International Security 41*(3), 72–109.

Stewart, B. M. and Y. M. Zhukov (2009, June). Use of force and civil–military relations in Russia: An automated content analysis. *Small Wars & Insurgencies 20*(2), 319–343.

[The White House] (2011, May). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Technical report, The White House, Washington, D.C.

Therneau, T. M. and P. M. Grambsch (2000). *Modeling Survival Data: Extending the Cox Model*. Statistics for Biology and Health. New York: Springer-Verlag.

Thompson, H. and C. Garbacz (2007). Mobile, fixed line and Internet service effects on global productive efficiency. *Information Economics and Policy 19*(2), 189–214.

Tilly, C. (1985, September). War Making and State Making as Organized Crime. In P. B. Evans, D. Rueschemeyer, and T. Skocpol (Eds.), *Bringing the State Back In* (First ed.)., pp. 169–191. Cambridge University Press.

Triolo, P., R. Creemers, and G. Webster (2017, July). China's Ambitious Rules to Secure 'Critical Information Infrastructure'.

Valeriano, B., B. M. Jensen, and R. C. Maness (2018). *Cyber Coercion: The Evolving Character of Cyber Power and Strategy*. New York, NY: Oxford University Press.

Valeriano, B. and R. C. Maness (2014, May). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research 51*(3), 347–360.

Valeriano, B. and R. C. Maness (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford ; New York: Oxford University Press.

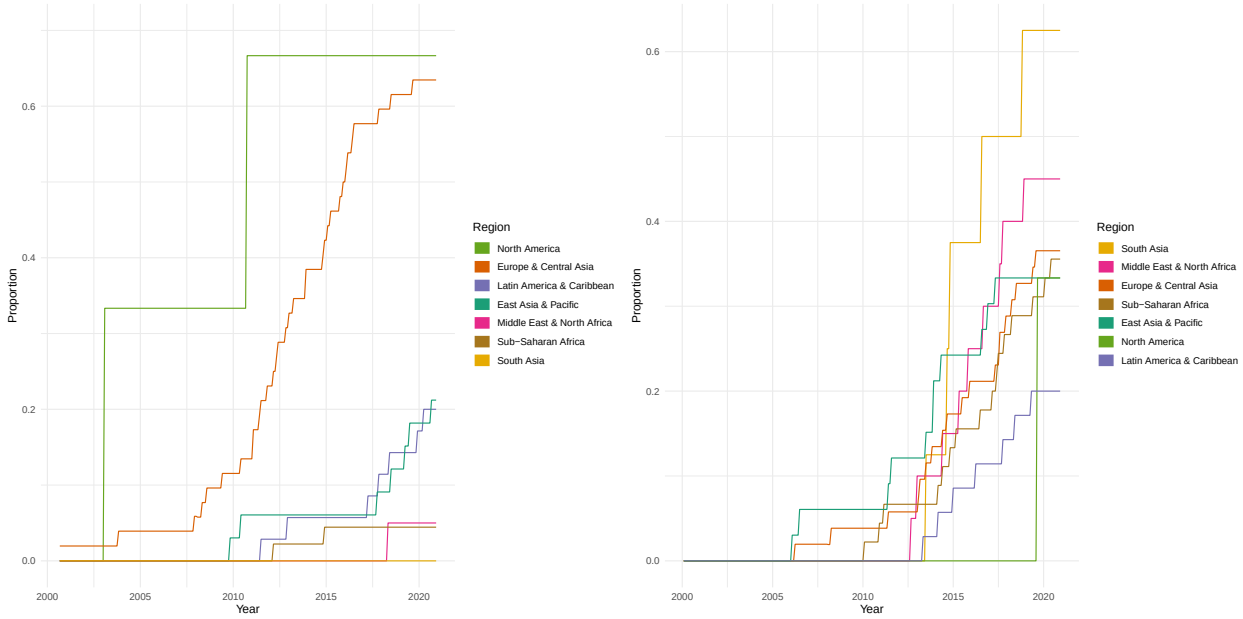
van Deursen, A. and J. van Dijk (2011, September). Internet skills and the digital divide. *New Media & Society 13*(6), 893–911.

Wagner, J. (2017, June). China's Cybersecurity Law: What You Need to Know. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

Waltz, K. N. (1979). *Theory of International Politics* (1st ed ed.). Boston, Mass: McGraw-Hill.

Wamala, F. (2011, September). *The ITU National Cybersecurity Strategy Guide*. Geneva: International Telecommunications Union.

