Public Cyberinstitutions: Signaling State Cybercapacity

by

Nadiya Kostyuk

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Political Science)
in the University of Michigan
2020

Doctoral Committee:

Professor James D. Morrow, Co-chair
Assistant Professor Yuri M. Zhukov, Co-chair
Professor John Ciorciari
Professor Susan Landau
Assistant Professor Tamar Mitts
Professor Nicholas Valentino

Nadiya Kostyuk

nadiya@umich.edu

ORCID iD: 0000-0003-0596-5752

For Anastasia, Valentyna, Joan & Amanda.

Acknowledgments

Over a decade ago I left my family in Ukraine in search of a better education. Many people supported me on this journey and, in particular, during my doctoral studies at the University of Michigan (UoM).

The members of my dissertation committee provided their support, guidance, patience, understanding, and encouragement throughout this process and were flexible in working with me remotely during the dissertation writing process. Most importantly, I thank them for agreeing to supervise a cybersecurity-centered dissertation—a rather novel topic in political science in which none of the committee members specialized. My dissertation tremendously benefited from close supervision of my dissertation chairs, James D. Morrow and Yuri M. Zhukov. I thank Jim for always being available to discuss how my ideas on cybersecurity fit into the larger international relations picture. I thank Yuri for seeing potential in my cybersecurity research during my first year of graduate school when very few considered this an issue worth studying.

John Ciorciari, both as my committee member and as a Director of the International Policy Center at the Ford School, was instrumental in advising me how to advance my ideas within the international policy context. Nick Valentino's positive and welcoming attitude helped me build confidence in my own work. Susan Landau was the best mentor I could have asked for during my pre-doctoral fellowship at the the Fletcher School. From her, I learned

how to write about policy and technology. Tamar Mitts was an invaluable member of my committee when I was moving away from Ann Arbor even though she was going throughout many life transitions of her own.

Besides my committee, I am grateful to many other UoM faculty members whose insight shaped and sharpened my intellectual thinking: Christian Davenport, Lisa Disch, Chris Fariss, Pauline Jones, Nachomi Ichino, Arthur Lupia, Walter Mebane, Robert Mickey, Ragnhild Nordås, and Iain Osgood. My scholarship has tremendously benefited from rigorous discussions at the Conflict & Peace, Research & Development and the Political Economy Workshop. My fellow graduate students at the department—Kiela Crabtree, Yiland Feng, Deanna Kolberg, Bomi Lee, Jieun Lee, Todd Lehmann, Anil Menon, Blake Miller, Steven Moore, Marzia Oceno, Thomas O'Mealia, Anita Ravishankar, Sinéad Redmond, Corina Simonelli, James Stickland, Jessica Sun, Roya Talibova, Michael Thompson-Brusstar, Sasha de Vogel, Carly Wayne, Princess Williams, Alton Worthington, Nicole Wu, Nicole Yadon, and Kirill Zhirkov—also left their intellectual mark on my formation as a scholar and made my time in graduate school very memorable. Lastly, the close friendships that I formed outside of the department with Koustav, Laura, Poonam, Renato, Sampurna, and Thembie were my support systems and kept me intact during difficult times.

My research has also benefited from the support of the Belfer Center for Science and International Technology at Harvard's Kennedy School, the Department of Computer Science and the Fletcher School of Law and Diplomacy at Tufts University, and the Cybersecurity, Internet Governance, Digital Economy, and Civic Tech Initiative at Columbia University's School of International and Public Affairs. Intellectual conversations with Michael Sulmeyer, Ben Buchanan, Trey Herr, Russell Stuart and Ivan Arreguín-Toft helped me better connect my academic research to ongoing policy conversations. Fiona Cunningham and Greg Falco became my life-long friends and made my time in Cambridge unforgettable. Cybersecurity lunches at Tufts University with Jared Chandler, Amanda Current, Kathleen Fisher, Jeff

Foster, Carolyn Gideon, Jeff Taliaferro, and Josephine Wolff sharpened my understanding of the technical side of cybersecurity and taught me how to explain my research to an interdisciplinary crowd.

I must thank my McNair family who I met when participating in the Ronald E. McNair Post-Baccalaureate Achievement Program during my undergraduate studies at John College of Criminal Justice at the City University of New York. Its Associate Director, S. Ernest Lee, introduced me to the American system of education and provided guidance on how I, a new immigrant, could survive in the Big Apple. My mentors, Dr. Peter Romaniuk and Dr. Gail Garfield, introduced me to scientific research and helped me understand that pursuing intellectual curiosity was my calling.

Lastly, I must thank my family—Anna, Adam, and Valentyna—who left their comfortable lives in Ukraine and crossed the ocean to join me in the United States to fulfill our American dream. I am also grateful to my new family that I met in the United States—Michael, Yani, Carol, Dennis, Sean, Kayla, Ryan, Jamie, Richard, Suzanne, Sylvia, Michael, Steven, and Giovanni—who opened the doors of their houses to a complete stranger and made me feel at home. There are no words to describe how grateful I am to my life partner, Jon, who taught me how to appreciate and enjoy my life in the Big Apple, be a true New Yorker, and who has been my rock throughout all these years.

I devote this dissertation to my grandmothers—Anastasia, Valentyna, Joan, and Amanda—who remain puzzled as to why it took me so long to obtain a degree, studying something that they cannot completely understand, but whose wisdom and unconditional love have been guiding me in life.

Contents

List of Figures

List of Tables

Abstract

Even though there has been a rapid increase in state cybercapacity over the last two decades, researchers have paid little attention to this phenomenon. In my dissertation *Public Cyberinstitutions: Signaling State Cybercapacity*, I employ a combination of formal theory, event history analysis, and interviews to shed light on what drives a state's decision to develop this capacity in the form of public cyberinstitutions (PCIs)—publicly observable efforts meant to signal the state offensive and defensive cybercapacity—and the effects these PCIs have on its adversaries' decision-making. Unlike existing scholarship which emphasizes the cyberthreat environment as the main driver of PCIs, I empirically model the international proliferation of PCIs as a diffusion process and argue that it happens through different types of networks. The distinct pathways behind different types of PCIs reflect the different types of signals each is intended to send.

National cybersecurity strategies diffuse through networks of "like-minded" states, with similar preferences on cybersovereignty. The development of a military cyberapparatus diffuses through military alliance networks, following the logic of complementarity. National strategies are among the less costly PCIs a country could adopt, but—because their purpose is to articulate a country's main goals, threats and priorities in the cyber domain—governments cannot adopt them without first considering the role the Internet plays within their polity and how heavily they wish to regulate it. Military cybersecurity units, meanwhile, have higher startup and maintenance costs, and the willingness to pay these costs sends a potentially informative signal to a country's allies and adversaries. Rather than

"free ride" off the cybercapabilities of one's allies, however, countries tend to complement the activities of their allies (e.g., invest more if their allies invest less). I test these theoretical explanations with newly collected data sets on national cybersecurity strategies and on state cybersecurity organizations between 1999 and 2018, and find robust empirical support.

Using an incomplete-information model I also demonstrate that PCIs meant to demonstrate an increase in cybercapacity only deter adversaries that are susceptible to the costs created by this increased cybercapacity. Despite this, states tend to over-invest in PCIs. In particular, weak cyber states tend to over-invest to convince adversaries that they are strong, whereas strong cyber states over-invest so that adversaries do not believe that they are weak states pretending to be strong. In doing so, these states reduce their overall cybercapacity. Through my interviews with cybersecurity experts, intelligence reports, and examples of attempted election interference campaigns, I establish the empirical plausibility of this theoretical result. These findings, which focus on a fundamentally new domain of warfare and statecraft, have important implications for national security policy.

Chapter 1

Introduction

1.1 Public Cyberinstitutions

The Internet is the backbone of the modern economy and modern communications. Billions of people have benefited from the opportunities provided by the adoption of information and communications technologies (ICTs). ICTs facilitate economic growth by increasing the reach of businesses, creating new employment opportunities, and lowering technology and supply costs. ICTs also increase efficiency by enabling more efficient allocation of goods and services and better integration between sales and production. Lastly, ICTs can help with fighting poverty, combating diseases, providing better education, and integrating isolated communities into the global economy.

While societal reliance on the Internet grows, technology remains inherently vulnerable to cyberthreats. Over the last two decades, countries worldwide have experienced an increase in the use of cyberoperations.[1] In 2010, countries learned that for at least two years the Stuxnet worm had been targeting an Iranian nuclear enrichment facility with the purpose

[1] *Joint Publication 3 13 Information Operations* (2014, II-9) define "cyberoperations" as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." Cyberoperations include both cyberespionage campaigns meant to collect intelligence and cyberattacks meant to destruct, damage, or destroy components of Internet-connected devices.

of slowing down the development of the nuclear weapon development program. In 2015 and 2016, Ukrainian power grids suffered cyberattacks that left citizens in the western part of the country and the capital without electricity for a number of hours. In 2017, the WannaCry ransomware attack encrypted more than 300,000 computers worldwide in 150 countries, causing damage in billions of dollars. Figure 1.1 displays targets of large cybercampaigns between 1999 and 2016.

Figure 1.1: *Targets of Major Cybercampaigns (1999-2016)*

The figure displays the distribution of targets of major cybercampaigns between 1999 and 2016. Valeriano and Maness (2018) defines cybercampaigns as an accumulation of cyberattacks meant to achieve strategically important goals. Source: Valeriano and Maness (2018)'s Dyadic Cyber Incidents Dataset (DCID) (version 1.5).

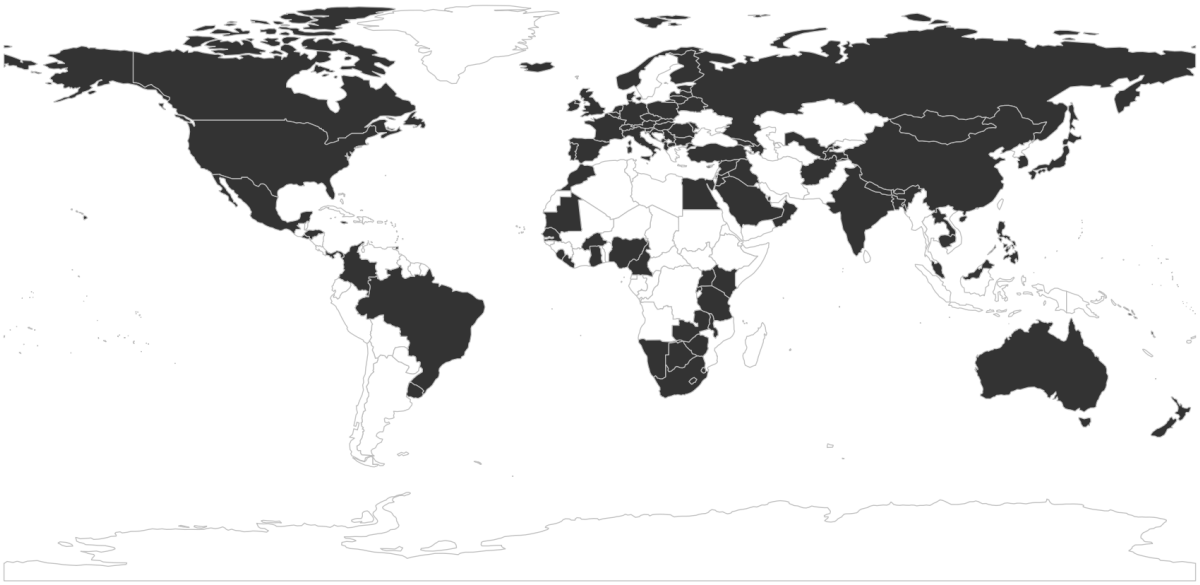
Nations have been taking steps to protect themselves in cyberspace. Some of these steps have been publicly observable. For instance, governments have: adopted new strategies, doctrines, and legislation; created new cybersecurity agencies or assigned cybersecurity responsibilities to existing agencies; and increased intra- and intergovernmental cooperation. I define these efforts as *public cyberinstitutions* (PCI). Figure 1.2a displays

countries that adopted at least one national cybersecurity strategy between 1999 and 2016, and Figure 1.2b displays countries that created at least one agency within its military responsible for cybersecurity. If cybercampaigns that a country has suffered were to drive cybercapacity development, why do we see a disconnect between Figure 1.1 and Figures 1.2a and 1.2b—many more nations have been developing their public cybercapability than those that suffered from large cybercampaigns? If the perception of potential attacks instead drove this development, why do some of the nations seem to lag behind? *What other factors could be driving a country's decision to adopt different types of PCIs? And what effects do they have?*

I view the global spread of cybercapacity as an example of diffusion where a nation's decision to publicly signal its cybercapacity influences other countries to publicly signal similar capacities. In this thesis, I argue that different types of diffusion networks are important for the public development of different types of PCIs. National cybersecurity strategies developed by countries with whom a nation shares preferences on cybersovereignty—a government's desire to exercise control over the Internet within their own borders—capture the diffusion of national strategies. Military cyberapparatuses developed by the nation's allies capture the diffusion of military cybercapacity. To test this theory, I apply an event history analysis to two new datasets on national cybersecurity strategies and state cybersecurity organizations.

In addition to explaining factors that motivate countries to publicly signal their cybercapacity, this dissertation also considers how effective these signals are in deterring adversaries. Using a formal model, I demonstrate that PCIs have a limited effect and deter only those adversaries that are susceptible to the additional costs created by PCIs. Despite that, countries tend to over-invest in PCIs to appear strong. To establish the empirical plausibility of this theoretical result, I use interviews with cybersecurity experts and the example of elections. Section 1.2 further elaborates on my theoretical explanations and the

Figure 1.2: *Distribution of State Cybercapacity (1999-2016)*



(a) National Cybersecurity Strategies

Source: National Cybersecurity Strategies (NCSS) data collected by the author. See Chapter 3 for a detailed description of this data set.

(b) National Military Organizations

Source: State Cybersecurity Organizations (SCO) data collected by the author. See Chapter 4 for a detailed description of this data set.

obtained results in turn.

1.2 Organization of the Dissertation

Chapter 2: Debates over Cybersovereignty as a Driver of the Global Cybersecurity Strategy Diffusion

This chapter explores potential drivers of national cybersecurity strategies—one of the first "public" lines of defense against cyberthreats. The few existing studies that use quantitative analysis tend to prioritize the threat environment as the main driver of state cybercapacity. In particular, Craig and Valeriano (2016*c*) show that a country's Internet dependency and democratic government increases the likelihood that it publishes its national cybersecurity strategy. Unlike existing works, I view the global spread of national cybersecurity strategies as an example of policy diffusion. Using a newly collected data set on national cybersecurity strategies between 1999 and 2018, I demonstrate that nations are more likely to adopt their first cybersecurity strategy if other nations with similar preferences on cybersovereignty have adopted cybersecurity strategies. These preferences matter because they define how governments will exploit the opportunities and address the challenges presented by this new global medium.

Currently, the views on cybersovereignty are split. One group of countries advocates for government control over distinct parts of the Internet whereas another camp prefers a single boundary-less Internet with free flow of information. I argue that before a government adopts its first national cybersecurity strategy, it should decide on the role it envisions for the Internet in its society. Observing the choices made by nations sharing similar views on this subject helps. This theory is robust to a number of alternative explanations and model specifications. By providing the first account of the spread of cybersecurity strategies as an example of policy diffusion, this research helps us better understand how policies spread in the information age.

Chapter 3: Alliances and Complementarity of State Military Cybercapacity

Whereas Chapter 2 outlines a theory of possible drivers of one of the most basic forms of public cyberdefensive capability—national cybersecurity strategies—this chapter attempts to understand how states choose to develop their offensive capabilities. Unlike existing scholarship, which measures these capabilities by cyberattacks and cyberoperations that have been attributed to nation-states, this research instead looks at the global spread of cybercapability in the form of the development of military cyberapparatuses.

Specifically, I distinguish between two ways in which a state can develop its cyberapparatus —assigning cybersecurity responsibilities to an existing agency and creating a new cybersecurity agency. What determines this choice? I argue that it depends on the type of signal a nation wants to send to its allies. If the country's allies signal toughness by creating new units, then the country may not need to do the same and instead assigns cybersecurity responsibilities to an existing military agency. But if the country's allies take a softer approach by assigning cybersecurity responsibilities to an existing military agency, then the country has an added incentive to create a new cybersecurity agency in order to signal toughness. As a result, the responses to allied behavior follow the logic of complementarity. To test this argument, I construct a new cross-national time-series data set on state cybersecurity organizations for the 1999-2018 period. The analysis provides robust empirical support for my theoretical argument.

This important finding demonstrates that the theories of "free riding" in military alliances do not necessarily translate when it comes to military cybercapacity (Olson and Zeckhauser 1966). If they did, they would have predicted (1) the assignment of new responsibilities to be the dominant strategy for all but the wealthiest alliance members, and (2) the smaller the ally, the more likely it is to free ride. As my finding shows, this is not necessarily the case. It is not that easy to free ride on military cybercapabilities of allies. Cyberdefenses are unique to each country and not easily transferable; close allies are often reluctant to disclose information

about their offensive cybercapabilities and/or commit cyberattacks on an ally's behalf (as compared with their willingness to offer military assistance during territorial invasions).

Chapter 4: Deterrence in the Cyber Realm: Public versus private cybercapacity

Having explained the drivers of different types of public cyber institutions (PCIs), Chapter 4 attempts to understand whether this increased capability can indeed deter adversaries. This focus on PCIs presents a significant departure from the existing literature, which primarily focuses on the coercive ability of cyberoperations and argues that it is limited due to the difficulty of attributing the origin of cyberoperations. By developing an institution, a state no longer needs to consider whether its signal might be lost in transmission. Moreover, the state no longer needs to worry about exposing its cybercapability via cyberoperations whose value diminishes after the first use. By developing PCIs, the state can send an immediate signal that allows adversaries to roughly estimate the state's cybercapacity. Can this signal deter adversaries from attacking the state, though?

Using an incomplete-information model, I demonstrate that deterrence works in cases when the adversary is susceptible to the costs created by these PCIs. Despite this limited effect, nations continue over-investing resources into public cybercapacity instead of distributing these resources between PCIs and covert cyberactivity to maximize their overall cybercapacity. This result demonstrates the inefficiency of resource distribution among governments—weak states over-invest to appear strong and strong states over-invest so that they do not appear to be weak states pretending to be strong. Using a series of interviews with cybersecurity experts, intelligence reports, and examples of attempted election interference, I establish the empirical plausibility of this theory. These results echo the findings of Chapter 3—weak cyber nations have an incentive to over-invest in their public capability to appear strong because they cannot always rely on their stronger partners for deterrence.

Chapter 5: Limitations and Future Research

In the concluding chapter of this dissertation, I outline the limitations of this dissertation and a few directions of future research. Since the dissertation primarily focuses on strategic factors in international politics, I plan to incorporate the role of domestic politics, and in particular public opinion, in my future work. How do people perceive the development of PCIs by their own and adversarial governments? Do they feel secure, anxious, or indifferent? For instance, how do Americans perceive the development of information troops by the Kremlin and how, if at all, do they want the U.S. government to respond? Similarly, how do Russians feel about the *U.S. National Cyber Strategy* (2018), which allows the U.S. government to confront its adversary on its home turf and how do they think the Kremlin should respond to this strategy?

By explaining the causes and effects of the initiation of state cyberapparatuses, my dissertation only looks at the tip of the iceberg. The development of cybercapacity is a complex process and involves public-private, inter- and intra-governmental interactions. For my future steps, I plan to take advantage of the datasets on state cybersecurity organizations and policies that I compiled and understand how these complex interactions occur within the government, how they translate into actual capacity, and what implications they have for how states lead their domestic and foreign policies.

1.3 Policy Implications

While each chapter outlines a number of policy implications that pertained to a particular question that it investigates, here I briefly outline just a few most important implications of this dissertation that takes the first stab at an important and novel area of scientific inquiry—state public cybercapacity.

My findings demonstrate that public signaling of cybercapacity might be a double-edge sword. While it can prevent some attacks, it also allows perpetrators to adjust their tactics to exploit new vulnerabilities. We have observed this in practice. For instance, responding to the U.S. government's effort to protect its 2018 elections, Russian bots and trolls adjusted their behavior and started operating during the election off-season (Roeder 2018). These influence campaigns, even if conducted during election off-seasons, shape public opinion and might affect public voting behavior. This cat-and-mouse game, to some extent, echoes the findings from the counter-terrorism literature that demonstrates that while observable counter-terrorism tactics (e.g., security checks in the airports) make people more secure, they are less effective against terror groups who can easily adjust their tactics to more easily achieve their goals (Bueno de Mesquita 2007).

Second, since states tend to over-invest in their public cybercapacity, policymakers should take the signaling of cybercapacity via PCIs with a grain of salt. While PCIs provide them with an immediate—even if rough—estimate of state cybercapacity, policymakers should consider a variety of indicators to accurately assess other nations' cybercapabilities. These indicators might include economic and technological indicators, cooperation with the private sector, reliance on allies, among others. Only having carefully evaluated all these indicators, governments may better evaluate their chances to withstand their enemies and minimize the risk of escalation.

Lastly, my findings hint at how the developments of state cybercapacity can affect future

evolution of state interactions and international politics. While existing military alliances are important for the development of military cybercapacity, my findings demonstrate that reliance on the cybercapacity of military allies is more problematic than it is in the case of conventional capabilities. Cyberdefenses are unique for individual countries and countries are reluctant to use their offensive cybercapabilities on behalf of their allies due to the diminishing nature of these capabilities. However, this might change, given that nations are currently working on synchronizing their capabilities that might improve their overall operational capacity. This development might suggest that future deterrent tactics might involve combination of both conventional military and cyberoperations.

My findings also suggest that in addition to working with their existing partners, countries also define new relationships. Specifically, as the world is currently debating the future of the Internet governance, new (cyber)alliances currently explore the use of cyberspace to define new and redefine old geopolitical spheres of influence. While these new alliances are at the early stages of their development, we are witnessing the birth of a new phenomenon that might have tremendous impact on how nations conduct their domestic and foreign policies.

Chapter 2

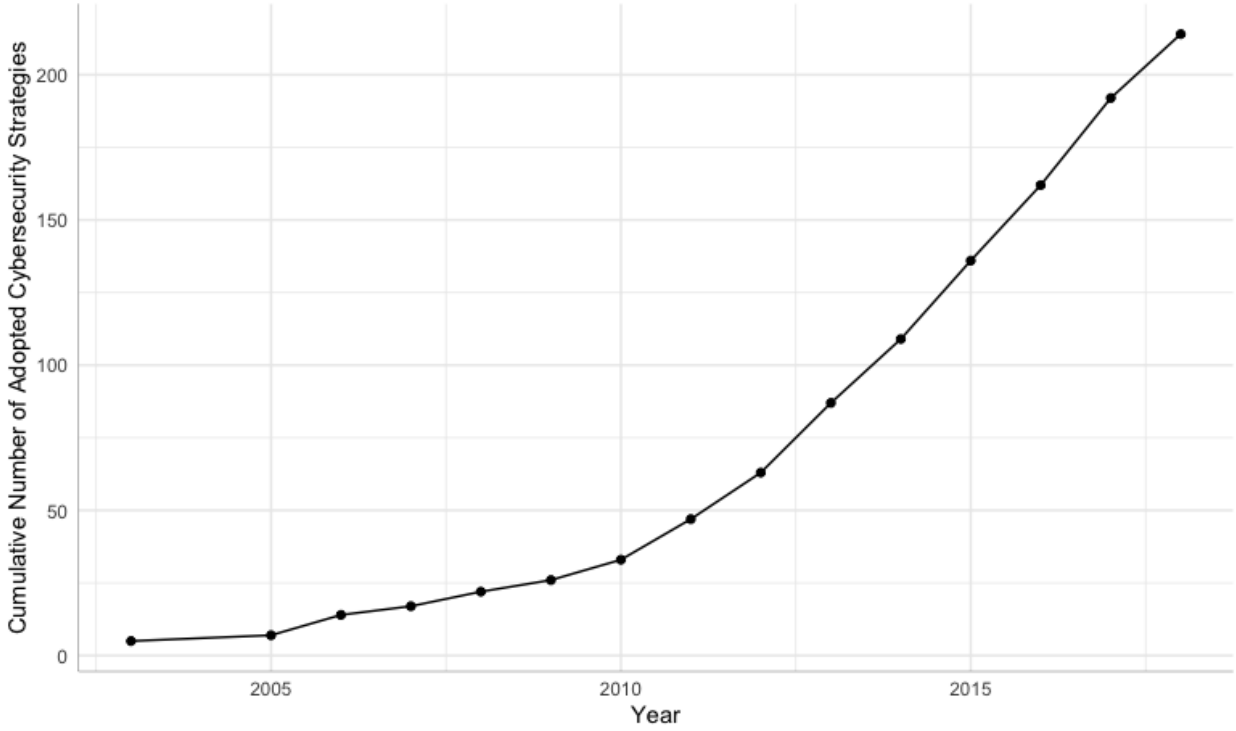
Debates over Cybersovereignty as a Driver of Global Cybersecurity Strategy Diffusion

The last decade has seen an explosion in the number of countries that adopted national cybersecurity strategies. Specifically, by the end of 2010, twenty-seven countries adopted a total of thirty-three strategies (Figure 2.1), whereas over the next eight years, an additional 104 countries adopted 184 new strategies. Despite the centrality and importance of this phenomenon, we know surprisingly little about the factors that drive this policy change.

Existing scholarship views the cyberthreat environment as the main explanation of this development (Craig and Valeriano 2016*a*,*b*,*c*). While cyberthreats have presented a serious concern for national economies and security over the last three decades,[1] I argue that it is not the main defining factor. Instead, I view strategy adoption as an example of policy diffusion in which one government's decision to adopt a strategy influences other governments' decisions to adopt similar strategies. The adoption of cybersecurity strategies—especially the first strategy—motivates governments to think about the role the Internet plays within

[1] The Morris worm—the first computer virus distributed via the Internet—attracted the attention of policymakers as early as 1988. The 1990s experienced an explosion in the number of viruses passing through the Internet as well as cyberespionage campaigns aimed at "surreptitiously snoop[ping] on a user's activity" (Al-Khatib 2016) and the 2000s witnessed a significant number of state-sponsored cyberoperations.

Figure 2.1: *Adoption of National Cybersecurity Strategies over Time*



Source: Author's calculations based on countries' data.

their society, the challenges and opportunities it presents, and whether and how they want to regulate it. Before they make this important decision, I argue that nations observe the choices of other nations that share similar views on this subject.

To test this hypothesis, I apply a Cox-Proportional Hazard model to a newly collected cross-sectional time-series data set of official cybersecurity policies from 1999 and 2018. I measure a country's stand on cybersovereignty using United Nations General Assembly (UNGA) resolution votes on national sovereignty (Voeten, Strezhnev and Bailey 2017). The analysis provides robust empirical support for my theoretical argument. This finding suggests that cyberthreats do not solely drive nations' decisions to adopt policies meant to guide their behavior in this new domain. Instead, new (cyber)alliance politics, which explores the use of cyberspace to (re)define new and existing geopolitical spheres of influence, has an important role to play.

This research helps us better understand how policies spread in the information age. Existing scholarship focuses on the effect of globalization on the spread of liberal economic ideas (Simmons and Elkins 2004), bilateral investment treaties (Elkins, Guzman and Simmons 2006), human trafficking laws (Simmons, Lloyd and Stewart 2018), and technological and military innovation (Pennings and Harianto 1992; Robertson, Swan and Newell 1996; Bitzinger 1994), but it fails to explain the effect of these global changes on the diffusion of policies meant to address the rapid growth and spread of ICTs. By filling this existing literature gap, this analysis makes a substantive contribution to the field of international relations.

This chapter also provides the first account of the spread of cybersecurity strategies as an example of policy diffusion. Most existing works on cybersecurity focus on cybercoercion, explaining how governments use cyberoperations and influence operations against other governments (Borghard and Lonergan 2017; Brantly 2016; Gartzke 2013; Kostyuk and Zhukov 2019; Libicki 2009; Lindsay and Gartzke 2015; Nye Jr 2017; Valeriano and Maness 2018) or use them as tools of repression against domestic opponents (Gohdes 2020, 2014; Lutscher et al. 2020; Roberts 2018; Rød and Weidmann 2015; Weidmann and Rød 2019). The few existing works on the main drivers of cybersecurity policies are comparative (Sabillon, Cavaller and Cano 2016) or country-specific (Osho and Onoja 2015). Lastly, by introducing highly comprehensive cross-national time-series data on national cybersecurity strategies that serve as a proxy of countries' first and basic defensive cybercapabilities, this research serves as an important stepping stone for future research on the causes and effects of state cybercapacity.

2.1 Diffusion of Cybersecurity Strategy

Since the mid-1990s, the Internet has had a revolutionary impact on various aspects of life, including culture, commerce, technology, and communication. The rapid growth of

this global network has contributed to innovation and economic growth, while allowing governments, criminals and other perpetrators to exploit network vulnerabilities. Over the past two decades, countries have started adopting policies to address the impact of the Internet on their societies, leading to the following two questions. Are cyberthreats and economic opportunities the only reasons why countries adopt cybersecurity strategies? What other factors contribute to the spread of these strategies internationally?

A few existing works on this topic argue that a country's cyberthreat environment drives its decision to build better defensive measures in the form of national cybersecurity strategies (Craig and Valeriano 2016*c*,*a*,*b*). The main logic of this explanation builds on the interest-capacity theoretical framework that international relations scholars use to explain the proliferation of conventional capabilities, such as nuclear weapons (Jo and Gartzke 2007), civil space capabilities (Early 2014), and drones (Fuhrmann and Horowitz 2017). In particular, an interest-based explanation focuses on a state's political or strategic needs as drivers of policy adoption, whereas a capacity-based explanation focuses on the state's resources and abilities. Threats to national security—in particular cyberthreats (Craig and Valeriano 2016*c*)—which fall under an interest-based explanation, are one of the main reasons why nations adopt their national cybersecurity strategies.

While a country's threat environment is an important factor to consider, I argue that it does not fully explain the decision to adopt a cybersecurity policy. Instead, I view the global spread of national cybersecurity strategies as an example of policy *diffusion*. Defined as "any pattern of successive adoptions of a policy innovation" (Eyestone 1977, 441), policy diffusion treats the policy adoption by one state as a result of the adoption of a similar policy by another state. Globalization has made it easier for national leaders to share their ideas, observe how others respond to similar challenges, while learning from their errors.

I further theorize that a nation is motivated to adopt its first cybersecurity strategy when other nations with similar preferences on "cybersovereignty" have adopted cybersecurity

strategies. The term "cybersovereignty" or "splinternet" describes a government's desire to control the part of the Internet within its own borders. Currently, there are two camps of nations with distinct views on cybersovereignty. The anti-cybersovereignty group of countries, led by the United States, advocates for a single Internet, arguing that any division of this medium into smaller components will derail the whole purpose of this global web meant to connect everyone. Governments in the pro-cybersovereignty camp, led by Russia and China, argue that state control over the Internet will allow them to better protect their citizens against cyberthreats and insulate online communications from foreign disruption and interference. In particular, Russia argues that such control is necessary to protect its population from external threats. Such control, however, will also allow them to monitor dissent and restrict the free flow of information.

A government's stand on cybersovereignty determines how it chooses to exercise control over the Internet for years to come. Given the tremendous importance of this subject affecting each country's national security, economy, and development, countries have passionately debated cybersovereignty on the floor of the United Nations General Assembly (UNGA). In 2010, the United States submitted its resolution, advocating for "possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information" (A/RES/63/41 2010, 2). The following year, Russia and China (along with Tajikistan and Uzbekistan) presented their resolution, advocating for a new international code of conduct for information security that should comply with the UN Charter and respect states' sovereignty and territorial integrity (A/66/359 2011).[2]

States have also been vocal about their position on cybersovereignty in their replies to UNGA resolutions on "Developments in the field of information and telecommunications in the context of international security." For instance, Germany advocated for cyberspace to be "a public good and a public space" (A/66/152 2011, 9), whereas Greece favored "....the

[2] Russia submitted the first, although rather general, resolution on the topic of information and telecommunications in the field of information security in 1998 (A/RES/53/70 1998).

requirement for a nation to preserve its sovereignty and maintain its own base of information" (A/66/152 2011, 11-12). In its September 2014 reply to UNGA resolution A/RES/ 68/243 (2013), France reiterated its anti-cybersovereignty view by stating that the country "does not use the term 'information security,' preferring the terms 'information systems security' or 'cybersecurity.' As an active proponent of freedom of expression online...France does not consider information as such to be a potential source of vulnerability requiring protection, except under conditions strictly established by law, in a proportionate and transparent way, in accordance with article 19 of the International Covenant on Civil and Political Rights" (A/69/112/Add.1 2014, 3). Responding to UNGA resolution A/RES/71/28 (2016), Belarus expressed its pro-cybersovereignty view, "...it is crucial to gradually advance the principle of non-interference in the internal affairs of sovereign States and mutual rejection of aggressive actions in the information sphere. Such steps should principally be achieved through support of the information sovereignty of United Nations Member States..."(A/72/315 2017, 6).

I argue that the adoption of national cybersecurity strategies by nations that share similar views on cybersovereignty—so-called *cybersovereignty partners*—provides information on the costs and benefits of developing similar strategies for nations that have no cybersecurity measures in place. These strategies also help nations build certain international reputations because when adopting a national cybersecurity strategy, nations tend to place themselves in one of the two cybersovereignty camps.

Before designing their strategies, nations understand that they are not able to eradicate cyberthreats alone—international cooperation remains vital. To make this cooperation successful, nations need to make their domestic cybersecurity apparatuses comparable with those of their partners. Before developing a cybersecurity strategy, a government needs to understand to which extent it prefers regulating the Internet in their polity. As a result, it looks at the strategies of nations that have similar preferences on this topic. Having developed a cybersecurity strategy, a nation signals to its partners its readiness to contribute to joint

efforts in addressing cyberthreats. As a result, I derive the following hypothesis to test my claims:

- **Hypothesis:** *If a country shares the same view on cybersovereignty with other nations that adopted national cybersecurity strategies in year $t-1$, then the country is likely to adopt its first national cybersecurity strategy in year t.*

2.2 Additional Alternative Explanations

In addition to considering a country's threat environment as one of the alternative explanations of cybersecurity strategy adoption (Section 2.1), I also consider a number of alternative explanations, such as *cultural similarity*, *communication channels and expert communities*, *harmonization after partners*, and *legitimacy or modern behavior*, and *regime type*. Section 2.5 demonstrates that none of these alternative explanations affect a country's choice to adopt its first cybersecurity strategy.

Alternative Explanation #1: Cultural Similarity

When developing policies, countries tend to learn from the successes and failures of culturally similar nations that have already adopted such policies (Rogers 1995; Simmons and Elkins 2004). As Figure 2.2 demonstrates, cultural proximity could indeed be a driver of cybersecurity policy. Not only is it easy for a nation to look at the policies of countries that use the same or similar (official) languages, it also ensures that various terms related to cybersecurity are not lost in translation. For instance, instead of cybersecurity, some countries use the term "information security" which emphasizes protecting information—its confidentiality, integrity, and availability. Simply substituting the broader term of "information security" with the much narrower term of "cybersecurity," meaning security of Internet-connected devices, in a national cybersecurity strategy might leave a nation

unable to execute its proposed defense plan and send a misleading signal to its domestic and international audiences.

While cultural similarity is an important factor for to consider, I argue that it is not a defining factor for the adoption of a cybersecurity policy, in particular. Globalization has created a world in which average citizens, and especially policymakers, speak multiple languages and travel extensively for work, both domestically and internationally. The Internet allows people to connect to almost any part of the world from their living-rooms within a matter of seconds. As a result, policymakers can choose to examine the policies of culturally-similar nations, as well as the policies of other, more far-flung, countries that are less similar to their own.

Alternative Explanation #2: Communication Channels and Expert Communities

The exchange of information among connected actors is a driving force behind diffusion of various sociological processes (Axelrod 1997; Rogers 1995). There is a great diversity of forums where this exchange can take place. Think-tanks, research institutes, and intergovernmental organizations (IGOs) are examples of forums that play significant roles in the spread of policies between governments (Brooks 2005; Füglister 2012; Stone 2004; Ward and Cao 2012). There has been a rapid increase in the number of bilateral and multilateral intergovernmental meetings over the last decade, during which governments exchanged knowledge and ongoing research devoted to various aspects of cybersecurity (Kostyuk 2020*b*). The exchange of information at these meetings could potentially explain global cybersecurity strategy diffusion.

Alternative Explanation # 3: Harmonization after Partners

To consider harmonization as a driver of strategy adoption (Bennett 1991), I consider the possibility that a country adopts its cybersecurity strategy in reaction to its so-called partners. I consider three groups of partners: (1) military allies; (2) trading partners; and

(3) United Nations partners (i.e., nations that vote similarly on United Nations General Assembly (UNGA) resolutions).

Countries sign long-term pacts to fight against common threats in physical and (now) virtual domains (Leeds, Long and Mitchell 2000; Marinov, Nomikos and Robbins 2015). Since states cannot avoid cooperation with their allies on cybersecurity and they absolutely pay attention to what more advanced alliance members are doing, some might argue that countries might adopt their strategies after their military allies. Similar to military capability, cybersecurity strategies signal the level of a country's defensive capability because they outline a set of measures that a nation plans to implement to protect itself from cyberthreats. But these measures are defensive in a broad sense, covering various aspects of everyday life (e.g., educating the public about proper cyberhygeine), technical means to protect Internet-connected devices, and joint research projects and international cooperation aimed at exchanging knowledge, resources, and assistance in order to increase national cybercapacity. All these steps are more basic and less resource- and expertise-intensive than the syncronization of state military cybercapacibilities with allies—a more advanced step in the process of state cybersecurity-apparatus creation—and this is not where nations generally start.

Since foreign policy interests are influential in alliance formation (Gibler and Rider 2004), some might argue that such interests might extend outside of military alliances to other non-military partnerships that also shape foreign policy preferences, such as voting blocs formed in the UNGA and trading partners. UNGA votes that measure preference similarities are generally described as cheap talk (especially given a non-biding nature of the UNGA resolutions) that reflect pre-existing coalitions and alliances (Farrell and Gibbons 1989; Voeten 2005). Moreover, they cover preferences on a variety of issues, not related to cybersecurity. Even though resolutions on "Developments in the field of information and telecommunications in the context of international security" have occupied the UNGA floor

since 1998 (A/RES/53/70-A/RES/74/29), they have either been adopted with a consensus or with almost no variation in voting (e.g., the United States was the one country to vote "no" on A/RES/63/37, which had 178 "yes" votes). This is not surprising, given that these resolutions contain rather vague language about threats presented by cyberspace when used by criminal and terrorist groups and the call for international cooperation meant to address these threats. As a result, I expect that there is no correlation between cybersecurity strategies by a country's so-called UNGA partners and the country's choice to adopt its strategy.

Lastly, I consider an impact of the country's trading partners. Given that cybercrime is a serious threat to international trade and e-commerce,[3] some might argue that a cybersecurity strategy signals to a country's trading partners that the government takes cybercrime seriously and is working on its eradication. But before designing an approach to fight cyberthreats, the government should decide how it views the Internet—single or divided—because this fundamental decision will determine the approach it designs.

Alternative Explanation # 4: Legitimacy or Modern Behavior

Modern organizations and institutions often come to resemble each other, not because of competitive selection or rational learning, but because institutions mimic each other (Meyer and Scott 1992; Powell and DiMaggio 1991). Using this "new institutionalism" perspective and applying the state-isomorphism idea (Finnemore 1996; Ramirez and Boli 1987), some might argue that national cybersecurity policies serve a similar role to national flags, airlines, and Olympic teams, as they have a lot of "symbolic throw-weight" (Selznick 1949; Suchman and Eyre 1992). Cybersecurity policies that are deemed appropriate by powerful leaders might signal "modern behavior" (Sagan 1997) and the fulfill a government's need to appear

[3] Close to $600 billion USD or about one percent of the global Gross Domestic Product (GDP) is lost to cybercrime each year (Lewis 2018). Major economies remain the main victims to cybercriminals who leverage black markets and digital currencies and adopt new technologies to fill their pockets (Cook 2017).

legitimate in the eyes of its constituency and the international community (Fordham and Asal 2007).

Alternative Explanation # 5: Regime Type

I consider two possible effects of regime type. First, public fears stemming from large cyberincidents may drive a state's decision to adopt cybersecurity policies; these observable national responses might make voters feel secure and guarantee leaders' reelection (Gelpi, Reifler and Feaver 2007; Gronke, Koch and Wilson 2003). Alternatively, cybersecurity can be a public good at the national level if the government provides it through enforcement or deterrence.

Second, since states with similar identities—regime type in this case—tend to co-ally, cooperate with each other, and learn from each other (Gartzke and Weisiger 2013; Lai and Reiter 2000; Smith 1995), some might argue that countries with the same regime type are more likely to follow each other's lead on a cybersecurity strategy adoption. But cybersovereignty preferences are not simply a proxy for regime type. For example, Greece, which is a democracy, prefers having control over the Internet. In its 2011 reply to the 2010 UNGA A/RES/65/41, Greece stated, "National sovereignty rights regarding information security in global information sharing should be maintained...." (A/66/152 2011, 11-12).

2.3 Data

Dependent Variable: National Cybersecurity Strategies. I focus on the adoption of cybersecurity strategies because they define the first and main efforts that national leaders take to develop defensive responses to cyberthreats. They also signal to domestic and international communities the significance a country's leadership attributes to cybersecurity. These strategies generally: express "high-level objectives, principles and priorities that guide a country in addressing cybersecurity"; describe the steps that the country will undertake

to achieve these objectives; list the stakeholders responsible for undertaking these steps; and set the country's cybersecurity agenda over the next few years (generally five years) (InternationalTelecommunicationsUnion 2018, 13).

More importantly, cybersecurity strategies, especially the first-adoptions, motivate governments to examine the role that the Internet plays in their society, the challenges and opportunities it presents, and whether and how governments want to regulate it. The existing views on this issue are split. On the one hand, there are countries that want to have a single Internet and believe that no single government should regulate it. On the other hand, there are those that want to split the Internet into smaller parts, each of which will be under control of a specific government. While there are still a number of undecided nations in the middle, a number of countries that belongs to either camp has been rapidly growing.

Depending on how countries view cybersovereignty, they use different terms to define Internet security. Anti-cybersovereignty nations generally use "cybersecurity" and pro-cybersovereignty nations generally use "information security." The former, narrower concept focuses on protecting vulnerabilities through ICTs whereas the latter, broader term includes information protection, including its confidentiality, integrity, and availability (CIA). As mentioned in Section 2.1, countries emphasize this important but striking difference in their statements to the UNGA. They also carefully choose between these two terms when crafting a name for their national strategies meant to address challenges and opportunities presented by ICTs and the Internet. For instance, many Western nations that favor *cybersecurity* refer to these policies as *national cybersecurity strategies*. Countries that favor *information security* tend to refer to these policies as *information security strategy* and *information and communication technology strategy*, among others. Sometimes, countries combine both concepts in their strategy names as Sri Lanka did in its 2018 Information and Cyber Security Strategy.

In addition to the choice between *cybersecurity* and *information security*, the choice

between *policy*, *strategy*, *(action) plan*, and *roadmap* further distinguishes the document names of various countries and complicates the selection criteria according to which the documents should be sorted in the final data set. While Western nations first adopt strategies that guide future policy, this characteristic does not seem to apply universally, at least not from the English translation of the document names. To ensure that my sample includes only the most relevant documents, I consulted country experts and databases of national cybersecurity strategies created by international organizations, such as the ITU, NATO Cooperative Cyber Defence Centre of Excellence, and the United Nations Institute for Disarmament Research.

Using this process, I have collected a highly comprehensive data set of national cybersecurity strategies (NCSS) adopted between 1999 and 2018. My data set has 223 strategies adopted by 132 nations. While most countries adopted only one strategy as of 2018 some countries adopted and revised multiple strategies during this time frame (e.g., Luxembourg has three strategies). These additional strategies are relevant for constructing weighted average effects of my main independent variable and diffusion variables, mentioned in Section 2.2.

My dependent variable is the adoption of the first national cybersecurity strategy (`Adoption`). Countries are coded as a "1" if they enacted such a strategy.[4] Figure 2.2 displays the global spread of cybersecurity strategy over time. Similar to Figure 2.1, Figure 2.2 shows rapid strategy diffusion starting in 2010. Specifically, by the end of 2009, only twenty-two nations had cybersecurity policies for a total of twenty-six policies; by the end of 2014, forty-seven nations adopted a total of 109 policies; and by the end of 2018, 132 nations adopted a total of 217 policies.

Main Explanatory Variable: Preferences on Cybersovereignty. Cybersovereignty,

[4] NCSS records the date, month, and year when a strategy was adopted. If information about date and month is not available, I assume that the strategy was adopted on January 1.

Figure 2.2: *Diffusion of Cybersecurity Strategies (2000-2018)*

(a) 2000-2009

(b) 2000-2014

(c) 2000-2018

which has been discussed for about a decade, is a relatively new concept for the UNGA. However, national (non-cyber) sovereignty occupied the UNGA floor from 1989 until 2005 in resolutions on "Respect for the Principles of National Sovereignty and Non-Interference in the Internal Affairs of States in their Electoral Processes" (A/RES /44/147-A/60/164). Similarly to the resolutions and statements on cybersovereignty these resolutions stressed the importance to respect "the principles of national sovereignty and non-interference in the internal affairs of any State" (A/RES/52/199 1997, 2). Even though these resolutions paid particular attention during election periods, they advocated for "the right, freely and without external interference, to determine [a country's] political status and to pursue their economic, social and cultural development" (A/RES/52/199 1997, 2). Fast-forward twenty year. States now argue for the same right to "freely and without external interference, to determine," but this time how to govern the Internet and conduct ICT-related activities.

I use a country's view on national sovereignty—its votes on UNGA resolutions on the topic of national sovereignty—as a proxy for the country's preferences on cybersovereignty. Specifically, I record instances in which one country voted "yes" on a UNGA resolution and another country voted "no" on the resolution. I assign a "1" if a dyad has different cybersovereignty preferences and a "0" if the dyad has the same cybersovereignty preferences. Since resolutions on national sovereignty appeared at the UNGA for the last time in 2005 (making 2006 the last available year for the lagged variable), I use the votes from this last year to fill the data for the remaining years (2007-2018), given that the state preferences on domestic and foreign policy issues tend to be rigid (Cordell et al. 2020; Voeten, Strezhnev and Bailey 2017).[5] Because the measure for similar preferences does not meet the proportionality

[5] Cordell et al. (2020) demonstrate that human rights reporting in the U.S. Department of State reports changed with a change in presidential administration. Voeten, Strezhnev and Bailey (2017) demonstrate that the language for many UNGA resolutions does not change much within a few consecutive years. The language of the resolutions on "Developments in the field of information and telecommunications in the context of international security" that occupied the UNGA floor since 1998 barely changed (A/RES/53/70-A/RES/74/29). Moreover, the voting patterns on these resolutions barely changed—the resolutions were either adopted with consensus or with almost no variation in voting.

assumption of the Cox-Proportional Hazard model that I employ in my analysis, I use the measure of dissimilar cybersovereignty preferences to create a weighted average effect of cybersecurity policies adopted by countries that do not share similar preferences on cybersovereignty in a period prior to the country adopting its first cybersecurity strategy (`Policies Weighted by Cybersovereignty Opponents`).[6]

Operationalizing Alternative Explanations. Given two nations, I measure their cultural similarity using: (1) a binary variable that records whether the nations have the same official language from Graham and Tucker (2019) (`Linguistic Partners`), (2) a binary variable that records whether they have similar colonial experiences from Graham and Tucker (2019) (`Colonial Partners`), and (3) a continuous variable that records the distance between the nations' capitals (`Neighbors (1)`).[7] To account for the impact of information channels, I use the nations' joint membership in international governmental organizations (IGOs) from Pevehouse et al. (2019) (`IGO Partners`). To identify their military allies, I use Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions (ATOP) data (`Allies (1)`) and the Correlates of War (COW) Project's data on formal alliances (version 4.1) (Gibler 2008) (`Allies (2)`). I identify each country's trade partners using: (1) bilateral trade data from the World Bank (`Trading Partners (1)`); (2) data on bilateral investment treaties from Graham and Tucker (2019) (`Trading Partners (2)`); and (3) preferential trade agreements from (Graham and Tucker 2019) (`Trading Partners (3)`). To account for the possibility that a state's foreign policy preferences drive strategy adoption, I use Voeten, Strezhnev and Bailey (2017)'s data on the UNGA votes (`UN Partners`). I measure the effect of modern behavior as a driving force of strategy adoption using each country's average membership

[6] The measure for similar preferences does not meet the proportionality assumption of the Cox-Proportional Hazard model even after interacting this measure with the starting time to address this issue; moreover, the measure for similar preferences is highly correlated with many other types of diffusion variables. See Section 2.7 of Appendix 2.7 for more details.