A Appendix



(a) Security Bureaucracy by Region

(b) Technical Bureaucracy by Region

Figure 5: Proportion of Countries with Cybersecurity Doctrine or Policy by Bureaucracy and by Region

Table 3: Cybersecurity Capacity Reviews

Country	Partner	Funder	Date
Jamaica	(OAS)		3/2014
Uganda	(GCSCC/CTO)	United Kingdom	?/2015
Armenia	(GCSCC/WB)		?/2015
Eswatini	(CTO/ITU)		1/2015
Montenegro	(GCSCC/WB)		1/2015
Colombia	(OAS)		1/2015
Fiji	(GCSCC/CTO)	United Kingdom	11/2015
Kosovo	(GCSCC/WB)		2/2015
Bhutan	(GCSCC/WB)		3/2015
Mexico	(OAS)		3/2015
Indonesia	(GCSCC)		6/2015
United Kingdom	(GCSCC)		9/2015
Thailand	(GCSCC/ITU)		?/2016
Senegal	(GCSCC/NL)		1/2016
Sierra Leone	(GCSCC/ITU)		7/2016
Rwanda	(CTO)		8/2016
Madagascar	(GCSCC/ITU)		8/2016
Malawi	(CTO)		1/2017
Mozambique	(CTO)	United Kingdom	1/2017
Tanzania	(CTO)	United Kingdom	1/2017
Tunisia	(GCSCC/GIZ)		1/2017
Zambia	(WB)	United Kingdom, Norway	1/2017
Lithuania	(GCSCC)		4/2017
Kyrgyzstan	(GCSCC/WB)	Republic of Korea	4/2017
Iceland	(GCSCC)		6/2017
Cyprus	(GCSCC)		7/2017
Myanmar	(GCSCC/WB)		8/2017
Georgia	(GCSCC/NRD Cyber Security/FCO)		?/2018
Ghana	(GCSCC/NUPI/WB)	Norway	1/2018
Nigeria	(GCSCC)	United Kingdom	10/2018
Bosnia Herzegovina	(GCSCC/WB)	Republic of Korea	10/2018
Sri Lanka	(GCSCC/WB)		10/2018
Botswana	(WB)	United Kingdom	10/2018
Namibia	(WB)	United Kingdom	10/2018
Mauritius	(WB/GCSCC)	United Kingdom	10/2018
Gambia	(GCSCC/WB)		11/2018
North Macedonia	(GCSCC/WB)	Republic of Korea	2/2018
Brazil	(GCSCC/FCO/OAS)	United Kingdom	3/2018
Samoa	(GCSCC/OCSC/ITU)		4/2018
Benin	(WB)	Japan	4/2018
Liberia	(WB)	Japan	4/2018
Niger	(WB)	Japan	4/2018
Tonga	(GCSCC/OCSC/ITU)		6/2018
Bangladesh	(GCSCC/NRD Cyber Security)		7/2018
Albania	(GCSCC/WB)		9/2018
Ecuador	(NRD)		?/2019
Lesotho	(WB/GCSCC)		?/2019
Switzerland	(GCSCC)	Switzerland	11/2019
Serbia	(WB)	United Kingdom/KWPF	2/2019
Vanuatu	(OCSC/ITU)	Australia - State Government of Victoria	3/2019
Cabo Verde	(WB)	Japan	4/2019
Cameroon	(WB)	Japan	4/2019
Ivory Coast	(WB)	Japan	4/2019
Kosovo	(GCSCC/WB)	Republic of Korea	7/2019
Kiribati	(OCSC)	Australia - State Government of Victoria	7/2019
Papua New Guinea	(OCSC/ITU)	Australia - State Government of Victoria	7/2019
Burkina Faso	(WB)	Japan	7/2019
Micronesia	(OCSC)	Australia - State Government of Victoria	1/2020

Table 4: Cybersecurity Review Survival

	Hazard Ratio
PTA Adoption	0.99989+
	(0.97365)
EIA Adoption	0.96816+
	(0.02646)
Ally Adoption	0.98941+
	(0.09986)
Internet Pct	0.99955+
	(0.96843)
Domestic Expertise	0.84709
	(0.584)
Number of Rivals	0.14185*+
	(0)
Distance Adoption	1.06544+
	(0.16122)
Contiguous Adoption	1.28679
	(0.61063)
Gov. Effectiveness	4.83566*+
	(0)
GDPpc (log)	0.32012*+
	(3e-05)
Population (log)	1.13013+
	(0.13014)
n	13707
n events	57
NPH Prop p¡.05	0
Global NPH Prop p¡.05	0.9076