[7] I run my robustness checks using a dummy variable indicating whether states share a land border or are separated by less than 400 miles of water from (Stinnett et al. 2002) (`Neighbors (2)`).

in IGOs from Pevehouse et al. (2019) (`IGO Membership`). To account for the effect of the conventional front on strategy adoption, I control for the total number of militarized interstate disputes that a country experienced in the year preceding its strategy adoption from Maoz (2005) (`Total MIDs`). I measure each country's threat environment using: (1) the number Internet users in the country as a percentage of the country's total population, taken from the World Bank (`Int_Users`),[8] (2) the cumulative number of large, known cybercampaigns that the country experienced in all years preceding its strategy adoption from Valeriano and Maness (2018)'s Dyadic Cyber Incident Dataset (DCID) (version 1.5) (`Target`),[9] and (3) strategies adopted by the country's adversaries (`Adversaries`). Lastly, I account for each country's regime type. Using Gurr, Marshall and Jaggers (2010)'s Polity IV score, I create a dummy variable that takes the value of 0 if this score is less than six, which represents an autocracy, and 1, if this score is at least six, which represents a democracy (`Democracy`). I use this variable to account for the effect of regime type similarities on strategy adoption (`Regime Partners`). Section 2.7 of Appendix 2.7 provides a detailed explanation of these variables and their variations.

Control Variables. In addition to considering the effect of the variables that I outlined in Section 2.2, I control for two other factors. First is the country's wealth measured by the country's GDP per capita, taken from the World Bank (`GDP_PerCapita`).[10] Second is the cumulative number of large, known offensive cyberoperations launched by (attributed to) a country in all years preceding its strategy adoption, taken from from DCID (`Attacker`).[11]

[8] I use logarithmic transformations to address this variable's skewness.

[9] Valeriano and Maness (2018) define a cybercampaign as an accumulation of cyberattacks meant to achieve strategically important goals.

[10] I use logarithmic transformations to address this variable's skewness. It is worth noting that `GDP_PerCapita` only considers a country's wealth. Future extensions of this work will incorporate the extent to which the type of economy (e.g., extractive) affects the calculations regarding security.

[11] Table 2.1 lists all variables, their measures and sources. As Table 2.1 demonstrates, the data on some of the variables ends around 2014 or even earlier (e.g., 2010 for `Strategies Weighted by Adversaries`). One way to address this data limitation would be to limit my analysis to 2014 or even 2010. This option would require the analysis to cover the less interesting times of international cyberconflict. I decided to

Table 2.1: *Variables and their Sources Included in the Analysis*

Mechanism or Concept	*Measure*	*Variable Name*	*Covered Period*	*Data Source(s)*
Cybersovereignty Preference Similarity	Weighted average effect of the strategies adopted by countries with different preferences on cybersovereignty in a period prior to the strategy adoption	`Strategies Weighted by Cybersovereignty Opponents (lag,sc)`	1999-2018	UNGAV; NCSS
Communications Channels	Weighted average effect of the strategies adopted by governments that have a joint membership in various IGOs with a nation in a period prior to this nation's strategy adoption	`Strategies Weighted by IGO Partners (lag,sc)`	1999-2014	IGOs; NCSS
Cultural Similarity	Weighted average effect of the strategies adopted by colonial partners in a period prior to the strategy adoption	`Strategies Weighted by Colonial Partners (lag,sc)`	1999-2018	WPED; NCSS
	Weighted average effect of the strategies adopted by linguistic partners in a period prior to the strategy adoption	`Strategies Weighted by Linguistic Partners (lag,sc)`	1999-2018	WPED; NCSS
Harmonization	Weighted average effect of the strategies adopted by a nation's neighbors in a period prior to this nation's strategy adoption	`Strategies Weighted by Neighbors (1) and (2) (lag,sc)`	1999-2016 1999-2018	COWConti-guity; R; NCSS
	Weighted average effect of the strategies adopted by a nation's allies in a period prior to this nations' strategy adoption	`Strategies Weighted by Allies (1) and (2) (lag,sc)`	1999-2016 1999-2012	ATOP; COW NCSS
	Weighted average effect of the strategies adopted by a nation's trading partners in a period prior to this nations' strategy adoption	`Strategies Weighted by Trading Partners (1), (2),and (3) (lag,sc)`	1999-2014 1999-2018 1999-2017	WB; WPED; NCSS
	Weighted average effect of the strategies adopted by a nation's UN partners in a period prior to this nations' strategy adoption	`Strategies Weighted by UN Partners (lag,sc)`	1999-2014	UNGAV NCSS
Legitimacy & Modern Behavior	A nation's average membership in IGOs in a period prior to this nation's strategy adoption	`IGO Membership (lag,sc)`	1999-2014	IGOs
Regime Similarity	Weighted average effect of the strategies adopted by countries with the same regime type in a period prior to the strategy adoption	`Strategies Weighted by Regime Partners (lag,sc)`	1999-2016	Polity IV; NCSS
Threat Environment	Cumulative number of large cyberattacks that a country has been a target of in all preceding periods prior to the policy adoption	`Target (lag,sc)`	1999-2016	DCID
	Cumulative number of large cyberattacks that has been attributed to a country in all preceding periods prior to its strategy adoption	`Attacker (lag,sc)`	1999-2016	DCID
	Number of Internet users as a percentage of a country's population	`Int_Users (log,sc)`	1999-2017	WB
	Cumulative number of militarized interstate disputes that a country experienced in a period prior to the strategy adoption	`Total MIDs (log, lag,sc)`	1999-2010	MIDs
	Weighted average effect of the policies adopted by a nation's rivals in a period prior to the nation's policy adoption	`Strategies Weighted by Adversaries (lag,sc)`	1999-2010	MIDs; NCSS
Control Mechanisms	GDP per capita	`GDP_PerCapita (log,sc)`	1999-2018	WB
	A binary variable identifying whether a country is a democracy	`Democracy`	1999-2016	Polity IV

Variable Name: `log`: logarithmized; `lag`: lagged; `sc`: standardized; **Sources:** *ATOP:* Alliance Treaty Obligations and Provisions (Leeds et al. 2002); *COW:* Correlates of War (Gibler 2008); *COW Contiguity:* COW Direct Contiguity Data (Stinnett et al. 2002); *DCID:* Dyadic Cyber Incident Dataset (Valeriano and Maness 2018); *IGOs:* Intergovernmental Organizations (Pevehouse et al. 2019); *MIDs:* Militarized Interstate Disputes data (Maoz 2005); *NCSS:* National Cybersecurity Strategies dataset, collected by the author using official governmental sources; *Polity IV score* (Gurr, Marshall and Jaggers 2010); *R:* calculated using `R` software package; *UNGAV:* United Nations General Assembly Voting Data (Voeten, Strezhnev and Bailey 2017); *WB:* World Bank; *WPED:* World Economics and Politics Dataverse (Graham and Tucker 2019)

2.4 Empirical Strategy

Spatial lags. To identify the effect of the strategies adopted by a country's "neighbors" that include but are not limited to its adversaries, allies, cultural and linguistic partners, I create spatial lags. Instead of lagging the value of the dependent unit one variable at a time and, as a result, adding a significant number of regressors to my model, I use spatial lags that capture the "weighted average of the dependent variable in the actor's 'neighborhood"' (Simmons and Elkins 2004, 178). I define a spatial lag for a country i as:

$$W_i([t-1]) * y_{-i}([t-1]) = \sum_{i=1,\ldots,N} W_{i,-i}([t-1]) * y_{-i}([t-1]), \tag{2.1}$$

where, $W_{i,-i}([t-1])$ is an $N \times N$ spatial weights matrix that capture's countries i's neighborhood in $t-1$. Each element in $W_{i,-i}$ measures different relationships between any two nations. For instance, it could measure physical distance between two nations' capitals (`Neighbors`), how much trade the two nations do (`Trading Partners`), or whether they signed a military alliance treaty (`Allies`). $\sum_{i=1,\ldots,N} W_{i,-i}$ captures the weight of the relationship between these two nations relative to the nation's total relationships with other nations in a given area of international relations. This weight captures the importance of a neighbor's influence on this country. For instance, if a nation has only one trading partner, then their trading relationship has a weight of 100%; consequently, the partner will most likely have a significant influence on this country's economic decisions. On the other hand, if a nation has twenty trading partners and each relationship has a weight of 5%, then the influence of an individual trading partner on the country's economic decisions will most likely be limited. $y_{-i}([t-1])$ represents whether a country's "neighbor" $-i$ adopted a cybersecurity

proceed with my analysis as the development of cybersecurity policies is too important of a contemporary policy topic to ignore. Instead of limiting my strategy sample, I extend data for my covariates all the way until 2018, using the previous values of these covariates. While this approach has its pros and cons (Van Buuren 2018), I decided to use it, as it makes it easy to track the various moving parts of my analysis.

strategy in year $t-1$. Combined, $W_i([t-1]) * y_{-i}([t-1])$ captures the total effect of the country's "neighbors" that adopted or did not adopt cybersecurity strategies in $t-1$.

Event history analysis: Cox Proportional-Hazards model. I use an event history model[12] that focuses on the spell of time until the adoption of a national cybersecurity strategy occurs. My unit of analysis is the country-year. The analysis begins in 1999 when the U.S. government started investigating a massive data breach of classified information. Called *Moonlight Maze*, this data breach affected various U.S. government agencies and defense contractors and was later labeled as the first example of an advanced persistent threat (APT)—a stealthy computer network operation during which a state-sponsored group gains unauthorized access to a computer network and remains undetected for some time. The analysis ends in 2018. If the country has not adopted a cybersecurity strategy by December 31, 2018, it is right-censored in my data set. Lastly, since many of the covariates change over time, I use interval censoring to capture time-varying covariates (Therneau and Grambsch 2000).

I fit the following Cox Proportional-Hazards (CPH) model that examines the effect of time-varying and time-invariant covariates on the country's decision to adopt the policy:

$$log(H(t; X_i([t-1]), y_i([t-1]))) \propto W_i([t-1])y_{-i}([t-1])\beta_1 + X_i([t-1])\beta_2,$$

where: $log(H(t; X_i([t-1]), y_i([t-1])))$ is the log of a hazard ratio that stands for the relative risk of country i adopting a cybersecurity strategy at time t; $W_i([t-1])y_{-i}([t-1])$ is an $n \times n$ spatial weights matrix, as explained above; $X_i([t-1]) = [x_{1i}([t-1]), \ldots, x_{ki}([t-1])]'$ is a matrix of k exogenous variables; and β_2 is a three-dimensional vector of coefficients. As explained earlier, I included the following exogenous variables: (1) the number of the country's Internet users as a percentage of its total population in a given year (`Int_Users`);

[12] Event history models became a common tool for studying policy diffusion (Berry and Berry 1990; Elkins, Guzman and Simmons 2006; Simmons and Elkins 2004; Simmons, Lloyd and Stewart 2018).

(2) the country's GDP per capita in a given year (`GDP_PerCapita`); and (3) the country's regime type (`Democracy`). I also use robust standard errors with clustering on the countries to account for time-varying coefficients. Lastly, to make my results easy to interpret, I standardize all continuous explanatory variables (all variables except `Democracy`).[13]

2.5 Findings

My central finding is that the cybersecurity strategies adopted by countries that share the same preferences on cybersovereignty most consistently explain global cybersecurity strategy diffusion. Tables 2.2-2.5 that display hazard ratios demonstrate that coefficients for `Strategies Weighted by Cybersovereignty Opponents` are consistently smaller than one meaning that `Strategies Weighted by Cybersovereignty Opponents` are negatively correlated with `Adoption`.

Table 2.2 considers the influence of `Strategies Weighted by Cybersovereignty Opponents` on a country's threat environment; it demonstrates that `Strategies Weighted by Cybersovereignty Opponents` is consistently negatively correlated with `Adoption`, even after controlling for different proxies of the cyberthreat environment. This result supports the argument that as a country starts building its defensive cybercapabilities in the form of national cybersecurity strategies, it is influenced by nations that share its preferences on cybersovereignty. It does so because its national cybersecurity strategy—the first significant document that the country adopts on the topic of cybersecurity—sets up the government's future program on how it will address challenges and opportunities presented by the Internet.

In particular, Model 2 in Table 2.2 uses `Target`—the cumulative number of large, known cybercampaigns attributed to the country in all years preceding its strategy adoption —as a proxy for the cyberthreat environment. The model demonstrates that `Target` is not correlated with `Adoption`. This is not surprising, given that large cybercampaigns are rare

[13] Section 2.7 of Appendix 2.7 provides a detailed explanation of diagnostic tests for non-proportional hazards.

Table 2.2: *Influence of strategies of cybersovereignty opponents and threat environment on national strategy adoption (hazard ratios)*

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*
	Base	`Target` *as proxy for cyberthreat environment*	`Strategies Weighed by Adversaries` *as proxy for cyberthreat environment*	`Int_Users` *as proxy for cyberthreat environment*	*All proxies for cyberthreat environment*
`Strategies Weighted by Cybersovereignty Opponents`	0.807**	0.800**	0.808**	0.789**	0.787**
	(0.66, 0.99)	(0.65, 0.98)	(0.66, 0.99)	(0.64, 0.97)	(0.64, 0.96)
`Attacker`	1.133	1.019	1.157	1.103	1.027
	(0.92, 1.39)	(0.77, 1.35)	(0.94, 1.43)	(0.89, 1.37)	(0.77, 1.38)
`Democracy`	1.777**	1.728**	1.816**	1.615**	1.619**
	(1.14, 2.76)	(1.01, 2.70)	(1.16, 2.83)	(1.03, 2.52)	(1.03, 2.54)
`IGO Membership`	1.077	1.089	1.074	1.029	1.026
	(0.84, 1.38)	(0.85, 1.39)	(0.84, 1.38)	(0.80, 1.32)	(0.80, 1.31)
`Total MIDs (log)`	0.977	0.919	1.023	0.959	0.956
	(0.79, 1.21)	(0.69, 1.22)	(0.83, 1.26)	(0.77, 1.20)	(0.73, 1.26)
`GDP_PerCapita (log)`	1.026***	1.025***	1.026***	——	——
	(1.01, 1.04)	(1.01, 1.04)	(1.01, 1.04)		
`Target`	——	1.005	——	——	1.005
		(1.00, 1.01)			(1.00, 1.01)
`Strategies Weighted by Adversaries`	——	——	0.882	——	0.874
			(0.71, 1.09)		(0.70, 1.10)
`Int_Users (log)`	——	——	——	1.053***	1.053***
				(1.03, 1.08)	(1.03, 1.08)
Additional Controls	✓	✓	✓	✓	✓
Concordance	0.651	0.647	0.658	0.666	0.668

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the hazard ratios and confidence intervals. There are 2,502 observations and 114 events. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. See Appendix 2.7 for more details and a more detailed presentation of results. *p<0.1; **p<0.05; ***p<0.01

and nations tend to pay attention to the changes in the global cyberthreat landscape. Since perception is important when it comes to the definition of a threat, I use two additional measures of the cyberthreat environment to incorporate this perception. First is `Strategies Weighted by Adversaries`, which is the weighted average effect of the

Table 2.3: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative network measures (hazard ratios)*

(a) Harmonization after Partners & Communications Channels

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*	*Model 6*	*Model 7*
	Ally Diffusion		*Trade Diffusion*			*Emulation after UN Partners*	*Communications Channels*
`Strategies Weighted by Cybersovereignty Opponents`	0.784**	0.785**	0.777**	0.782**	0.783**	0.783**	0.785**
	(0.64, 0.96)	(0.64, 0.96)	(0.64, 0.95)	(0.64, 0.96)	(0.64, 0.96)	(0.64, 0.96)	(0.64, 0.96)
`Strategies Weighted by Allies (1)`	0.986	——	——	——	——	——	——
	(0.88, 1.11)						
`Strategies Weighted by Allies (2)`	——	1.003	——	——	——	——	——
		(0.86, 1.15)					
`Strategies Weighted by Trading Partners (1)`	——	——	1.233**	——	——	——	——
			(1.01, 1.51)				
`Strategies Weighted by Trading Partners (2)`	——	——	——	1.050	——	——	——
				(0.84, 1.31)			
`Strategies Weighted by Trading Partners (3)`	——	——	——	——	1.121	——	——
					(0.95, 1.32)		
`Strategies Weighted by UN Partners`	——	——	——	——	——	0.793	——
						(0.26, 2.41)	
`Strategies Weighted by IGO Partners`	——	——	——	——	——	——	0.992
							(0.73, 1.34)
`Int_Users (log)`	1.052*** (1.03, 1.08)	1.052*** (1.03, 1.08)	1.050*** (1.03, 1.07)	1.052*** (1.03, 1.08)	1.051*** (1.03, 1.08)	1.053*** (1.03, 1.08)	1.052*** (1.03, 1.08)
`Democracy`	1.577** (1.01, 2.47)	1.574** (1.01, 2.48)	1.582** (1.01, 2.47)	1.569** (1.01, 2.46)	1.544* (0.99, 2.42)	1.594** (1.01, 2.50)	1.577** (1.01, 2.46)
Additional Controls	✓	✓	✓	✓	✓	✓	✓
Concordance	0.663	0.663	0.667	0.663	0.667	0.663	0.663

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the hazard ratios and confidence intervals. There are 2,502 observations and 114 events. Each model includes additional controls that are not statistically significant: `Attacker`, `IGO Membership`, `Target`, and `Total MIDs`. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. See Appendix 2.7 for more details and a more detailed presentation of results. *p<0.1; **p<0.05; ***p<0.01

strategies adopted by a nation's rivals in a period prior to the nation's strategy adoption. Similar to `Target`, `Strategies Weighted by Adversaries` is not correlated with `Adoption` (Model 3 in Table 2.2). Second is the number of Internet users as a percentage of a country's population (`Int_Users`). `Int_Users` is positively correlated with `Adoption` even if I consider the cumulative effect of all proxies for the cyberthreat environment in Model 5 of Table 2.2.

Table 2.2 also shows that `IGO Membership` is not correlated with `Adoption`, suggesting that countries do no adopt their national cybersecurity strategies because of prestige or to demonstrate modern behavior. Moreover, the country's conventional environment (`Total MIDs`) is unlikely to influence this choice. `Democracy`, on the other hand, is positively correlated with `Adoption` across all models in Table 2.2, suggesting that democracies are more likely to adopt national cybersecurity strategies than autocracies. Lastly, while `GDP_Per Capita` and `Int_Users` are positively correlated with `Adoption` across all models, these two variables are highly correlated, thus I proceed with including only `Int_Users`, in addition to all other controls listed in Model 5, into all sequential models.

Robustness Tests: Alternative Network Measures. Section 2.2 outlines a number of alternative networks through which diffusion can take place, such as the country's allies, colonial partners (i.e., nations that a share common colonial past), geographic neighbors, IGO partners (i.e., nations that have memberships in the same IGOs), linguistic partners, regime partners (i.e.., nations that share the same regime type), trading partners, and UN partners (i.e., nations that voted similarly on UNGA resolutions). Are any of these alternative networks better explanations of cybersecurity strategy diffusion than countries that have the same preferences on cybersovereignty?

Tables 2.3 and 2.4 show that, more likely than not, `Strategies Weighted by Cybersovereignty Opponents` capture the diffusion of national cybersecurity strategies. Model 1 of Table 2.3 shows that cybersovereignty preferences are not correlated with

Table 2.3: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative network measures (hazard ratios)*

(b) Cultural & Regime Similarity

	Model 8	*Model 9*	*Model 10*	*Model 11*	*Model 12*	*Model 13*	*Model 14*
	Emulation after Colonial Partners	*Emulation after Linguistic Partners*	*Emulation after Neighbors*		*Emulation after Regime Partners*		
`Strategies Weighted by Cybersovereignty Opponents`	0.779**	0.781**	0.785**	0.785**	0.785**	0.785**	0.785**
	(0.64, 0.95)	(0.64, 0.95)	(0.64, 0.96)	(0.64, 0.96)	(0.64, 0.96)	(0.64, 0.96)	(0.64, 0.96)
`Strategies Weighted by Colonial Partners`	0.919	——	——	——	——	——	——
	(0.81, 1.04)						
`Strategies Weighted by Linguistic Partners`	——	0.915	——	——	——	——	——
		(0.78, 1.07)					
`Strategies Weighted by Neighbors (1)`	——	——	0.989	——	——	——	——
			(0.90, 1.17)				
`Strategies Weighted by Neighbors (2)`	——	——	——	1.001	——	——	——
				(0.90, 1.11)			
`Strategies Weighted by Regime Partners (1)`	——	——	——	——	0.885	——	——
					(0.61, 1.27)		
`Strategies Weighted by Regime Partners (2)`	——	——	——	——	——	0.755	——
						(0.52, 1.09)	
`Strategies Weighted by Regime Partners (3)`	——	——	——	——	——	——	0.958
							(0.64, 1.43)
`Int_Users (log)`	1.053***	1.053***	1.051***	1.052***	1.052***	1.053***	1.052***
	(1.03, 1.08)	(1.03, 1.08)	(1.03, 1.08)	(1.03, 1.08)	(1.03, 1.08)	(1.03, 1.08)	(1.03, 1.08)
`Democracy`	1.603**	1.583**	1.573**	1.576**	1.768**	1.895**	1.612*
	(1.02, 2.51)	(1.02, 2.47)	(1.01, 2.46)	(1.01, 2.47)	(1.03, 3.02)	(1.16, 3.10)	(1.00, 2.61)
Additional Controls	✓	✓	✓	✓	✓	✓	✓
Concordance	0.665	0.666	0.662	0.663	0.662	0.664	0.663

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the hazard ratios and confidence intervals. There are 2,502 observations and 114 events. Each model includes additional controls that are not statistically significant: `Attacker`, `IGO Membership`, `Target`, and `Total MIDs`. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. See Appendix 2.7 for more details and a more detailed presentation of results.
*p<0.1; **p<0.05; ***p<0.01

Table 2.4: *Robustness of diffusion via strategies of cybersovereignty opponents: Cumulative influence of alternative network measures (hazard ratios)*

	Model 1 `Trade` *as total bilateral trade*	*Model 2* `Trade` *as signed annual BIT*	*Model 3* `Trade` *as signed annual PTA*
`Strategies Weighted by Cybersovereignty Opponents`	0.776**	0.772**	0.779**
	(0.64, 0.95)	(0.63, 0.94)	(0.64, 0.95)
`Strategies Weighted by Adversaries`	0.871	0.880	0.876
	(0.69, 1.09)	(0.70, 1.10)	(0.70, 1.10)
`Strategies Weighted by Colonial Partners`	0.927	0.933	0.942
	(0.82, 1.05)	(0.82, 1.06)	(0.83, 1.07)
`Strategies Weighted by Linguistic Partners`	0.930	0.924	0.930
	(0.79, 1.09)	(0.79, 1.08)	(0.80, 1.08)
`Strategies Weighted by Trading Partners (1)`	1.268**	——	——
	(1.03, 1.56)		
`Strategies Weighted by Trading Partners (2)`	——	1.113	——
		(0.89, 1.40)	
`Strategies Weighted by Trading Partners (3)`	——	——	1.125
			(0.95, 1.33)
`Int_Users (log)`	1.053**	1.055**	1.054**
	(1.03, 1.08)	(1.03, 1.08)	(1.03, 1.08)
`Democracy`	1.673**	1.632**	1.607**
	(1.07, 2.61)	(1.04, 2.55)	(1.03, 2.52)
Additional Controls	✓	✓	✓
Concordance	0.678	0.674	0.677

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the hazard ratios and confidence intervals. There are 2,502 observations and 114 events. Each model includes additional controls that are not statistically significant: `Attacker`, `IGO Membership`, `Target`, and `Total MIDs`. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. See Appendix 2.7 for more details and a more detailed presentation of results. *p<0.1; **p<0.05; ***p<0.01

alliances. This lack of correlation persists even when instead of using Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions (ATOP) data to define allies (Model 1), I use the Correlates of War (COW) Project's data on formal alliances (version 4.1) (Gibler 2008) (Model 2). Models 3-6 of Table 2.3 consider emulation after trading partners. While Model 3 displays a positive correlation between `Strategies Weighted by Trading Partners (1)`

Table 2.5: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative measure of the adopted strategies (hazard ratios)*

	Model 1
	Cumulative strategy adoption
`Strategies Weighted by Cybersovereignty Opponents`	0.810^{**}
	(0.69, 0.96)
`Strategies Weighted by Adversaries`	0.946
	(0.83, 1.07)
`Strategies Weighted by Trading Partners (1)`	0.885
	(0.63, 1.24)
`Strategies Weighted by Colonial Partners`	1.003
	(0.86, 1.17)
`Strategies Weighted by Linguistic Partners`	0.849^{*}
	(0.71, 1.02)
`Int_Users (log)`	1.050^{***}
	(1.02, 1.08)
`Democracy`	1.459
	(0.91, 2.33)
Additional Controls	✓
Concordance	0.665

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the hazard ratios and confidence intervals. There are 2,502 observations and 114 events. Each model includes additional controls that are not statistically significant: `Attacker`, `IGO Membership`, and `Target`. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. See Appendix 2.7 for more details and a more detailed presentation of results. *p<0.1; **p<0.05; ***p<0.01

and `Adoption`, this result is not robust to alternative specifications of trade relationships. Specifically, instead of identifying a country's trade partners using bilateral trade data from the World Bank (`Trading Partners (1)` in Model 3), I used the number of annually signed bilateral investment treaties (BITs) (`Trading Partners (2)` in Model 4) and preferential trade agreements (PTA) (`Trading Partners (3)` in Model 5) (Graham and Tucker 2019). Moreover, Models 6 and 7 of Table 2.3a show no evidence of emulation after UN partners and via communications channels.

Table 2.3b provides further support for my main explanation of the global

spread of cybersecurity strategies—`Strategies Weighted by Cybersovereignty Opponents`—demonstrating that additional alternative explanations, such as cultural and regime similarity, do not contribute to this global spread. Models 8-11 in Table 2.3b find no support for the cultural similarity explanation. This result is robust even after I use an alternative measure to define a country's geographic neighbors—in addition to using the distance between two capitals (`Neighbors (1)` in Model 10), I use a dummy variable that identifies whether these countries share a land border or are separated by at most 400 miles of water (`Neighbors (2)` in Model 11) (Stinnett et al. 2002). Similarly, Models 12-14 in Table 2.3b find no support for the regime type similarity explanation. This result is robust even after I use three alternative ways to measure whether countries share the same regime type.[14]

In addition to considering individual influences of these alternative networks, I also consider their cumulative influence. Instead of piling highly correlated explanatory variables upon one another (Appendix A), I employ the Akaike Information Criterion (AIC) to select which of these networks provide the best fit.[15] The results confirm that the "best" model should include `Strategies Weighted by Cybersovereignty Opponents`, as well as `Strategies Weighted by Adversaries`, `Strategies Weighted by Colonial, Linguistic, and Trading Partners`. Table 2.4 presents the results and confirms the negative correlation between `Strategies Weighted by Cybersovereignty Opponents` and `Adoption`. Similarly, Table 2.4 shows that there is a positive correlation between the strategies of trading partners and `Adoption` (Model 1), but this result disappears when I measure trading relationships using the number of signed annual BITs (Model 2) and PTAs

[14] Specifically, I create a dummy variable that identifies whether two countries share the same regime, using Gurr, Marshall and Jaggers (2010)'s Polity IV score. I use the following three cut-points to identify such nations: (1) nations that score a "6" or above receive a "1" (i.e., democracy) and those nations that score a "5" or below receive a "0" (i.e., autocracy) (`Regime Partner (1)`); (2) nations that score a "5" or above receive a "1" (i.e., democracy) and those nations that score a "4" or below receive a "0" (i.e., autocracy) (`Regime Partner (2)`); and (3) nations that score a "4" or above receive a "1" (i.e., democracy) and those nations that score a "3" or below receive a "0" (i.e., autocracy) (`Regime Partner (3)`).

[15] Section 2.7 of Appendix 2.7 provides the results.

Table 2.6: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative Model Specification (odds-ratios)*

	Model 1	*Model 2*	*Model 3*	*Model 4*
	Base	`Trade` *as total bilateral trade*	`Trade` *as signed annual BIT*	`Trade` *as signed annual PTA*
`Strategies Weighted by Cybersovereignty Opponents`	0.746**	0.739**	0.737**	0.740**
	(0.59, 0.94)	(0.58, 0.94)	(0.58, 0.93)	(0.58, 0.94)
`Strategies Weighted by Adversaries`	——	0.869	0.877	0.872
		(0.66, 1.02)	(0.67, 1.03)	(0.68, 1.02)
`Strategies Weighted by Colonial Partners`	——	0.931	0.937	0.942
		(0.80, 1.07)	(0.80, 1.07)	(0.81, 1.08)
`Strategies Weighted by Linguistic Partners`	——	0.933	0.925	0.929
		(0.77, 1.08)	(0.76, 1.08)	(0.767, 1.08)
`Strategies Weighted by Trading Partners (1)`	——	1.301**	——	——
		(1.04, 1.62)		
`Strategies Weighted by Trading Partners (2)`	——	——	1.082	——
			(0.81, 1.40)	
`Strategies Weighted by Trading Partners (3)`	——	——	——	1.177
				(0.96, 1.44)
`Int_Users (log)`	1.707***	1.735***	1.759***	1.754***
	(1.20, 2.47)	(1.22, 2.51)	(1.23, 2.55)	(1.23, 2.54)
`Democracy`	1.699**	1.810**	1.761**	1.723**
	(1.04, 2.79)	(1.05, 2.99)	(1.08, 2.90)	(1.05, 2.85)
Time FE	✓	✓	✓	✓
Additional Controls	✓	✓	✓	✓
Akaike Inf. Crit.	750.948	749.186	754.006	751.890

Note: Results are from a Discrete Time Survival Model. The reported values are the odds-ratios and confidence intervals. There are 2,502 observations. Each model includes additional controls that are not statistically significant: `Attacker`, `IGO Membership`, `Target`, and `Total MIDs`. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. See Appendix 2.7 for more details and a more detailed presentation of results.
*p<0.1; **p<0.05; ***p<0.01

(Model 3). Lastly, across all models in Tables 2.3-2.4, there are positive correlations between `Int_Users` and `Adoption`, and `Democracy` and `Adoption`.

Robustness Tests: Alternative Measure of the Adopted Strategies. In addition to considering whether a country's so-called "neighbor" adopted a cybersecurity strategy in the year prior to the year during which the country adopted its strategy, I use a binary variable that records whether the country's "neighbor" adopted a cybersecurity strategy in any year prior to the year during which the country adopted its strategy. As Table 2.5 demonstrates a negative correlation between `Strategies Weighted by Cybersovereignty Opponents` and `Adoption` persists.

Robustness Tests: Alternative Model Specification. In addition to employing a Cox Proportional-Hazards (CPH) Model, I also use a Discrete Time Survival (DTS) Model to make sure that my results are robust to the model specification. Since a baseline hazard in a CPH model incorporates the effect of time, I use time fixed effects in my DTS model. Table 2.6 confirms that my earlier obtained results—`Strategies Weighted by Cybersovereignty Opponents` are negatively correlated with `Adoption`—are robust to the model specification.

2.6 Discussion and Implications

This paper asks a basic question: *what drives a state's decision to develop its defensive cybercapabilities in the form of strategies?* Contrary to the few existing works demonstrating that a country's cyberthreat environment drives cybersecurity strategy adoption (Craig and Valeriano 2016*c*,*a*,*b*), this research shows that the diffusion of national cybersecurity strategies occurs along blocks of nations with distinct preferences on cybersovereignty. Similar to existing works on policy diffusion (Brooks 2005; Drezner 2005; Füglister 2012; Stone 2004; Ward and Cao 2012; Volden 2006), this finding points to the irrelevance of

geographical borders on a government's development of policies that drive their complex interactions in this globalized world. Information and communication technologies and the Internet have completely transformed our understanding of distance and neighborhoods, and are slowly defining new *cyber*partnerships that form among nations that will decide the future of Internet regulations (Kostyuk 2020*b*). These cyberpartnerships, which are currently in the early stages of development, will have long-term effects on how national leaders rank their national priorities and conduct their domestic and foreign policy.

National cybersecurity strategies, to some extent, serve as a new form of soft power that developed nations exercise when they conduct their foreign policy pertaining to cybersecurity. In particular, these strategies send an informative signal to developing nations about the country's preferences on cybersovereignty and point them in the direction they should be moving if they want to form new partnerships with more cyber-advanced nations. In that sense, the efforts to harmonize cyberpolicies has "a coercive effect on the states that have been slow to act" (Bennett 1991, 228). As nations continue developing their cybercapabilities, developing nations will have more catching up to do to be on par with their more advanced partners. If they fail to do so, they face the possibility of being abandoned by their more advanced partners (Kostyuk 2019*b*: #27).

This research also demonstrates the effect of other variables on the country's choice to adopt a cybersecurity strategy. Not surprisingly, a country's Internet dependency and the desire of democratic leaders to respond to their constituencies over cybersecurity concerns drive this choice. The public, however, might react to a worsening global landscape of cyberthreats and not to the events directly affecting their country. For instance, Luxembourg, with an Internet penetration rate of almost ninety-eight percent of its population, has not suffered any major, known cybercampaigns (at least according to DCID). But the country has adopted three national cybersecurity strategies over the last decade—in 2011, 2015, and 2018—with "strengthening of public trust in the digital environment" as one

of its main objectives (*National Cybersecurity Strategy III* 2018, 7).

As the above example demonstrates, countries generally do not stop with adopting their first strategy. As the world evolves, countries continue revising and updating their policies to address newly presented challenges. Future research could explore why the small nation of Luxembourg adopted three cybersecurity strategies over eight years, whereas Finland, which has globally known tech-companies such as Nokia, Mesto, and Kone, adopted only one strategy in 2013. In addition to exploring the temporal or vertical variation of multiple adoptions within a cybersecurity policy area, research should explore the horizontal spread of these policies. Countries do not stop only with the first strategy, they adopt new policies and reinvent the old ones, "with the comprehensiveness of some policies expanding as they spread" (Hays 1996; Volden 2006). For instance, in 2019, the Danish Ministries of Health, Transportation and Energy adopted their own versions of cybersecurity strategies (*Cybersecurity Strategy for Health* 2019; *Cybersecurity Strategy for Transportation* 2019; *Cybersecurity Strategy for Energy* 2019).

In addition to adopting cybersecurity strategies, countries also develop a variety of other policies meant to address the challenges and opportunities of the online environment—government policies and regulations (e.g., *Electronic Design Concept of Society* (2010); *E-Government Strategy* (2017)), information and communication strategies (e.g., *Information and Communication Technologies Policy* (2003); *Cambodia ICT Master Plan* (2014)), digital agendas (e.g., *Digital Agenda* (2015, 2016)), and cyberdoctrines (e.g., *Cyber Security Strategy for Defense* (2014); *The DOD Cyber Strategy* (2015)), among others. Investigating vertical or temporal variation (i.e., other stages of policy development) as well as horizontal variation (i.e., branching out different policies to different governmental agencies and variability within these policies) in policy evolution promises to provide a more complete view of how policies move from one government to another.

While my findings have only marginally increased our existing knowledge on this topic,

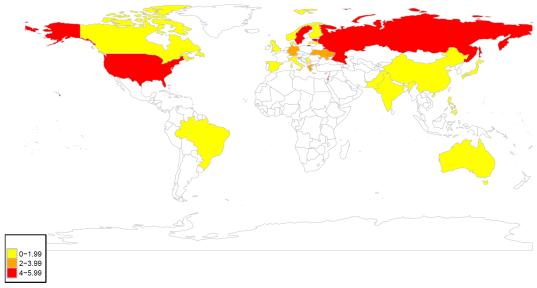
they serve as a useful point of departure not only for international relations scholars but for political scientists in general. The impact of ICTs and the Internet on our lives will continue to grow with the number of Internet-connected devices (known as the Internet-of-things), artificial intelligence, and quantum computing. To address these challengers, local leaders have been developing cyberdefenses by drafting policies and regulations. Despite this boom in policies and regulations, there is almost no literature that explains this spread, which has important policy implications. As a result, this undeveloped area of scientific inquiry leaves many questions that I encourage scholars across different subfields—international relations, comparative politics, and American politics—to explore. Only a cumulative approach will allow us to fully understand how nations build their cybercapabilities—a complex, continuously evolving and expanding area of political science and public policy research that has significantly impacted how nations interact in the age of information technologies.

2.7 Appendix

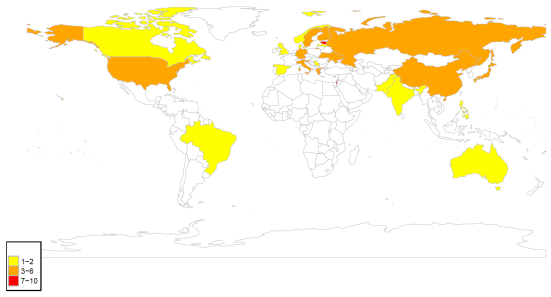
Elite Interviews: Diffusion of cybersecurity strategies

Between February and December of 2018, I conducted sixty-four interviews of cybersecurity experts specializing in twenty-five countries most of whom were either current or former government employees.[16] I personally conducted all interviews in-person or via Skype or email, to control for potential interviewer effects and maintain consistency across interviews. I conducted between one and nine (Estonia and Israel) interviews per country, with a total duration of 43.33 hours. The duration of the interviews was between 15 minutes and 3 hours, with a median of 1 hour and mean of 1.48 hours. Figure 2.3a displays total duration of my interviews by country and Figure 2.3b displays a number of the interviews I conducted in each country. These interviews shed some light on the alternative explanations that I explore in Section 2.2 of the main manuscript.

Figure 2.3: *Summary of the Interviews*



(a) Total Duration by Country (in hours)



(b) Total Number of Interviews by Country

Data

Data Sources: Cultural Similarity

I measure cultural similarity in one of the three following ways. First is linguistic similarity between countries. Using Graham and Tucker (2019)'s World Economics and Politics

[16] I received an IRB approval to conduct my interviews on February 14, 2018 (Study #HUM00127749).

Dataverse (WEPD), I create a binary variable that measures whether two nations speak the same official language. I use that variable to create a weighted average effect of the cybersecurity strategies adopted by a country's linguistic partners in a period prior the country's strategy adoption (`Strategies Weighted by Linguistic Partners`). Second are the shared identities and values of nations because they shape the channels through which ideas flow (Rogers 1995). I measure shared identities by using a binary variable that records whether two nations have similar colonial experiences (Graham and Tucker 2019). Similarly, I use that binary variable to create a weighted average effect of the cybersecurity strategies adopted by a country's colonial partners in a period prior the country's strategy adoption (`Strategies Weighted by Colonial Partners`). Last are geographic neighbors which I measure by the distance between the nations' capitals.[17] Similarly, I use the binary variable from above to create a weighted average effect of the cybersecurity strategies adopted by a country's neighbors in a period prior the country's strategy adoption (`Strategies Weighted by Neighbors (1)`).

Data Sources: Communication Channels and Expert Communities

While it is effectively impossible to account for all the various channels in which discussions related to cybersecurity take place, the most natural place to start is with an international organization devoted specifically to cybersecurity. However, since no such agency yet exists, as an alternative, I use a country's membership in international governmental organizations (IGOs)—viewed as norm "carriers" (Eyre and Suchman 1996)—to capture the degree to which the country tends to adopt international norms. This measure also incorporates the impact of information channels through which participants transmit positive and negative lessons of cybersecurity. To create a weighted average effect of cybersecurity strategies adopted by governments that share memberships in IGOs in the year prior to

[17] I run my robustness checks using a dummy variable for CONTIGUITY indicating whether states share a land border or are separated by less than 400 miles of water (Stinnett et al. 2002).

a nation's strategy adoption (`Strategies Weighted by IGO Partners`), I use Pevehouse et al. (2019)'s dyadic data on countries' joint memberships in various IGOs. This data includes information on 534 IGOs that discuss issues related to various spheres of life. Even though some of these IGOs do not have an explicit connection to cybersecurity, I incorporate countries' joint membership in all IGOs because no sphere of life remains unaffected by the Internet and the cybersecurity concerns caused by its spread.

Data Sources: Harmonization after Partners

To consider harmonization as a driver of strategy adoption (Bennett 1991), I consider the possibility that a country adopts its cybersecurity strategy in reaction to its so-called partners. I consider three groups of partners: (1) military allies; (2) trade partners; and (3) United Nations partners (i.e., nations that voted similarly to the country on the resolutions adopted at the United Nations General Assembly (UNGA)).

To identify the country's military allies, I use Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions (ATOP) data (`Allies (1)`) and the Correlates of War (COW) Project's data on formal alliances (version 4.1) (Gibler 2008) (`Allies (2)`). I use these variables to record a weighted average effect of cybersecurity strategies adopted by the country's allies in a period prior to the country adopting its first cybersecurity strategy (`Strategies Weighted by Allies (1)` and `Strategies Weighted by Allies (2)`). I use `Strategies Weighted by Allies (1)` in my main analysis because ATOP extends to 2016 and `Strategies Weighted by Allies (2)` as my robustness checks because the COW data ends in 2012.

I identify the country's trade partners using the following three variables: (1) bilateral trade data from the World Bank (`Trading Partners (1)`); (2) data on bilateral investment treaties (`Trading Partners (2)`) (Graham and Tucker 2019); and (3) preferential trade agreements (`Trading Partners (3)`) (Graham and Tucker 2019).

Similarly, I record a weighted average effect of cybersecurity strategies adopted by the country's trading partners in a period prior to the country adopting its first cybersecurity strategy (`Strategies Weighted by Trading Partners (1)`, `Strategies Weighted by Trading Partners (2)`, and `Strategies Weighted by Trading Partners (3)`). I use `Strategies Weighted by Trading Partners (1)` in my main analysis, and `Strategies Weighted by Trading Partners (2)` and `Strategies Weighted by Trading Partners (3)` to run robustness checks.

Votes in the United Nations General Assembly (UNGA) have been commonly used to construct a measure of state foreign policy preferences (Bailey, Strezhnev and Voeten 2017; Ball 1951; Gartzke 1998; Lijphart 1963; Moon 1985; Russett 1966; Signorino and Ritter 1999). To account for the possibility that states' foreign policy preferences drive strategy adoption, I use UNGA Voting Data (Voeten, Strezhnev and Bailey 2017). I use Voeten, Strezhnev and Bailey (2017)'s index that measures voting similarity between two nations—`agree2un`—to create a weighted average effect of cybersecurity strategies adopted by the country's UN partners in a period prior to the country adopting its first cybersecurity strategy (`Strategies Weighted by UN Partners`).

Data Sources: Legitimacy, Prestige, or Modern Behavior

I measure the effect of modern behavior or prestige as a driving force of strategy adoption using a country's average membership in various international governmental organizations (IGOs), using Pevehouse et al. (2019)'s data (`IGO Membership`). As explained earlier, even though there are no official international organizations related to cybersecurity, discussions on this topic take place in various international forums, including IGOs.[18]

[18] To measure the effect of prestige, I have also considered controlling for a cumulative sum of cybersecurity strategies adopted in the year prior to the country's strategy adoption. However, because my survival analysis includes time-varying covariates and this variable is the same across all nations and only differs by year, I opted to run my robustness checks using the variable that has no country-specific variation.

Data Sources: Threat Environment or Security Concerns

I consider two types of threats about which a nation should be concerned: conventional and so-called *digital*. To account for the effect of the conventional front on strategy adoption, I control for the total number of militarized interstate disputes that a country experienced in the year preceding its strategy adoption (`Total MIDs`). To create this variable, I use Militarized Interstate Disputes (MID) data, which measures the presence of "a threat, display, or use of force by one state against another" (Maoz 2005).[19]

I measure the country's threat environment using the following three measures. First is the number Internet users in a country as a percentage of the country's total population, taken from the World Bank (`Int_Users`).[20] This variable serves as a proxy for the country's vulnerability to cyberthreats and its capacity to execute cyberattacks (North Korea is an exception).

Second is the cumulative number of large, known cybercampaigns that a country experienced in all years preceding its strategy adoption (`Target`).[21] The more cybercampaigns the country experienced, or the larger those campaigns, the more likely it is to develop defensive measures against such threats.[22] National cybersecurity strategies are generally the first and most basic strategies, but they are also the foundational defenses that a country creates because they: outline "high-level objectives, principles, and priorities that guide a country in addressing cybersecurity;" describe steps that the country will undertake to achieve these objectives; and list stakeholders responsible for undertaking these steps (InternationalTelecommunicationsUnion 2018, 13). For instance, the Estonian government

[19] As a robustness check, I considered controlling for the total number of rivalries that a country had in the year prior to its strategy adoption using Klein, Goertz and Diehl (2006)' data on state rivalries. But because this data set has been updated only until 2001, I am unable to use it in my analysis that focuses on the 1999-2018 period.

[20] I use logarithmic transformations to address this variable's skewness.

[21] Valeriano and Maness (2018) define a cybercampaign as an accumulation of cyberattacks meant to achieve strategically important goals.

[22] The estimate of the baseline hazard of the CPH model that I employ for this analysis encompasses a temporal effect of the global landscape of cyberthreats.

formulated its first cybersecurity strategy as "a direct consequence of the 2007 attacks," which reminded the government that it "paid little attention to the security side of [the country's] e-governance and e-services" (Kostyuk 2019*b*: Estonia, #6).[23]

To create `Target` variables, I use Valeriano and Maness 2018's Dyadic Cyber Incident Dataset (DCID) (version 1.5)—one of the two only available datasets on major, known cybercampaigns. The Council on Foreign Relations' Cyber Operations Tracker (COT)[24] is another data set that tracks cyberoperations. But since the majority of cyberincidents in the COT data depicts non-state cyberoperations or cases of governments using spyware to track actions of opposition leaders, this data is less suited for this project.

Variations in reporting can be a serious problem for conflict event data (Weidmann 2016), especially for cyberoperations, due to: their relevant recency and novelty; the often desired secrecy surrounding their execution; and the difficulty of attribution of their origin. Even though these factors are valid concerns, they do not present an issue for this study for the following reasons. DCID records cybercampaigns—an accumulation of cyberattacks meant to achieve strategically important goals—instead of sole instances of cyberattacks. This approach ensures that the recorded data suffers less, if at all, from reporting bias than does data on individual cyberattacks. For instance, it is much easier to check the validity of the fact that Estonia suffered from a cybercampaign in 2007 than to find information on each individual cyberattack which the country experienced during a three-week-long cybercampaign. Moreover, it is hard not to notice a full-scale cybercampaign, especially when a significant amount of time has passed since the start of a campaign—between four and twenty years (i.e., the 2000-2016 period), for the attacks in DCID. Similarly, English-speaking outlets are more likely to cover a full-scale cybercampaign than individual, low-level cyberattacks. Lastly, it is much easier to use multiple sources to mistakenly record

[23] During 2018, I conducted sixty-five interviews of cybersecurity experts that were fundamental for the development of my theory as they shed some light on the alternative explanations. Section 2.7 of the Online Appendix provides an overview of these interviews.

[24] *Source:* https://www.cfr.org/interactive/cyber-operations.

an individual cyberattack, which often lacks specific details, than to over-report large-scale cybercampaigns.

While it is difficult to attribute an origin of cyberoperations, attribution is often no longer a technical problem but a complex political choice (Clark and Landau 2011; Rid and Buchanan 2015). A few governments that can attribute cyberoperations used to be reluctant to do so because public accusations require them to present proof, which can require them to reveal their sources and compromise ongoing secret operations, and to take actions in response to the suffered attack.[25] Governments are not willing to take blame for cyberoperations as this would obligate them to face consequences for their actions. Private companies, however, have business incentives to discover and attribute cyberoperations because public attribution brings them new clients and increases their revenue. Because revenue motivates companies to go after large cybercampaigns and ignore individual, low-level attacks, misattribution or lack of attribution is unlikely to be the case for the DCID data.[26]

Countries that do not have the capacity to attribute cyberoperations often benefit from such third-party public attribution. For instance, the Iranian government found out that its nuclear enrichment facility had been subjected to cyberattacks for at least two years from reports published by private companies in 2010. To address the possibility that a country might adopt a policy only when it discovers that it has been a target of cyberoperations from outside sources, I supplement the start and end dates of the DCID's cybercampaigns with the date of the campaigns' public discovery.

This discussion suggests that despite DCID's limitations, the overt cybercampaigns listed

[25] Recent indictments by the U.S. Department of Justice (e.g., USDepartmentOfJustice (2014), USDepartmentOfJustice (2016), USDepartmentOfJustice (2018*a*), USDepartmentOfJustice (2018*b*), and USDepartmentOfJustice (2018*c*)) demonstrate that this behavior might be changing. States might be more willing to use their ability to publicly attribute cyberoperations as a way of signaling their cybercapability, meant to deter their opponents.

[26] It is worth noting that in order to minimize reporting bias, DCID follows a well-established practice in conflict studies: they use multiple sources to record an event and make sure that these various sources attribute this even to the same origin.

in DCID serve as a good proxy for a government's overall cyberthreat environment. The most prominent cybercampaigns "would be expected to have the largest impact on the government [cybersecurity] policy," which is the main focus of this study (Craig and Valeriano 2016*c*, 5).

To signal its capability and demonstrate that it is on par with its adversaries, a nation can adopt policies similar to those of its adversaries. In that sense, interstate competition can drive strategy adoption. To account for this possibility, my third measure of the country's cyberthreat environment record a weighted average effect of cybersecurity strategies adopted by the country's adversaries in a period prior to the country adopting its first cybersecurity strategy (`Strategies Weighted by Adversaries`).

Data Sources: Regime Type

To account for public opinion as a driver of policy adoption, I control for the country's regime type. Specifically, I use Gurr, Marshall and Jaggers (2010)'s Polity IV score to create a dummy variable that takes the value of 0 if this score is less than six representing an autocracy, and 1, if this score is at least six representing a democracy (`Democracy`).

I use the following two measures to identify nations that share the same regime type:

1. `Regime Partners (1)`: a dummy variable that identifies whether two countries share the same regime, using Gurr, Marshall and Jaggers (2010)'s Polity IV score; nations that score a "5" or above receive a "1" (i.e., democracy) and those nations that score a "4" or below receive a "0" (i.e., autocracy); and
2. `Regime Partners (2)`: a dummy variable that identifies whether two countries share the same regime, using Gurr, Marshall and Jaggers (2010)'s Polity IV score; nations that score a "6" or above receive a "1" (i.e., democracy) and those nations that score a "5" or below receive a "0" (i.e., autocracy).

Similarly, I record a weighted average effect of cybersecurity strategies adopted by countries

that share the same regime type with the country in a period prior to the country adopting its first cybersecurity strategy (`Strategies Weighted by Regime Partners (1/2)`).

Empirical Strategy

Cox Proportional-Hazards model. One assumption of the Cox Proportional-Hazards (CPH) model is that no two countries adopt strategies at the same time. In practice, this is not necessarily the case. Many countries adopt strategies in the same year. To "break this tie," I used the Efron approximation in my model as it is a tighter approximation to the exact marginal. Another assumption of the CPH model is that the hazard ratios do not vary over time. This means that if a country's Internet dependency increases the probability that the country adopts a cybersecurity strategy by ten percent, this effect should remain the same in 2010 and 2020. In practice, however, this assumption is often not met. For instance, because citizens might be more aware of the impact of the Internet in 2020, the country's Internet dependency in 2020 might have a higher effect on its probability of the strategy adoption than in 2010. This results in a non-proportional hazard model (Box-Steffensmeier, Reiter and Zorn 2003). One way to test this assumption is to use the Therneau and Grambsch non-proportionality test that uses scaled Schoenfeld residuals (Grambsch and Therneau 1994). Since some of variables violate this assumption (i.e., `Cybersovereignty Partners`, `Int_Users`, `GDP_PerCapita`), I interact these variables with starting time (`tstart`) to address this issue (Therneau, Crowson and Atkinson 2020). Despite following this recommendation by the authors of the R package, the effect of these variables should be generally understood as an average effect over the entire studied period and not as a conditional effect over a particular period of time.

While this test detects a number of specification errors in addition to non-proportionality, it may yield a false-positive test if the model is specified incorrectly (Therneau, Grambsch and Fleming 1990; Grambsch and Therneau 1994; Therneau and Grambsch 2000). Thus

scholars recommend improving the model specification for the correct functional form of the covariates (i.e., detect any non-linear fit). This could be done by either "including polynomial functions of variables or using a non-parametric method such as splines" (Keele 2010, 192). Since polynomials may be "poor approximations for more complex linear functional forms" (Keele 2010, 195), local form of estimation—splines—are used to model non-linearity (Beck and Jackman 1998; Beck, Katz and Tucker 1998; Ruppert, Wand and Carroll 2003). Since in some circumstances it is difficult to use the splines, I use the inverse hyperbolic sine function instead (Shadden and Zorn 2011).[27] I ran robustness checks where I use the inverse hyperbolic since function for continuous covariates.

Model Selection. Next I consider the cumulative effect of diffusion variables. Because some of the control variables and diffusion variables are significantly correlated as shown in Figure 2.4, I use the Akaike's selection criteria to select the variables that best explain the cybersecurity strategy adoption (`Adoption`). Lower value of AIC suggests a "better" model. Each model automatically included clustering by country and selected between the type of the main explanatory variables (`Strategies Weighted by Cybersovereignty Partners` and `Strategies Weighted by Cybersovereignty Opponents`) and control variables. Table 2.7 displays the AIC values for the best four models. It demonstrates that the "best" model should include `Democracy` and `Int_Users`. Furthermore, these results demonstrate that it is important to include `Strategies Weighted by Cybersovereignty Opponents`. Lastly and importantly, most of the earlier defined control variables contribute to the model fit. Even though `Total MIDs` and `Attacker` does not show up in the top four models, I proceed with including these controls in my sequential analysis to avoid model overfit.

Because many of the diffusion variables are significantly correlated, as shown in Figure 2.4, I again use the AIC values to select top four models that provide the best fit. Because I

[27] I considered using log-like functions but since the log function is not defined at zero, I used the inverse hyperbolic sine function, which looks like the log function but is defined at zero.

Table 2.7: *Model Selection: Control Variables*

ID	*# of Predictors*	*AIC*	*Model*
1	3	1012.35	`Strategies Weighted by Cybersovereignty Opponents` + `Int_Users` + `Democracy`
2	4	1013.50	`Strategies Weighted by Cybersovereignty Opponents` + `Int_Users` + `Democracy` + `Target`
3	4	1013.71	`Strategies Weighted by Cybersovereignty Opponents` + `Int_Users` + `Democracy` + `GDP_PerCapita`
4	4	1013.86	`Strategies Weighted by Cybersovereignty Opponents` + `Int_Users` + `Democracy` + `IGO Membership`

Table 2.8: *Model Selection: All Diffusion Variables*

ID	*# of Predictors*	*AIC*	*Model*
1	10.00	1015.58	original 6 + `Strategies Weighted by Cybersovereignty Opponents` + `Strategies Weighted by Trading Partners` + `Strategies Weighted by Adversaries`
2	11.00	1015.82	original 6 + `Strategies Weighted by Cybersovereignty Opponents` + `Strategies Weighted by Trading Partners` + `Strategies Weighted by Adversaries` + `Strategies Weighted by Colonial Partners`
3	11.00	1016.25	original 6 + `Strategies Weighted by Cybersovereignty Opponents` + `Strategies Weighted by Trading Partners` + `Strategies Weighted by Adversaries` + `Strategies Weighted by Linguistic Partners`

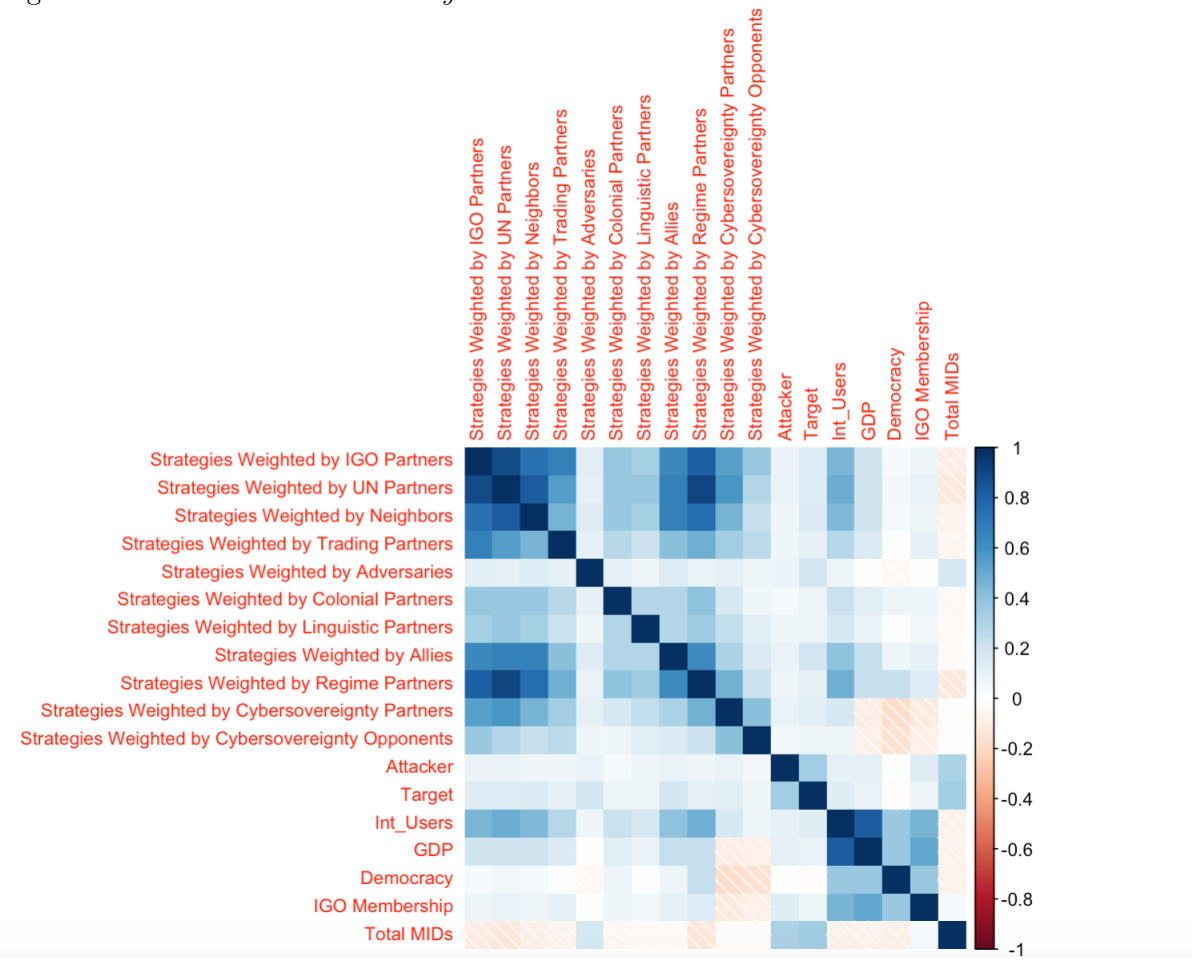
focus on selecting the diffusion variables that contribute to the "best" model, each model under consideration automatically includes six original controls—`Attacker`, `GDP_PerCapita`, `IGO Memerbship`, `Int_Users`, `Target`, `Total MIDs`—as well as clustering by country. Table 2.8 displays the results. Similarly to the earlier obtained results (Table 2.7), the "best" model should include `Strategies Weighted by Cybersovereignty Opponents`. Additionally, `Strategies Weighted by Trading Partners (1)`, `Strategies Weighted by Colonial Partners`, `Strategies Weighted by Linguistic Partners`, `Strategies Weighted by Adversaries` contribute to the better-fitted model.

Concordance statistic which uses "computes the agreement between an observed response and a predictor."[28] is another way of checking the model fit. Popularized by Harrell Jr, Lee and Mark (1996), this technique became tone of the most used measures of goodness-of-fit in survival models. Out of all the models presented in Tables 2.10-2.13, the models

[28] *Source:* https://www.rdocumentation.org/packages/survival/versions/3.1-12/topics/concordance

that have multiple diffusion variables have the highest concordance value (Table 2.11). Similarly to the results obtained from using the AIC criteria (Table 2.8), this model includes `Strategies Weighted by Cybersovereignty Opponents`, `Strategies Weighted by Trading Partners (1)`, `Policies Weighted by Adversaries`, `Strategies Weighted by Colonial Partners`, and `Strategies Weighted by Linguistic Partners`. I also ran the analysis when I compared concordance for the model that contains only six control variable and obtained a value of 0.63. This result further confirms that the model that contains `Strategies Weighted by Cybersovereignty Opponents` does a better job predicting which country will adopt a cybersecurity strategy at a particular time.

Figure 2.4: *Correlation Plot: Yearly Data*



Summary Statistics and Correlation Plots

Figure 2.4 depicts the correlation plot and Table 2.9 shows the summary statistics for the main dependent and explanatory variables. All variables besides `Democracy` have been re-scaled to make it easy to interpret the obtained results.

Table 2.9: *Summary Statistics*

Variable Name	*Minimum*	*Median*	*Mean*	*Maximum*
`Adoption`	0.00	0.00	0.04	1.00
`Strategies Weighted by Adversaries (lag, sc)`	-0.11	-0.11	0.00	11.46
`Strategies Weighted by Allies (1) (lag, sc)`	-0.53	-0.35	0.00	10.42
`Strategies Weighted by Allies (2) (lag, sc)`	-0.33	-0.33	0.00	10.06
`Strategies Weighted by Colonial Partners (lag, sc)`	-0.33	-0.33	0.00	6.24
`Strategies Weighted by Cybersovereignty Opponents (lag, sc)`	-0.45	-0.45	0.00	2.38
`Strategies Weighted by Cybersovereignty Partners (lag, sc)`	-0.70	-0.42	0.00	3.42
`Strategies Weighted by IGO Partners (lag, sc)`	-0.77	-0.38	0.00	13.51
`Strategies Weighted by Linguistic Partners (lag, sc)`	-0.36	-0.36	0.00	10.68
`Strategies Weighted by Neighbors (1) (lag, sc)`	-0.71	-0.41	0.00	14.00
`Strategies Weighted by Neighbors (2) (lag, sc)`	-0.17	-0.17	0.00	7.30
`Strategies Weighted by Trading Partners (1) (lag,sc)`	-0.53	-0.52	0.00	6.59
`Strategies Weighted by Trading Partners (2) (lag, sc)`	-0.54	-0.54	0.00	7.77
`Strategies Weighted by Trading Partners (3) (lag, sc)`	-0.54	-0.17	0.00	6.59
`Strategies Weighted by UN Partners (lag, sc)`	-0.88	-0.42	0.00	2.43
`Strategies Weighted by Regime Partners (lag, sc)`	-0.70	-0.46	0.00	2.73
`Attacker (lag, sc)`	-0.12	-0.12	0.00	20.81
`Target (lag, sc)`	-0.16	-0.16	0.00	17.98
`GDP_PerCapita (log, sc)`	-2.34	-0.02	0.00	2.44
`Int_Users (log, sc)`	-1.95	0.20	0.00	1.37
`Democracy`	0.00	1.00	0.56	1.00
`IGO Membership (lag, sc)`	-3.07	-0.05	0.00	2.97
`Total MIDs (lag, log, sc)`	-0.50	-0.50	0.00	8.27

Variable Name: `log:` logarithmized; `lag:` lagged; `sc:` standardized

Results

For ease of interpretation, I standardize all continuous explanatory variables (variables besides `Democracy`). All tables present unexpontentiated estimates and standard errors.

Table 2.10: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative network measures (hazard ratios (log))*

(a) Harmonization after Partners & Communications Channels

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*	*Model 6*	*Model 7*
	Ally Diffusion		*Trade Diffusion*			*Emulation after UN Partners*	*Communications Channels*
`Strategies Weighted by Cybersovereignty Opponents`	−0.244**	−0.242**	−0.252**	−0.246**	−0.245**	−0.245**	−0.241**
	(0.108)	(0.108)	(0.108)	(0.109)	(0.108)	(0.108)	(0.109)
`Strategies Weighted by Allies (1)`	−0.014						
	(0.091)						
`Strategies Weighted by Allies (2)`		0.003					
		(0.071)					
`Strategies Weighted by Trading Partners (1)`			0.209**				
			(0.102)				
`Strategies Weighted by Trading Partners (2)`				0.049			
				(0.133)			
`Strategies Weighted by Trading Partners (3)`					0.115		
					(0.092)		
`Strategies Weighted by UN Partners`						−0.231	
						(0.692)	
`Strategies Weighted by IGO Partners`							−0.008
							(0.172)
`Attacker`	−0.018	−0.013	−0.022	−0.014	0.011	−0.023	−0.014
	(0.170)	(0.169)	(0.169)	(0.168)	(0.170)	(0.171)	(0.169)
`Target`	0.006	0.006	0.006	0.006	0.005	0.006	0.006
	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)
`Int_Users (log)`	0.051***	0.051***	0.049***	0.051***	0.050***	0.052***	0.051***
	(0.014)	(0.013)	(0.013)	(0.013)	(0.013)	(0.014)	(0.013)
`Democracy`	0.455**	0.454**	0.459**	0.451**	0.435*	0.466**	0.456**
	(0.232)	(0.233)	(0.233)	(0.232)	(0.233)	(0.234)	(0.232)
`IGO Membership`	0.034	0.036	0.029	0.040	0.014	0.040	0.036
	(0.135)	(0.135)	(0.136)	(0.135)	(0.136)	(0.135)	(0.135)
`Total MIDs (log)`	−0.101	−0.104	−0.105	−0.102	−0.097	−0.104	−0.103
	(0.138)	(0.137)	(0.137)	(0.137)	(0.137)	(0.137)	(0.137)
Concordance	0.663	0.663	0.667	0.663	0.667	0.663	0.663

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the log of hazard ratios and standard errors. There are 2,502 observations and 114 events. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Int_Users` do not include `GDP_PerCapita` because the two variables are highly correlated. *p<0.1; **p<0.05; ***p<0.01

Table 2.10: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative network measures (hazard ratios (log))*

(b) Cultural & Regime Similarity

	Model 8	*Model 9*	*Model 10*	*Model 11*	*Model 12*	*Model 13*	*Model 14*
	Emulation after Colonial Partners	*Emulation after Linguistic Partners*	*Emulation after Neighbors*		*Emulation after Regime Partners*		
`Strategies Weighted by Cybersovereignty Opponents`	−0.250**	−0.247**	−0.242**	−0.242**	−0.243**	−0.242**	−0.242**
	(0.108)	(0.108)	(0.108)	(0.108)	(0.108)	(0.108)	(0.108)
`Strategies Weighted by Colonial Partners`	−0.085						
	(0.063)						
`Strategies Weighted by Linguistic Partners`		−0.089					
		(0.077)					
`Strategies Weighted by Neighbors (1)`			0.025				
			(0.084)				
`Strategies Weighted by Neighbors (2)`				0.001			
				(0.061)			
`Strategies Weighted by Regime Partners (1)`					−0.123		
					(0.191)		
`Strategies Weighted by Regime Partners (2)`						−0.281	
						(0.193)	
`Strategies Weighted by Regime Partners (3)`							−0.043
							(0.207)
`Attacker`	−0.018	−0.010	−0.011	−0.014	−0.018	−0.026	−0.015
	(0.168)	(0.170)	(0.169)	(0.169)	(0.168)	(0.168)	(0.169)
`Target`	0.005	0.005	0.006	0.006	0.006	0.006	0.006
	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)	(0.005)
`Int_Users (log)`	0.052***	0.051***	0.050***	0.051***	0.051***	0.051***	0.051***
	(0.013)	(0.013)	(0.013)	(0.013)	(0.013)	(0.013)	(0.013)
`Democracy`	0.472**	0.459**	0.453**	0.455**	0.570**	0.639**	0.478*
	(0.232)	(0.232)	(0.232)	(0.232)	(0.296)	(0.271)	(0.257)
`IGO Membership`	0.039	0.045	0.039	0.036	0.035	0.034	0.037
	(0.133)	(0.135)	(0.135)	(0.135)	(0.135)	(0.135)	(0.135)
`Total MIDs (log)`	−0.099	−0.103	−0.107	−0.104	−0.103	−0.102	−0.102
	(0.137)	(0.137)	(0.138)	(0.138)	(0.137)	(0.137)	(0.137)
Concordance	0.665	0.666	0.662	0.663	0.662	0.664	0.663

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the log of hazard ratios and standard errors. There are 2,502 observations and 114 events. All variables but `Democracy` are standardized. All results based on two-tailed tests. *p<0.1; **p<0.05; ***p<0.01

Table 2.11: *Robustness of diffusion via strategies of cybersovereignty opponents: Cumulative influence of alternative network measures (hazard ratios (log))*

	Model 1 `Trade` *as total bilateral trade*	*Model 2* `Trade` *as signed annual BIT*	*Model 3* `Trade` *as signed annual PTA*
`Strategies Weighted by Cybersovereignty Opponents`	-0.253^{**}	-0.259^{**}	-0.250^{**}
	(0.108)	(0.109)	(0.107)
`Strategies Weighted by Adversaries`	−0.139	−0.128	−0.132
	(0.098)	(0.098)	(0.097)
`Strategies Weighted by Colonial Partners`	−0.076	−0.070	−0.060
	(0.064)	(0.065)	(0.064)
`Strategies Weighted by Linguistic Partners`	−0.072	−0.080	−0.073
	(0.077)	(0.078)	(0.078)
`Strategies Weighted by Trading Partners (1)`	0.237^{**}		
	(0.102)		
`Strategies Weighted by Trading Partners (2)`		0.107	
		(0.134)	
`Strategies Weighted by Trading Partners (3)`			0.118
			(0.091)
`Attacker`	0.015	0.026	0.049
	(0.170)	(0.169)	(0.171)
`Target`	0.004	0.004	0.004
	(0.005)	(0.005)	(0.005)
`Int_Users (log)` ∗tstart)	0.052^{***}	0.053^{***}	0.052^{***}
	(0.013)	(0.013)	(0.013)
`Democracy`	0.515^{**}	0.489^{**}	0.474^{**}
	(0.234)	(0.232)	(0.234)
`IGO Membership`	0.018	0.044	0.009
	(0.136)	(0.135)	(0.136)
`Total MIDs (log)`	−0.042	−0.045	−0.036
	(0.137)	(0.137)	(0.138)
Additional Controls	✓	✓	✓
Concordance	0.678	0.674	0.677

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the log of hazard ratios and standard errors. There are 2,502 observations and 114 events. All variables but `Democracy` are standardized. All results based on two-tailed tests. *p<0.1; **p<0.05; ***p<0.01

Table 2.12: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative measure of the adopted strategies (hazard ratios (log))*

	Model 1
	Cumulative strategy adoption
`Strategies Weighted by Cybersovereignty Opponents`	-0.210^{**}
	(0.095)
`Strategies Weighted by Adversaries`	-0.056
	(0.078)
`Strategies Weighted by Trading Partners (1)`	-0.122
	(0.161)
`Strategies Weighted by Colonial Partners`	0.003
	(0.093)
`Strategies Weighted by Linguistic Partners`	-0.164^{*}
	(0.104)
`Attacker`	0.023
	(0.172)
`Target`	0.005
	(0.005)
`Int_Users (log)`	0.049^{***}
	(0.014)
`Democracy`	0.378
	(0.243)
`IGO Membership`	0.069
	(0.140)
`Total MIDs (log)`	-0.019
	(0.156)
Additional Controls	✓
Concordance	0.665

Note: Results are from a Cox Proportional-Hazards Model. The reported values are the log of hazard ratios and standard errors. There are 2,502 observations and 114 events. All variables but `Democracy` are standardized. All results based on two-tailed tests. *p<0.1; **p<0.05; ***p<0.01

Table 2.13: *Robustness of diffusion via strategies of cybersovereignty opponents: Alternative Model Specification (odds-ratios (log))*

	Model 1	*Model 2*	*Model 3*	*Model 4*
	Base	`Trade` *as total bilateral trade*	`Trade` *as signed annual BIT*	`Trade` *as signed annual PTA*
`Strategies Weighted by Cybersovereignty Opponents`	-0.292^{**}	-0.302^{**}	-0.305^{**}	-0.301^{**}
	(0.120)	(0.121)	(0.122)	(0.121)
`Strategies Weighted by Adversaries`		-0.141	-0.132	-0.137
		(0.100)	(0.100)	(0.100)
`Strategies Weighted by Colonial Partners`		-0.072	-0.065	-0.060
		(0.073)	(0.074)	(0.073)
`Strategies Weighted by Linguistic Partners`		-0.070	-0.079	-0.074
		(0.085)	(0.086)	(0.085)
`Strategies Weighted by Trading Partners (1)`		0.263^{**}		
		(0.114)		
`Strategies Weighted by Trading Partners (2)`			0.079	
			(0.140)	
`Strategies Weighted by Trading Partners (3)`				0.163
				(0.104)
`Attacker`	0.034	0.055	0.069	0.105
	(0.189)	(0.194)	(0.193)	(0.194)
`Target`	0.079	0.063	0.060	0.053
	(0.094)	(0.095)	(0.095)	(0.095)
`Int_Users (log)`	0.535^{***}	0.551^{***}	0.565^{***}	0.562^{***}
	(0.184)	(0.184)	(0.185)	(0.184)
`Democracy`	0.530^{**}	0.593^{**}	0.566^{**}	0.544^{**}
	(0.250)	(0.254)	(0.252)	(0.253)
`IGO Membership`	0.101	0.078	0.105	0.069
	(0.148)	(0.151)	(0.149)	(0.150)
`Total MIDs (log)`	-0.085	-0.026	-0.024	-0.014
	(0.146)	(0.147)	(0.147)	(0.147)
Time FE	✓	✓	✓	✓
Additional Controls	✓	✓	✓	✓
Akaike Inf. Crit.	750.948	749.186	754.006	751.890

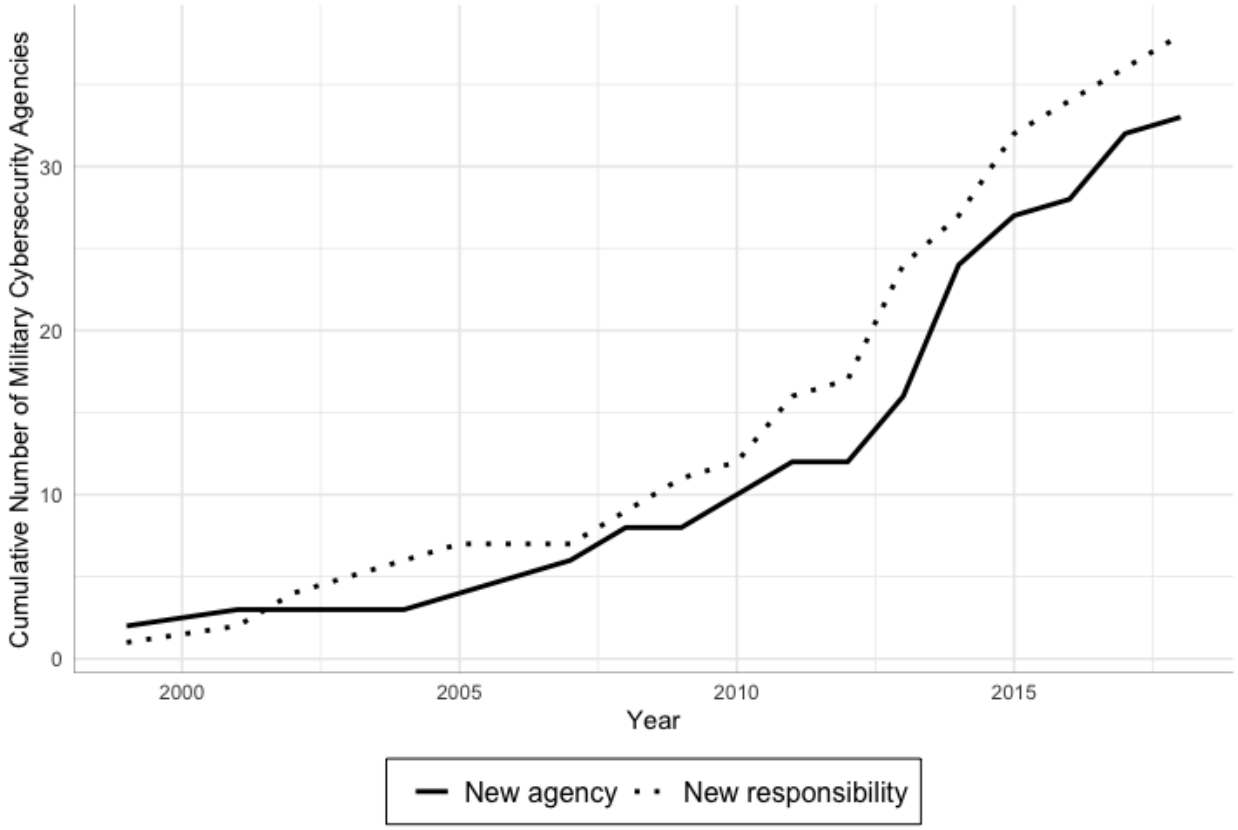
Note: Results are from a Discrete Time Survival Model. The reported values are the log of odds-ratios and standard errors. There are 2,502 observations. All variables but `Democracy` are standardized. All results based on two-tailed tests. *p<0.1; **p<0.05; ***p<0.01

Chapter 3

Diffusion of State Military Cybercapacity: The Theory of Complementarity In Alliances

Facing a growing number of cyberthreats, states have begun building their operational capacity in the cyber domain by publicly initiating the development of their military cyberapparatuses. Specifically, as this initial step, some nations assign cybersecurity responsibilities to existing military agencies (`New responsibility`), as Albania did with its Defence Intelligence and Security Agency (DISA) in 2014, and some nations create brand new military units devoted to cybersecurity (`New agency`), as Argentina did with its Computer Science Troops in 2005. Figure 3.1 displays the distribution of the initial choices that countries made when developing their military cyberapparatus between 1999 and 2018. Delegating responsibility to an existing agency allows the country to quickly begin working on cybersecurity, but it can be difficult to optimize the development of operational capacity. Creating a new agency, on the other hand, takes more time and resources, but it sends a stronger signal of commitment and more effectively increases the country's military cybercapacity. *What explains this choice? And more specifically, why create new units at all, if that option is costlier and entails a longer path to operational capacity?*

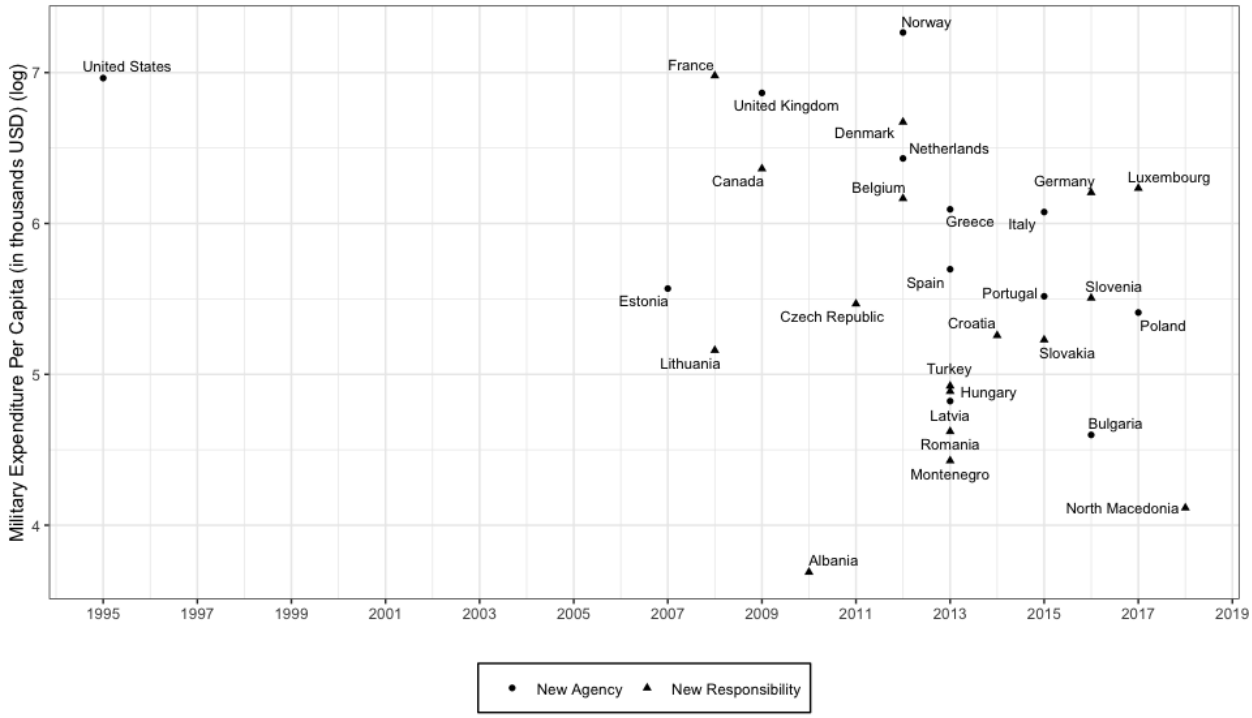
Figure 3.1: *New Cybersecurity Responsibility versus New Cybersecurity Military Agency over Time*



Note: The figure displays a cumulative number of military cybersecurity agencies that countries created when initiating the development of their military cybersecurity apparatuses. *New agency*—nations started with creating brand new units. *New responsibility*—nations started with assigning their existing agencies to deal with cybersecurity. *Source:* Author's calculations based on State Cybersecurity Organizations (SCO) data.

International relations scholars have been using the theory of free-riding in military alliances for decades to explain how allies pool their resources to defend against a common threat (Olson and Zeckhauser 1966; Palmer 1990; Plümper and Neumayer 2015; Sandler 1993). This theory predicts that wealthier allies tend to contribute disproportionately large shares of their defense spending to provide defense—a common public good shared by all members of an alliance—and smaller allies are more more likely to free-ride using the contributions of these larger allies. Using this distinction, the theory of free-riding would predict that all but the wealthiest alliance members should opt for the lower-cost option ("new

Figure 3.2: *Initiation of Military Cyberapparatuses by NATO countries*



Note: The figure displays the initiation of military cyberappatuses by NATO nations over time. *New agency*—nations started with creating brand new units. *New responsibility*—nations started with assigning their existing agencies to deal with cybersecurity. *Sources:* (1) State Cybersecurity Organizations (SCO) data developed by the author, and (2) National Material Capabilities (NMC) Data (version 5.0) (Greig and Enterline 2017). Since NMC was last updated in 2012, I use countries' military expenditure per capita in 2012 for all nations that started the development of their military cybersecurity apparatuses post 2012.

responsibility"). Figure 3.2, which displays the public development of military cybercapacity by NATO members, demonstrates that this is not necessarily the case.

I argue that the choice depends on the signal a country wants to send to its allies and is affected by the previous choices its allies made when they developed their own military cyberapparatuses, following the logic of complementarity. If the country's allies signal toughness by creating brand new military cybersecurity units, the country takes a softer approach and assigns cybersecurity responsibilities to an existing military agency. But if the allies have taken a softer approach and only assign new responsibilities to existing agencies, the country is more likely to take an extra step and create a brand new unit. I test the

validity of my argument using a newly-constructed cross-national time-series data set on state cybersecurity organizations for the 1999-2018 period. I find robust empirical support for the theory of complementarity in alliances.

This empirical analysis carries important implications for the study of national security policy. This study contributes to an existing body of works that examines the factors that shape a country's defense policy[1] and presents a departure from these works by treating the spread of military cybersecurity agencies as an example of capacity diffusion. This study further contributes to the literature on complementarity and substitutability of conventional military operations and cyberoperations (Kostyuk and Gartzke 2019) by demonstrating that the former is more often the case.

By investigating the changes in allies' military cybersecurity apparatuses, this research points to a new phenomenon—the role that a country's allies' behavior plays on its decision to publicly signal its military cybercapabilities. Despite the abundance of literature on military alliances[2] and their effect on the aggregation of military capabilities (Schweller 1994; Sweeney and Fritz 2004), no existing works study the effect of allies on a state's choice to publicly signal its military cybercapability. Lastly, and most importantly, this research explains why the free-riding theory of alliance does not always explain the behavior of military allies when it comes to the cyber domain.

3.1 Signaling State Military Cybercapacity

Military Cybersecurity Apparatus as a Proxy for Military Cybercapacity. There are two main ways that a state can publicly signal its offensive military cybercapability. It

[1] Some of these factors include military strategic culture (Johnston 1998; Kier 1995; Legro 1996), political institutions (Avant 2000), organizational biases (Snyder 1984*b*), social structure and ethnicity (Hoyt 2007; Rosen 1996), regime type (Reiter and Stam 2002), global norms (Katzenstein 1996), strategic threats (Goldman 2007; Posen 1984; Zisk 1993; Sechser and Saunders 2010), and organizational capacity and financial flexibility (Horowitz 2010).

[2] Some prominent works on alliances include: Benson and Clinton (2016); Grant (2013); Leeds et al. (2002); Morrow (1991); Stephen (1987); Walt (1997).

can execute an attack or develop its military cyberapparatus. While cyberattacks provide targets with a good estimate of the attacker's capability, this signaling method has a few disadvantages. First, it devalues the existing capacity because it indicates vulnerabilities that the target can fix. Second, the target can execute a reprisal against the attacker. Third, if the cyberattack is not publicly attributed, which often takes time and is not an option for many countries, then the attack will not send a signal to the entire international community.

Why is the development of a military cyberapparatus a better option? Signaling via cyberapparatus development has benefits over signaling via cyberoperations because it preserves the value of cyberoperations, which diminishes after the first use, and provides other nations with an immediate, albeit rough, estimate of the state's cybercapacity. Such public signaling is generally true for military cybersecurity units. Even though states generally create their first offensive cybercapacity unit within their signals intelligence (SIGINT) agencies because these agencies tend to be the best equipped to deal with "cyber" issues (Kostyuk 2019*b*: #3),[3] the specifics of these agencies' work makes it preferable for their existence to be less widely known.

Contrary to cyberintelligence agencies whose main goal is to penetrate adversarial (and often allies') networks and to stay undetectable for as long as possible, the development of military cybersecurity units *publicly* and *loudly* signals the country's capability and intent to use its cyberoffenses to punish aggressors to the entire international community (Kostyuk 2019*b*: #11). With the development of military cybersecurity agencies, states tend to release information about their projected military personnel, changes (if any) to existing military doctrines, and projected budgets. For example, after the 2009 creation of the U.S. Cyber Command, the Department of Defense (DoD) released its new doctrine, which treated "cyberspace as an operational domain" (*Strategy for Operating in Cyberspace* 2011, 5). The DoD further created its 133-teams Cyber Mission Force with 6,200 cyberoperators

[3] China is an exception in this regard. See Cunningham (2018)'s work for more details.

in 2015. The following year, the Russian government committed between $200 million and $250 million USD per year to significantly strengthen its cyberoffensive capabilities and to create a cyber-deterrent that "will equate to the role played by nuclear weapons" (Gerden 2016). And the 2017 U.S. DoD's cyber budget of $6.7 billion USD was devoted to "strengthening cyber defenses and increasing options available in case of a cyber-attack" (U.S.DepartmentOfDefense 2016).

Types of signals of military cybercapacity. The development of a country's military cybercapacity is visible to the international community. Because it signals the country's power to hurt and its ability to withstand an attack, the state will consider how it wants to initiate the development of its military cyberapparatus. I consider two ways in which this initiation can happen. First, a state can assign cybersecurity responsibility to an existing agency within the Ministry (or Department) of Defense (MoD/DoD) or to the ministry itself. For instance, by helping draft the 2014 Afghani national cybersecurity strategy, the Afghan DoD became responsible for contributing to the establishment of a secure and resilient cyberspace in Afghanistan. Second, the state can create a new military cybersecurity unit within MoD or an army division. For example, Argentina created Computer Science Troops within its Armed Forces in 2005. These two methods differ in how developed bureaucratic capacity translates into operational capacity and, as a result, send different signals about the country's distribution of capabilities and its ability to inflict pain and defend itself and its allies.

Assigning cybersecurity responsibilities to an existing agency allows the country to more quickly begin working on cybersecurity but given the need to adapt the agency's standard operating procedures, it might be harder to optimize its work in this new area. Specifically, the assignment of cybersecurity responsibilities to an existing military agency requires mutual adaptation in which both innovation and organization change in important

ways. For instance, in addition to ensuring the safety of Albanian maritime space, the Albanian Inter-institutional Maritime Operational Center (IMOC) within the country's MoD became responsible for civil emergencies, airspace control and the development of cyberdefence capability. These new responsibilities shape how IMOC ensures the safety of maritime space, and IMOC's organizational culture shapes how it develops its cyberdefenses. Moreover, the addition of a new responsibility can also result in a mission creep, as cybersecurity exceeds the core responsibilities of the agency. As a result, the assignment of a cybersecurity responsibility to an existing military agency sends a mild signal about the country's cyberdefensive and cyberoffensive operational capacity.

Unlike new responsibility assignment, new agency creation requires more time and resources but it can be designed to maximize effectiveness. Since a new agency's sole responsibility is cyber defense, offense, and/or intelligence, a mission creep that can significantly slow down the development of operational cybercapacity is not an issue for such agencies. For instance, the sole responsibility of the Cyber Defense Unit located within the Japanese Ministry of Defense and its Self Defense Forces is "monitoring information and communications networks and responding to cyber attacks on a round-the-clock basis."[4] Agencies that have only one focus are afforded speed in the decision-making process and higher levels of command and control. For these reasons, a new entity sends a stronger signal of commitment to boosting the country's military cybercapacity that translates into a higher operational cybercapacity.

Since the creation of a new agency happens within MoD, MoD automatically becomes responsible for cybersecurity when it creates a new cybersecurity unit. I consider such cases as instances of "new agencies" because the nation chooses to send a stronger signal of commitment by developing a new military cybersecurity agency. For instance, the 2016 Bulgaria's national cybersecurity strategy made its MoD responsible for "maintain[ing] and

[4] For more information, please visit the website of the Japanese Ministry of Defense: https://www.mod.go.jp/e/publ/answers/cyber/index.html

develop[ing] existing and build new advanced capabilities for cyber defense, compatible with those of NATO and the EU..." (*National Cybersecurity Strategy* 2016, 42-43). In addition to enlisting this rather broad goal, it also committed to building the Operational Center for Cyber Defense, meant to "respond to cyber and hybrid effects of national and international scale" (*National Cybersecurity Strategy* 2016, 42-43). Luxembourg's Directorate of Defense, on the other hand, simply listed cyberattacks and hybrid warfare as key threats to develop a capacity to defend against in its *Defence Guidelines for 2025 and Beyond* (2017, 12).

In the development of a cyberapparatus, it might seem logical to start by assigning an existing agency with cybersecurity responsibilities and then eventually develop a new specialized unit to deal with cyberthreats. Nations also might start by developing smaller specialized units and then elevate them into separate commands or even branches. Historical examples of the development of air power and space capabilities demonstrate this evolution. Formed as part of the U.S. Army in 1907, U.S. Army Air Corps eventually became the aerial warfare service component (1926-1941) and received even greater autonomy from the Army's middle-level command structure when it became the United States Army Air Forces (USAAF) in 1941. In 1947, USAAF turned into the U.S. Air Force (USAF), signaling the establishment of a separate branch of the U.S. Armed Forces. The Space Force was initially established within the Air Force Space Command in 1982 and became an independent military branch in 2019. Similar evolution takes place within the development of military cyberapparatuses. For example, Argentina created Computer Science Troops within its Armed Forces in 2005 and established a Joint Cyber Defense Command in 2014. Established under the U.S. Strategic Command in 2009, the U.S. Cyber Command was elevated to the 10th combatant command in 2018. While these evolutionary developments shed light on how countries increase their operational cybercapacity, they lie beyond the scope of this research that aims to explain the initiation of state military cyberapparatuses.

3.2 Theory of Complementarity of Military Cybercapacity

I view the development of initial military cyberapparatuses as an example of capacity diffusion affected by how a country's allies initiate the development of their own cyberapparatuses. To maximize their security against common threats in the information age, nations consider the potential contributions of their allies before they decide how to start publicly developing their military cybercapacity.[5] What determines this choice?

The theory of free-riding in military alliances argues that defense is a public good and as such its benefits are available for consumption to all allies, even to those that do not necessarily contribute to its production (Olson and Zeckhauser 1966). This theory makes the following two predictions about ally behavior. First, larger allies contribute more to defense spending (e.g., the Unites States' disproportionately large contribution of its defense spending to the North Atlantic Treaty Organization (NATO)). Second, it is easier for smaller allies to under-contribute to the alliance without noticeably affecting the alliance's overall capacity (Olson and Zeckhauser 1966; Palmer 1990; Sandler 1993). As a result, the smaller the ally, the more likely it is to free-ride. Plümper and Neumayer (2015) provide a modification to this prediction by showing that while the vast majority of smaller NATO allies are free-riders, the extent of free-riding is not a function of country size—the relatively larger small NATO allies do not free-ride any less than the smallest NATO allies.

By applying the theory of free-riding to the development of military cybercapabilities, we should see: (1) that the lower-cost option ("new responsibility") is the dominant strategy for all but the largest/wealthiest alliance members, and (2) that smaller allies are more

[5] Since cyberoperations are often used along with or to substitute military operations, states do not necessarily form new military alliances to deal with these threats. Instead they tend to add this new domain to their existing agreements, as North Atlantic Treaty Organization (NATO) did when it announced cyberspace as a new operational domain in 2016.

likely to free-ride and adopt the lower-cost option. Figure 3.2, which displays the public development of military cybercapacity by NATO members, demonstrates that these two free-riding theories do not necessarily hold. While the United States and the United Kingdom started the development of their public military cybercapacities with new agencies, other wealthy NATO partners, such as France, Canada and Germany, preferred assigning new responsibilities to existing agencies. Some smaller allies, such as Estonia, Latvia, Bulgaria, which should have assigned existing military agencies with new cybersecurity responsibilities (according to the free-riding theory), developed brand new agencies.

Why does the free-riding theory not completely explain the behavior of military allies when it comes to the development of capability in the cyber domain? Since nations want to maximize their cumulative operational cybercapacity, I argue that complementarity of a nation's capabilities and its allies' capabilities better explains this behavior and guides how nations start to publicly acquire their military cybercapacity. Building a new unit versus assigning cybersecurity responsibilities to an existing agency, to some extent, resembles the choice between acquiring arms or relying on allies' arms. If the country's allies assigned cybersecurity responsibilities to military agencies, then they are able to produce additional security quickly; the efficiency of this capability, however, might be in question. To increase the strength of the alliance's overall security, the state is more likely to develop a new military cybersecurity unit. As the nations' allies have already acquired some sort of military cybercapacity, the nation can take its time and focus on the production of a more reliable and efficient capability in its newly established agency. The opposite direction of this relationship is also true. If the nations' allies have already created new cybersecurity units, then the nation has less incentive to create a brand-new unit as it can rely on its allies for protection. But to reassure its allies that it is willing to contribute its fair share, the nation is likely to assign cybersecurity responsibilities to an existing agency. In either case, the nation increases the alliance's overall security and strengthens the signal of the alliance's overall

military cybercapability.

Moreover, fear of abandonment by a strong partner drives a weak partner's desire to increase its value to an alliance (Snyder 1984*a*). For instance, after the North Atlantic Treaty Organization (NATO) announced cyberspace to be a new operational domain, Estonia was one of the few nations that rapidly started developing offensive cybercapabilities for NATO (Hankewitz 2018). Estonia also followed its NATO partners' lead on the disclosure of its offensive capabilities and its stand on the applicability of international law to cyberspace: "Estonia does not deny possession of offensive capabilities, the same way like other NATO Allies do. Estonia is also very clear that the use of any retaliation measures/offensive capabilities will be introduced in accordance with international law, e.g., Article 51 of the UN Charter" (Kostyuk 2019*b*: #42). While smaller, less resourceful nations are not able to match their allies' capability, this does not prevent them from complementing their allies' actions. Their smaller bureaucracies might allow them to more efficiently create new military cybersecurity units, even if these units are of a significantly smaller size. Alternatively, weaker allies might be content with the larger ally's anticipated protection, and simply assign responsibility to existing agencies.

Using the theory of complementary of military cybercapacity discussed above, I derive the following two hypotheses:

- **Hypothesis 1a:** *Assignment of a new cybersecurity responsibility to an existing military agency by a country's allies in year $t-1$ increases the likelihood that the country creates a new military cybersecurity unit in year t.*

- **Hypothesis 1b:** *Creation of a military cybersecurity agency by a country's allies in year $t-1$ increases the likelihood that the country assigns a new cybersecurity responsibility to an existing military agency in year t.*

3.3 Alternative Explanations

I also considers a number of alternative explanations that might drive the recent global spread of military cybersecurity units, such as *cultural similarity*, *expert communities*, *foreign policy preferences*, *geography*, *prestige*, and *regime type*. My results demonstrate that none of these alternative explanations are correlated with a country's choice to develop its military cybersecurity apparatus.

Alternative Explanation 1: Cultural Similarity

Since cybersecurity is a rather novel topic, national leaders tend to operate in poor-information environments when devising their military cybersecurity apparatus. The natural place to look for relevant information is the military cybersecurity organizations created by nations that share similar cultural contexts (Simmons and Elkins 2004, 175). But given the ease of communication in the globalized world, I argue that cultural similarity is not a defining factor of how countries choose to publicly signal the initiation of their military cyberapparatuses. Figure 1.2, which displays the spread of military cybersecurity units from 1999 to 2018, provides further evidence for this claim. As a result, I expect that the development of military cyberapparatuses by the country's linguistic partners to be either negatively correlated or not correlated with the country's choice to develop its military cybersecurity apparatus.

Alternative Explanation 2: Expert Communities

Information exchanges drive diffusion of various sociological processes (Axelrod 1997; Rogers 1995). Such exchanges on the topic of military cybercapacity can take place between governments either on a bilateral basis or on a multilateral basis in various international forums. These multilateral exchanges may openly advocate for specialization. For instance after the 1999 Kosovo bombing and the expansion of the alliances in the early 2000's, NATO

began to aggressively push for the development of niche capabilities to more efficiently pool resources from smaller members for out-of-area operations. Specifically, the Czech Republic specialized in chemical, biological, radiological and nuclear defense (CBRN), Hungary specialized in engineer troops, and Denmark focused on sealift. As these examples illustrate, smaller nations specialize in different types of conventional military capabilities. Such specialization is not the case for military cybercapacity (at least for now). If specialization influenced the choice between a new responsibility and a new agency, then countries would have developed different operational cybercapacities and would have created a variety of new cybersecurity units (e.g., within navy, army, etc.). This, however, is not the case—nations generally develop cyberoperations units within its armed forces tasked with the rather general missions of conducting combat activities in cyberspace and taking part in allied operations.

Alternative Explanation 3: Foreign Policy Preferences

Since foreign policy interests are influential in alliance formation (Gibler and Rider 2004), some might argue that such interests might extend outside of military alliances to other non-military partnerships that also shape foreign policy preferences, such as voting blocs formed in the United Nations' General Assembly (UNGA) and trading partners. Since neither of these partnerships have any relationship to cybersecurity, I expect them to be either negatively correlated or not correlated with the country's choice to develop its military cybersecurity apparatus.

Alternative Explanation 4: Geography

Countries develop their military cybercapabilities to fight wars. Most international conflicts occur within a limited set of dyads—"interstate rivals" (Goertz and Diehl 1993; Lemke and Reed 2001). Contiguity (Boulding 1962; Bremer 1992; Diehl 1985; Hensel et al. 2000; Senese 2005) and claims over territory (Hensel et al. 2000; Huth 2009; Vasquez 1995, 2001, 2009)

are correlates with escalation. Moreover, conflicts over territory between contiguous states are more likely to re-emerge (Hensel 1994; Stinnett and Diehl 2001). Using this logic, the development of military cybercapacity by a country's geographic neighbors might motivate the country to develop its own capacity. Given how easy it is to attack adversaries via cyber means, I argue that geographical constraints should be less of a concern for the development of military cybercapacity than it is for the development of conventional military capacity.

Alternative Explanation 5: Prestige

Countries' maintenance of technologically sophisticated militaries "symbolize modernity, efficacy, and independence" (Suchman and Eyre 1992). Using this logic, the creation of military cybercapacity might signal "modern behavior" and improve the country's international status or prestige (Sagan 1997). It can also fulfill a government's need to appear legitimate in the eyes of its constituency and the international community (Fordham and Asal 2007).

Alternative Explanation 6: Regime Type

I consider two possible effects of regime type. First, the inherently transparent nature of democracies might motivate democratic leaders to publicly signal state cybercapacity. As one of my interviewees put it, "as any democracy, Estonia remains open about its cybercapabilities as it is [a] reasonable" thing to do (Kostyuk 2019*b*: #42). Terrorism literature argues that the feeling of security causes citizen preferences to align with "observable" counter-terrorism measures and motivates governments to "allocate resources to observable counter-terror" (Bueno de Mesquita 2007, 9). While this might suggest why democracies are more likely to publicly signal its military cybercapacity than autocracies, it does not explain the choices countries make when they initiate the development of their military cybersecurity apparatuses.

Second, Gartzke and Weisiger (2013); Lai and Reiter (2000); Smith (1995) demonstrate

that states with similar identities—a regime type in this case—tend to co-ally. These nations are more likely to cooperate with each other and learn from each other. Using this logic, countries with the same regime type are more likely to follow each other's public initiation of a military cybersecurity apparatus.

Alternative Explanation 7: Threat Environment

The threat environment is an important factor to consider as it has been one of the main drivers of the proliferation of non-cyber military capabilities, such as nuclear weapons (Jo and Gartzke 2007), civil space capabilities (Early 2014), and drones (Fuhrmann and Horowitz 2017). The lack of international regulations on the use of offensive cybercapabilities might make nations insecure, motivating them to develop cybercapabilities in response to their rivals developing and using such capabilities (Buchanan 2017; Deibert 2011). Given the complementarity of cyberoperations and conventional operations (Kostyuk and Gartzke 2019), nations might also react to conventional threats that involve "an explicit threat, display, or use of force" (Gochman and Maoz 1984, 587). Under this imminent sense of threat, national leaders might be more likely to send a firm signal to their adversaries about their readiness to respond to attacks.

There are a number of alternative explanations that I do not directly test in this study. Kier (1997), for instance, shows that a state's unique military culture explains its choice of military doctrine. Other scholars point to bureaucratic and organizational factors as drivers of military innovations (Grissom 2008) and military effectiveness (Brooks 2007). One might expect that these factors drive the initiation of a military cybersecurity apparatus. Yet it is infeasible to operationalize many of these variables with a quantitative cross-national time-series design.

3.4 Data

Dependent Variable: Military Cybersecurity Units. I collected the first of its kind, comprehensive cross-national, time-series data set on State Cybersecurity Organizations (SCO) that contains information on more than 2,700 organizations responsible for dealing with various aspects of cybersecurity from 203 countries between 1999 and 2018. SCO distinguishes between different civilian, intelligence, and military agencies. For this project, I only use military agencies.

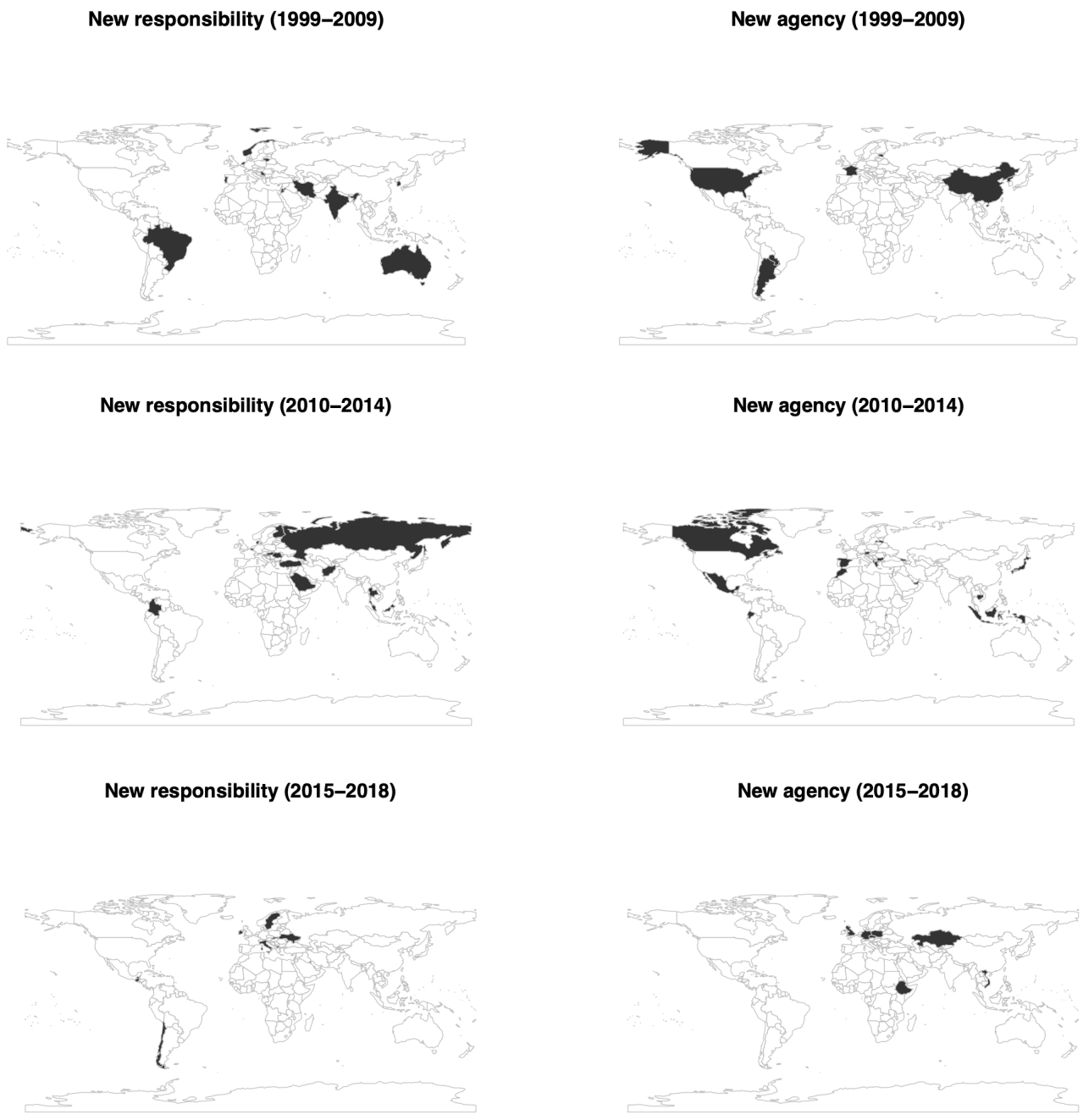
This data set includes information on when a military agency became responsible for cybersecurity or when a country created new units. Since I am interested in public signaling of military cybercapacity, I record the date when the information about the creation of a new unit or an assignment of a new responsibility became public. Generally, countries identify changes to their military cybersecurity apparatuses in announcements, press releases, updated or new military doctrines, or national cybersecurity strategies. But sometimes, the actual date of the agency creation is different from the public one. This can happen when a unit, for instance, conducts cyberoperations secretly and does not publicly announce its existence or purpose. For instance, information about China's military cybercapacity became widely known with public attribution when the Mandiant report published evidence that linked a cyberespionage campaign to China's 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (McWhorter 2013). To make sure that my sample contains the most relevant information, I consulted country cybersecurity experts,[6] primary sources[7] and secondary sources.[8]

[6] Section 3.8 of Appendix 3.8 briefly describes the interviews of cybersecurity experts that I conducted for this project.

[7] SCO includes contact information and a website for each of the recorded agencies, if such information is available. In cases when researchers found competing information from various sources, they made an attempt to contact the agency itself to clarify which information should be recorded in SCO.

[8] Some of my secondary resources include country-specific reports on the state of their cybersecurity, databases created by the international organizations, such as the ITU, NATO Cooperative Cyber Defence Centre of Excellence, the United Nations Institute for Disarmament Research, and various outlets.

Figure 3.3: *Diffusion of Military Cybercapacity (1999-2018)*



Since I focus on the 1999-2018 period in my analysis, I only include information on sixty-nine military agencies developed during this time. Thirty-eight countries assigned new responsibilities to existing agencies, including Hungary and India, which assigned the new responsibilities to their Ministries of Defense in 2013 and at least 2004, respectively. Thirty-one countries created new agencies, including Canada in 2011 when it created the Directorate of Cybernetics under the Canadian Armed Forces. Figure 3.3 displays how this choice evolved over time. By the end of 2009, militaries or the Departments of Defense of nineteen nations have been dealing in some capacity with cybersecurity; eleven of them assigned the new responsibility of handling this new domain to existing agencies (the top left plot of Figure 3.3) and eight of them created new units (the top right plot of Figure 3.3). From 2010 until the end of 2014, sixteen more nations assigned new responsibilities to existing agencies (the middle left plot of Figure 3.3) and sixteen more nations created new units (the middle right plot of Figure 3.3). From 2015 until the end of 2018, eleven more nations assigned new responsibilities to existing agencies (the bottom left plot of Figure 3.3) and nine more nations created new units (the bottom right plot of Figure 3.3).

Since I am interested in explaining the choice that a country has to make, my dependent variable receives a "1" when a country assigns an existing military unit to be responsible for cybersecurity (`Assign`), and a "2" when the country creates a new military cybersecurity agency (`Create`).

Main Predictor: Alliances. The most popularly used datasets on military alliances are Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions and Correlates of War (COW) Project's data on formal alliances (version 4.1) (Gibler 2008). Since the period in which I am interested is quite recent, ATOP Alliance data set, which contains a more detailed description of recent events and is more comprehensive, is more suitable for my analysis.[9] I

[9] Section 3.8 of Appendix 3.8 provides a detailed overview of both datasets and further expands on reasons of why I use ATOP over COW Alliances.

use SCO, which records all instances of the assignment of new cybersecurity responsibilities to existing military agencies and new military cybersecurity unit creation during the studied period, and military allies from ATOP to record a weighted average effect of the assignment of cybersecurity responsibilities to existing agencies (`New Responsibilities Weighted by Allies`) or the creation of new military cybersecurity units (`New Agencies Weighted by Allies`) by the country's allies in a period prior to the country initiating its military cybersecurity apparatus.[10]

Measures of Alternative Explanations. I use Graham and Tucker (2019)'s World Economics and Politics Dataverse (WEPD) to create dummy variable that takes a value of "1" when two nations share the same official language (`Linguistic Partners`). To estimate the weighted average effects of the foreign preferences expressed at the UNGA, I use Voeten, Strezhnev and Bailey (2017)'s data on the UNGA resolution votes (`UN Partners`). I use the following three measures of a country's trading partners to account for their effect: (1) the annual number of bilateral trade agreements between two countries, taken from the World Bank (`Trading Partners (1)`); (2) the annual number of signed bilateral investment treaties between two nations from Graham and Tucker (2019) (`Trading Partners (2)`); and (3) the annual number of signed preferential trade agreements from Graham and Tucker (2019) (`Trading Partners (3)`).

I identify the country's geographic neighbors using the inverse distance between the two capitals (`Neighbors (1)`) and a dummy variable that identifies whether two countries share a land border or are separated by at most 100 miles of water (`Neighbors (2)`) (Stinnett et al. 2002). To investigate the effect of expert communities in multilateral exchanges, I consider intergovernmental organizations (IGOs) whose primarily focus is security, defense, and peace from Pevehouse et al. (2019)'s data set. I use the country's membership in these IGOs to measure the effect of prestige on the creation of a new cybersecurity military apparatus. To

[10] Section 3.5 explains how I created this weighted average effect.

consider the effect of the regime type, I use Gurr, Marshall and Jaggers (2010)'s Polity IV score to create a dummy variable that takes the value of a "0" if this score is less than six representing an autocracy, and "1," if this score is more than equal to six representing a democracy (`Democracy`).

I use the following three measures of the cyberthreat environment. First is the number Internet users in a country as a percentage of the country's total population, taken from the World Bank (`Internet Users`).[11] Second is the cumulative number of large, known cybercampaigns[12] that a country experienced in all years preceding its continued development of its military cyberapparatus (`Target`) from Valeriano and Maness (2018)'s Dyadic Cyber Incident Dataset (DCID) (version 1.5).[13] Third is the weighted average effects of newly-assigned responsibilities and newly-created units developed by the country's adversaries in a period prior to the country initiating development of its own military cybersecurity apparatus (`New Responsibilities/Agencies Weighted by Adversaries`). To create these effects, I use SCO and Maoz (2005)'s data on Militarized Interstate Disputes (MID) that records "interactions between or among states involving threats to use military force, of military force, or actual uses of military force" to identify the country's adversaries.[14] To measure conventional military threats, I use the MID data to create the total number of MIDs that the country experienced in the year preceding its choice to cybermilitarize (`Total MIDs`) (Gochman and Maoz 1984, 587). Section 3.8 of Appendix 3.8 provides a detailed

[11] I use logarithmic transformations to address the variable's skewed distribution.

[12] Valeriano and Maness (2018) defines cybercampaigns as an accumulation of cyberattacks meant to achieve strategically important goals.

[13] Section 3.8 of Appendix 3.8 provides a detailed explanation of this data set and its limitations.

[14] Because the MID data treats incidents that involve police and border control as a use of force (e.g., disputes on the U.S.-Canadian border that involve fishing vessels), I exclude such events from the final data set by removing events with an outcome labeled as "released (for seizure)." I have also considered two alternative datasets to serve as a proxy for a country's threat environment. First is Klein, Goertz and Diehl (2006)'s data on state rivalries; it is not suitable for this analysis because it was last updated in 2001. Second is the International Crisis Behavior (ICB) data (version 12) that contains information on 476 international crises during 1918-2015 (Brecher, Wilkenfeld et al. 1997; Brecher et al. 2016). Because political acts, such as "subversion, alliance formation by adversaries, diplomatic sanctions, severance of diplomatic relations, [or] violation of treaty," trigger about a quarter of foreign policy crises in the ICB data, I omit from using it in my analysis (Hewitt 2003, 671-672).

overview of how I created additional variables that account for the alternative explanations.

Additional Controls. Besides these variables, I also account for two additional controls: (1) a country's GDP per capita as a proxy for its wealth, taken from the World Bank, as a measure of the country's wealth (`GDP_PerCapita`); and (2) a number of alliances the country is part of in a given year, taken from ATOP (`Number of Alliances`). I hypothesize that an increase in a country's wealth and a number of alliances it has is positively correlated with its decision to develop its military cyberapparatus.

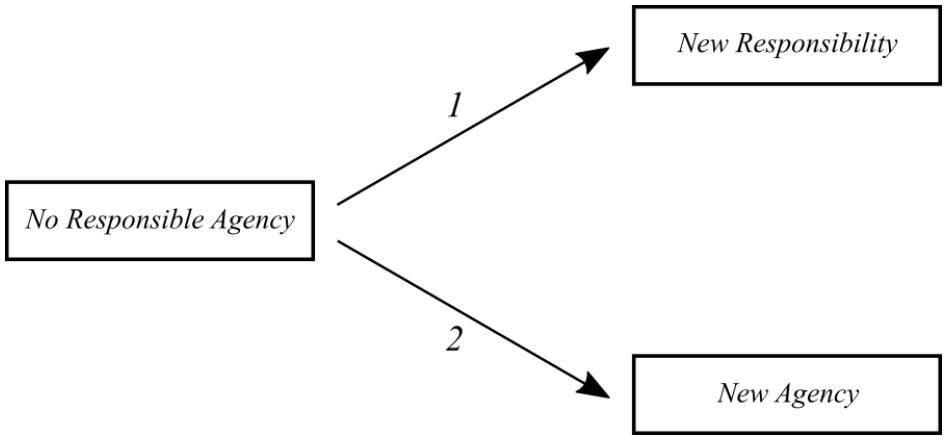
3.5 Empirical Strategy

Lagged network-weighted effects. To identify the effect of the agencies developed by a country's "neighbors" I create lagged network-weighted effects. Instead of lagging the value of the dependent unit one variable at a time and, as a result, adding a significant number of regressors to my model, I use lagged network-weighted effects that capture the "weighted average of the dependent variable in the actor's 'neighborhood"' (Simmons and Elkins 2004, 178). I define such effects for a country i as:

$$W_i * y_{-i}(t) := \sum_{j \neq i} W_{i,j}(t) y_j(t), \tag{3.1}$$

where, $W_{i,j}(t)$ is an $N \times N$ spatial weights matrix that capture's country i's neighborhood. Each element in $W_{i,j}$ measures various relationships between any two nations (e.g., alliances, trading relationship). $\sum_{j \neq i} W_{i,j}$ captures the weight of the relationship between these two nations relative to the nation's total relationships with other nations in a given area of international relations. This weight captures the importance of a neighbor's influence on this country. $y_{-i}(t)$ represents whether a country's "neighbor" $-i$ assigned a new responsibility to an existing military agency or created a new unit. Combined, $W_i * y_{-i}(t)$ captures the total effect of the country's "neighbors" that developed or did not develop their military

Figure 3.4: *Competing Risks Scheme*



cybersecurity apparatuses.

Method: Competing Risks Event History Model. I use a competing-risks event history model.[15] Specifically, I employ a Cox Proportional-Hazards (CPH) model that tests for conditions that create a greater likelihood that a country initiates the development of its military cybersecurity apparatus. I use a competing-risks model because the country chooses to either create: (1) a new responsibility or (2) a new unit (Figure 3.4). My unit of analysis is the country-year. My analysis begins in 1999 when the United States government discovered that it had been victim of the first advanced persistent threat (APT)[16] —the *Moonlight Maze*, which was a data breach that affected various U.S. government agencies and defense contractors—and ends in 2018. If a country has not started developing its military cybersecurity apparatus by December 31, 2018, it is right-censored in my data set. Since many of the covariates change over time, I use interval censoring to capture time-varying covariates (Therneau and Grambsch 2000).

I fit the following competing-risks CPH models, which examines the effect of

[15] Event history models have been widely used in political science to explain diffusion processes (Berry and Berry 1990; Elkins, Guzman and Simmons 2006; Simmons and Elkins 2004; Simmons, Lloyd and Stewart 2018).

[16] APTs are cyberoperations during which a state-sponsored group gains unauthorized access to a computer network and remains undetected for some time.

time-varying and time-invariant covariates on the country's decision to develop its military cyberapparatus. Equation 3.2 presents the log hazard that stands for the relative risk of the country assigning a new responsibility to an existing military agency.

$$log(H_y(t; X_i, y, z)) = W_i * y_{-i}([t-1])\beta_1 + W_i * z([t-1])\beta_2 + X_i([t-1])\beta_3 + log\lambda_y(t), \quad (3.2)$$

where: $log(H_y(t; X_i([t-1]), y_i([t-1])))$ is the log hazard that stands for the relative risk of country i assigning a new responsibility to an existing military agency at time t; $W_i * y_{-i}([t-1])$ is an $n \times n$ spatial weights matrix, explained above, that represents a dispersion variable which stands for a convolution of the country's "neighbors" that assign new responsibilities to existing military agencies; $W_i * z_{-i}([t-1])$ is an $n \times n$ spatial weights matrix that represents a dispersion variable which stands for a convolution of the country's "neighbors" that create new military military units; $X_i([t-1]) = [x_{1i}([t-1]), \ldots, x_{ki}([t-1])]'$ is a matrix of k exogenous variables; β_3 is a three-dimensional vector of coefficients; and $log\lambda(t)$ is baseline hazard. As explained earlier, I included the following non-diffusion regressors: (1) the number of the country's Internet users as a percentage of its total population in a given year (`Int_Users`); (2) the country's GDP per capita in a given year (`GDP_PerCapita`); and (3) the country's regime type (`Democracy`). I also use robust standard errors with clustering on the countries to account for time-varying coefficients. Lastly, to make my results easy to interpret, I standardize all continuous explanatory variables (all variables except `Democracy`).

Equation 3.3 presents the log hazard that stands for the relative risk of the country creating a new military unit.

$$log(H_z(t; X_i, y, z)) = W_i * y([t-1])\beta_1 + W_i * z([t-1])\beta_2 + X_i([t-1])\beta_3 + log\lambda_z(t), \quad (3.3)$$

where: $log(H_z(t; X_i([t-1]), y_i([t-1])))$ is the log hazard that stands for the relative risk of country i creating a new military agency at time t; and the rest of the variables are explained

above in Equation 3.2.

3.6 Findings

My central finding is that a country's choice of how to develop its military cyberapparatus is most consistently explained by the choices its allies made when publicly developing their own military cybercapability. The results summarized in Tables 3.1-3.3 suggest that the country's desire to complement its military cybercapabilities with those of its allies is likely a major driver of the diffusion of public military cybercapacity.

Table 3.1 displays results from models that consider only the influence of allies and the threat environment. Model 1, which presents a base model giving the effect of allies' cyberapparatuses, shows that both the development of new agencies and the assignment of old agencies with new responsibilities are positively correlated with `Assign` and `Create`. With additional controls (Model 2), we clearly start seeing the complementarity of allies: the country's allies that assigned new responsibilities are positively correlated with the country's decision to create a new military cybersecurity unit and the country's allies that created new agencies are positively correlated with the country's decision to assign a new responsibility to an existing military agency.

In addition to allies' cyberapparatuses, Models 3-6 of Table 3.1 also consider the effect of the country's threat environment on its decision to publicly develop its military cybercapacity. Model 3 shows that conventional threats are not correlated with `Assign` but are positively correlated with `Create`. This result remains consistent across all the models in Tables 3.1 and 3.3 and might point to the complementarity of conventional and digital fronts. Models 4-6 consider different measures of the cyberthreat environment. Model 4 shows that the cumulative number of attacks a country suffered in the years before it begins developing its military cyberapparatus (`Target`) is not correlated with `Assign` and `Create`. `Internet Users` is positively correlated with `Assign` and `Create` (Model 5). And `New`

Table 3.1: *Influence of allies and threat environment on the development of public military capacity (hazard ratios)*

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*	*Model 6*
	Base	*Base+ controls*	*Conventional threats*	`Target` *as proxy for cyberthreat environment*	`Internet Users` *as proxy for cyberthreat environment*	`Adversarial Cyberapparatus` *as proxy for cyberthreat environment*
			Dependent Variable: `Assign`			
`New Responsibilities Weighted by Allies`	1.138***	1.030	1.003	1.00	0.984	1.022
	(1.04, 1.25)	(0.82, 1.29)	(0.77, 1.30)	(0.77, 1.31)	(0.77, 1.26)	(0.80, 1.30)
`New Agencies Weighted by Allies`	1.508***	1.706***	1.697***	1.695***	1.662***	1.715***
	(1.21, 1.88)	(1.26, 2.30)	(1.26, 2.29)	(1.26, 2.28)	(1.18, 2.34)	(1.26, 2.33)
`Number of Alliances`	——	1.701* (0.97, 2.98)	1.593* (0.94, 2.71)	1.593* (0.94, 2.68)	1.736** (1.01, 2.98)	1.628* (0.95, 2.80)
`GDP_PerCapita (log)`	——	2.384*** (1.67, 3.39)	2.457*** (1.71, 3.53)	2.457*** (1.71, 3.53)	——	2.455*** (1.71, 3.52)
`Total MIDs (log)`	——	——	1.251 (0.87, 1.80)	1.300 (0.86, 1.97)	1.179 (0.80, 1.73)	1.148 (0.76, 1.73)
`Target`	——	——	——	0.883 (0.56, 1.38)	——	——
`Int_Users (log)`	——	——	——	——	4.564*** (2.03, 10.24)	——
`New Responsibilities Weighted by Adversaries`	——	——	——	——	——	1.141* (0.99,132)
`New Agencies Weighted by Adversaries`	——	——	——	——	——	0.131 (0.86,146)

Note: The dependent variable is `Assign`—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.

(a) Influence of Allies and Threat Environment on the Assignment of a New Cybersecurity Responsibility to an Existing Military Agency

Table 3.1: *Influence of allies and threat environment on the development of public military capacity (hazard ratios)*

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*	*Model 6*
	Base	*Base+ controls*	*Conventional threats*	`Target` *as proxy for cyberthreat environment*	`Internet Users` *as proxy for cyberthreat environment*	`Adversarial Cyberapparatus` *as proxy for cyberthreat environment*
			Dependent Variable: `Create`			
`New Responsibilities Weighted by Allies`	1.238*** (1.08, 1.42)	1.292*** (1.12, 1.48)	1.293*** (1.13, 1.49)	1.293*** (1.13, 1.49)	1.263*** (1.10, 1.45)	1.307*** (1.13, 1.51)
`New Agencies Weighted by Allies`	1.220*** (1.03, 1.45)	1.233 (0.93, 1.56)	1.21 (0.93, 1.56)	1.21 (0.85, 1.56)	1.158	1.211 (0.91, 1.61)
`Number of Alliances`	——	2.476*** (1.30,4.69)	1.998** (1.03,3.29)	1.998** (1.03,3.89)	2.148*** (1.12,4.13)	2.050*** (1.05,4.00)
`GDP_PerCapita (log)`	——	2.093*** (1.44,3.04)	2.22*** (1.51,3.28)	2.22*** (1.51,3.28)	——	2.295*** (1.54,3.42)
`Total MIDs (log)`	——	——	1.658***	1.49*** (1.11, 2.45)	1.567*** (1.14, 2.16)	1.500** (1.01, 2.23)
`Target`	——	——	——	1.010 (0.81, 1.26)	——	——
`Int_Users (log)`	——	——	——	——	3.825*** (2.02,7.25)	——
`New Responsibilities Weighted by Adversaries`	——	——	——	——	——	1.186*** (0.88,1.46)
`New Agencies Weighted by Adversaries`	——	——	——	——	——	1.134 (1.08,1.30)
Additional Controls	——	✓	✓	✓	✓	✓
Clustering by country	✓	✓	✓	✓	✓	✓
Concordance	0.689	0.777	0.791	0.792	0.813	0.794

Note: The dependent variable is `Create`—the country's decision to initiate the development of its military cyberapparatuses by creating a brand new unit. Results are from a Competing Risks Cox Proportional-Hazards Model. The reported values are the hazard ratios and their confidence intervals. There are 2,727 observations and 69 events. Additional controls include: `Democracy`, `IGO Membership`. They are no statistically significant across all models. All variables but `Democracy` are standardized. All results based on two-tailed tests. Models with `Internet Users` do not include `GDP Per Capita` because the two variables are highly correlated. See Appendix 3.8 for more details and a more detailed presentation of results. *p<0.1; **p<0.05; ***p<0.01

(b) Influence of Allies and Threat Environment on the Creation of a New Military Cybersecurity Agency

`Responsibilities Weighted by Adversaries` marginally increase the state's likelihood of developing its military cyberapparatus (Model 6). This result might suggest that the perception of cyberthreats is more influential than the cyberattacks that the country suffered.

Lastly, the models in Table 3.1 also show a robust positive correlation between the country's wealth (`GDP Per Capita`) and the number of alliances of which it is a member (`Number of Alliances`) and its decision to develop its military cyberapparatus.

Robustness Tests: Alternative Network Measures. I consider a number of alternative definitions of networks through which diffusion of military cybercapacity can occur. Tables 3.2 and 3.3, which present the obtained results, further demonstrate support for the theory of complementarity in alliances.

Model 1 in Table 3.2, which tests the cultural similarity explanation, demonstrates that new agencies developed by a country's linguistic partners are negatively correlated with its public development of a military cybersecurity apparatus. This result is not surprising, given the few widely-spoken languages in this interconnected world. Models 2-5 in Table 3.2 tests the similarity in foreign policy preferences as an alternative explanation of diffusion of military cybercapacity. Model 2, which considers the effect of UN partners, demonstrates that the agencies developed by such partners are negatively correlated with `Assign` and have no effect on `Create`. Models 3-5 show that new cybersecurity responsibilities assigned to existing military agencies of the country's trading partners are positively correlated with the country's choice to create a new military cybersecurity unit. This finding is robust across different specifications of trading partners. The results in Models 3-5, which demonstrate continued importance of alliances in the development of a country's military cyberapparatus even after controlling for other foreign policy preferences, provide further empirical support for the theory of complementarity in alliances.

This theory finds additional empirical support when testing it against a number of

Table 3.2: *Robustness of diffusion via military cyberapparatuses of allies: Alternative network measures (hazard ratios)*

(a) Influence of Cultural Similarity and Foreign Policy Preferences on the Assignment of a New Cybersecurity Responsibility

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*
	Cultural Similarity		*Foreign Policy Preferences*		
	Dependent Variable: `Assign`				
`New Responsibilities Weighted by Allies`	0.82	0.54	0.96	0.90	0.95
	(-0.74, 0.34)	(-1.6, 0.37)	(-0.33, 0.26)	(-0.63, 0.41)	(-0.35, 0.25)
`New Agencies Weighted by Allies`	1.64***	1.65***	1.75***	1.72***	1.75****
	(0.17, 0.82)	(0.14, 0.85)	(0.24, 0.88)	(0.27, 0.82)	(0.23, 0.89)
`New Responsibilities Weighted by Linguistic Partners`	0.46	——	——	——	——
	(-2.08, 0.54)				
`New Agencies Weighted by Linguistic Partners`	0.17***	——	——	——	——
	(-3.04, -0.46)				
`New Responsibilities Weighted by UN Partners`	——	0.98	——	——	——
		(-1.08, 1.03)			
`New Agencies Weighted by UN Partners`	——	0.92***	——	——	——
		(-0.14, -0.03)			
`New Responsibilities Weighted by Trade Partners (1)`	——	——	0.77**	——	——
			(-0.49, -0.04)		
`New Agencies Weighted by Trade Partners (1)`	——	——	0.84	——	——
			(-0.59, 0.24)		
`New Responsibilities Weighted by Trade Partners (2)`	——	——	——	1.15	——
				(-0.11, 0.39)	
`New Agencies Weighted by Trade Partners (2)`	——	——	——	0.46***	——
				(-1.24, -0.3)	
`New Responsibilities Weighted by Trade Partners (3)`	——	——	——	——	0.94
					(-0.35, 0.23)
`New Agencies Weighted by Trade Partners (3)`	——	——	——	——	0.96
					(-0.23, 0.15)
`Internet Users (log)`	1.18***	1.14***	1.17***	1.17***	1.18***
	(0.1, 0.24)	(0.05, 0.2)	(0.1, 0.23)	(0.09, 0.22)	(0.09, 0.23)
`Number of Alliances`	1.88**	1.47	1.64*	1.70**	1.61*
	(0.1, 1.16)	(-0.17, 0.94)	(-0.04, 1.02)	(0.02, 1.03)	(-0.06, 1.02)
`Total MIDs (log)`	1.22	1.36**	1.26	1.29	1.24
	(-0.16, 0.55)	(0.02, 0.59)	(-0.1, 0.56)	(-0.05, 0.56)	(-0.12, 0.55)

Note: The dependent variable is `Assign`—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.

Table 3.2: *Robustness of diffusion via military cyberapparatuses of allies: Alternative network measures (hazard ratios)*
(b) Influence of Cultural Similarity and Foreign Policy Preferences on the Assignment of a New Cybersecurity Responsibility

	Model 1	*Model 2*	*Model 3*	*Model 4*	*Model 5*
	Cultural Similarity		*Foreign Policy Preferences*		
	Dependent Variable: `Create`				
`New Responsibilities Weighted by Allies`	1.18**	1.23***	1.32****	1.28****	1.23***
	(0.02, 0.32)	(0.05, 0.37)	(0.11, 0.43)	(0.1, 0.39)	(0.07, 0.35)
`New Agencies Weighted by Allies`	1.14	1.11	1.18	1.15	1.21
	(-0.15, 0.4)	(-0.31, 0.52)	(-0.16, 0.49)	(-0.13, 0.41)	(-0.09, 0.48)
`New Responsibilities Weighted by Linguistic Partners`	1.04	——	——	——	——
	(-0.08, 0.16)				
`New Agencies Weighted by Linguistic Partners`	0.31*	——	——	——	——
	(-2.49, 0.14)				
`New Responsibilities Weighted by UN Partners`	——	0.61	——	——	——
		(-1.77, 0.78)			
`New Agencies Weighted by UN Partners`	——	1.00	——	——	——
		(-0.08, 0.09)			
`New Responsibilities Weighted by Trade Partners (1)`	——	——	1.44**	——	——
			(0.05, 0.68)		
`New Agencies Weighted by Trade Partners (1)`	——	——	1.09	——	——
			(-0.62, 0.8)		
`New Responsibilities Weighted by Trade Partners (2)`	——	——	——	1.23**	——
				(0.02, 0.4)	
`New Agencies Weighted by Trade Partners (2)`	——	——	——	1.27**	——
				(0.01, 0.47)	
`New Responsibilities Weighted by Trade Partners (3)`	——	——	——	——	1.31**
					(0.03, 0.51)
`New Agencies Weighted by Trade Partners (3)`	——	——	——	——	0.78
					(-0.6, 0.1)
`Internet Users (log)`	1.11***	1.10***	1.11***	1.11***	1.12***
	(0.05, 0.16)	(0.03, 0.16)	(0.05, 0.16)	(0.05, 0.16)	(0.05, 0.17)
`Number of Alliances`	2.40***	2.05**	2.20**	2.16**	2.13**
	(0.21, 1.54)	(0.1, 1.34)	(0.18, 1.4)	(0.15, 1.38)	(0.14, 1.38)
`Total MIDs (log)`	1.61***	1.63***	1.59***	1.62***	1.59***
	(0.14, 0.81)	(0.16, 0.81)	(0.13, 0.81)	(0.15, 0.81)	(0.13, 0.8)
Additional Controls	✓	✓	✓	✓	✓
Clustering by country	✓	✓	✓	✓	✓
Concordance	0.832	0.831	0.826	0.823	0.823

Note: The dependent variable is `Create`—the country's decision to initiate the development of its military cyberapparatuses by creating a brand new unit. Results are from a Competing Risks Cox Proportional-Hazards Model. There are 2,727 observations and 69 events. *p<0.1; **p<0.05; ***p<0.01

Table 3.3: *Robustness of diffusion via military cyberapparatuses of allies: Alternative network measures (hazard ratios)*

(a) Influence of Expert Communities, Geography, and Regime Similartiy on the Assignment of a New Cybersecurity Responsibility

	Model 6	*Model 7*	*Model 8*	*Model 9*	*Model 10*
	Expert Communities	*Geography*		*Regime Similarity*	
	Dependent Variable: `Assign`				
`New Responsibilities Weighted by Allies`	0.89	0.88	0.95	0.96	0.96
	(-0.51, 0.29)	(-0.53, 0.28)	(-0.37, 0.27)	(-0.36, 0.27)	(-0.35, 0.26)
`New Agencies Weighted by Allies`	1.74**	1.71***	1.76****	1.76****	1.74***
	(0.23, 0.89)	(0.21, 0.86)	(0.24, 0.89)	(0.26, 0.87)	(0.28, 0.83)
`New Responsibilities Weighted by IGO Partners`	1.13	——	——	——	——
	(-0.3, 0.55)				
`New Agencies Weighted by IGO Partners`	0.99	——	——	——	——
	(-0.4, 0.39)				
`New Responsibilities Weighted by Neighbors (1)`	——	1.13	——	——	——
		(-0.4, 0.65)			
`New Agencies Weighted by Neighbors (1)`	——	1.29	——	——	——
		(-0.25, 0.76)			
`New Responsibilities Weighted by Neighbors (2)`	——	——	0.89	——	——
			(-0.38, 0.14)		
`New Agencies Weighted by Neighbors (2)`	——	——	0.70*	——	——
			(-0.74, 0.02)		
`New Responsibilities Weighted by Regime Partners (1)`	——	——	——	0.73	——
				(-0.9, 0.27)	
`New Agencies Weighted by Regime Partners (1)`	——	——	——	0.94	——
				(-0.99, 0.86)	
`New Responsibilities Weighted by Regime Partners (2)`	——	——	——	——	0.63
					(-1.01, 0.09)
`New Agencies Weighted by Regime Partners (2)`	——	——	——	——	0.75
					(-0.99, 0.41)
`Internet Users (log)`	1.17***	1.16***	1.18***	1.18***	1.18***
	(0.09, 0.23)	(0.08, 0.22)	(0.1, 0.23)	(0.1, 0.23)	(0.1, 0.23)
`Number of Alliances`	1.60	1.56	1.71*	1.64*	1.65*
	(-0.1, 1.04)	(-0.1, 0.99)	(0.01, 1.06)	(-0.04, 1.03)	(-0.04, 1.04)
`Total MIDs (log)`	1.27	1.28	1.27	1.24	1.24
	(-0.08, 0.57)	(-0.08, 0.57)	(-0.09, 0.57)	(-0.11, 0.54)	(-0.12, 0.54)

Note: The dependent variable is `Assign`—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.

Table 3.3: *Robustness of diffusion via military cyberapparatuses of allies: Alternative network measures (hazard ratios)*
(b) Influence of Expert Communities, Geography, and Regime Similarity on the Assignment of a New Cybersecurity Responsibility

	Model 6	*Model 7*	*Model 8*	*Model 9*	*Model 10*
	Expert Communities	*Geography*		*Regime Similarity*	
	Dependent Variable: `Create`				
`New Responsibilities Weighted by Allies`	1.28****	1.18**	1.27***	1.28****	1.28****
	(0.11, 0.38)	(0.01, 0.33)	(0.1, 0.38)	(0.11, 0.39)	(0.1, 0.39)
`New Agencies Weighted by Allies`	1.16	1.06	1.20	1.19	1.20
	(-0.18, 0.48)	(-0.37, 0.49)	(-0.11, 0.47)	(-0.12, 0.46)	(-0.11, 0.47)
`New Responsibilities Weighted by IGO Partners`	1.44	——	——	——	——
	(-0.19, 0.91)				
`New Agencies Weighted by IGO Partners`	0.82	——	——	——	——
	(-1.22, 0.82)				
`New Responsibilities Weighted by Neighbors (1)`	——	1.83***	——	——	——
		(0.15, 1.06)			
`New Agencies Weighted by Neighbors (1)`	——	1.12	——	——	——
		(-0.24, 0.45)			
`New Responsibilities Weighted by Neighbors (2)`	——	——	1.01	——	——
			(-0.19, 0.21)		
`New Agencies Weighted by Neighbors (2)`	——	——	0.88	——	——
			(-0.41, 0.16)		
`New Responsibilities Weighted by Regime Partners (1)`	——	——	——	0.87	——
				(-0.62, 0.33)	
`New Agencies Weighted by Regime Partners (1)`	——	——	——	0.70	——
				(-1.52, 0.8)	
`New Responsibilities Weighted by Regime Partners (2)`	——	——	——	——	1.01
`New Agencies Weighted by Regime Partners (2)`	——	——	——	——	0.78
					(-1.24, 0.74)
`Internet Users (log)`	1.10*** (0.04, 0.16)	1.09*** (0.02, 0.15)	1.12*** (0.05, 0.17)	1.12*** (0.05, 0.17)	1.12*** (0.05, 0.17)
`Number of Alliances`	2.07** (0.07, 1.38)	2.11** (0.15, 1.35)	2.09** (0.11, 1.36)	2.09** (0.11, 1.36)	2.06** (0.11, 1.34)
`Total MIDs (log)`	1.69*** (0.17, 0.88)	1.76*** (0.21, 0.92)	1.64*** (0.16, 0.83)	1.60*** (0.14, 0.81)	1.61*** (0.15, 0.81)
Additional Controls	✓	✓	✓	✓	✓
Clustering by country	✓	✓	✓	✓	✓
Concordance	0.822	0.826	0.825	0.819	0.821

Note: The dependent variable is `Create`—the country's decision to initiate the development of its military cyberapparatuses by creating a brand new unit. There are 2,727 observations and 69 events. Additional controls include: `Democracy`, `IGO Membership`. They are no statistically significant across all models. *p<0.1; **p<0.05; ***p<0.01

additional alternative explanations in Table 3.3. Specifically, Model 6 finds no support for the expert communities explanation. Expert communities might become more instrumental beyond the initiation phase when countries start shaping up their military cyberapparatuses and specialize in certain types of cybercapabilities. Models 7-8 in Table 3.3 find no robust support for the influence of geographic neighbors, suggesting that similarly to language, geographic proximity is an unimportant factor in the information age. The last alternative explanation—regime similarity—also finds no support (Models 9-10 in Table 3.3). The lack of robust empirical support for these alternative explanations provides further evidence for the theory of complementarity in alliances.

In addition to the alternative network specifications, all models in Tables 3.2 and 3.3 include additional controls. Similar to the earlier obtained results (Table 3.1), all models in Tables 3.2 and 3.3 demonstrate (1) a robust positive correlation between `Internet Users` and both `Assign` and `Create`; (2) a robust positive correlation between `Number of Alliances` and `Create`; and (3) a robust positive correlation between `Total MIDs` and `Create`.

3.7 Discussion and Implications

This research asks a basic question: *What drives a state's decision to initiate the development of its military cyberapparatus and how does the state decide to initiate it?* It demonstrates that a country's allies play a vital role. The responses to allied behavior follow the logic of complementarity. If the country's allies signal toughness by creating new units, then the country may not need to do so and assigns cybersecurity responsibilities to an existing military agency. But if the country's allies take a softer approach by assigning cybersecurity responsibilities to an existing military agencies, then the country has an added incentive to create a new cybersecurity agency in order to signal toughness.

The genuineness of this signal, however, is the question. Even when a nation openly

speaks about possetting offensive capabilities, its leadership might prefer using more traditional tools whose value does not diminish after the first use to help their allies. Moreover, allies are reluctant to share their offensive capabilities. Since the nature of cyberoperations requires more secrecy than traditional capabilities, even allies as close as the FiveEye members tend not to completely share their offensive cybercapabilities (Kostyuk 2019*b*: # 56, 57). Countries are also reluctant to share their military defensive systems with their allies. Even in the cases when these systems can be replicated which is easier said than done, countries are particularly careful in sharing them with their allies due to the fear of a leak or the risk of the systems being kept insecure.

My findings also demonstrate that an increase in the number of militarized interstate disputes that the country suffered in a prior year increases the likelihood that it creates a new military cybersecurity unit this year. This finding points to the fact that countries might be developing their military cybercapabilities to respond to conventional threats. Further research is needed to investigate whether an increase in MIDs leads to an increase of the country's conventional military capability. If it does not, this finding might point to the substitutability of conventional and military tools.

As I presented the first comprehensive analysis of a complex political phenomenon, future research should delve further into this topic. Several avenues of research present themselves. First is the continued development of military cybercapability. While this research only looks at the country's initial step, countries tend not to stop right there. For instance, India's Ministry of Defense started dealing with cybersecurity since at least 2004 and it did not create the Defense Cyber Agency within this ministry until 2019. The Lithuanian Ministry of National Defence became responsible for cybersecurity in 2008, but it did not create the Cyber Security and Information Technology Department until 2014. While the author attempted to apply a multi-state event history model to understand what drives the country's decision to transition from assigning a new responsibility to creating a new

unit, currently available data is not sufficient to fully explain this complex phenomenon. Researchers should further pursue this question when such data becomes available.

Second is unit size and actual capacity. While current research remains agnostic to the unit size, future research should understand how the effect of a signal changes based on the unit type and purpose. How do nations perceive the fact that the Dutch Ministry of Defense created its Joint Information Facility Command (JIVC) in 2012 and its Joint Sigint Cyber Unit (JSCU) in 2014? What if a nation does not attempt to send a signal and simply restructures its bureaucracy? I would expect that even if these re-organizational changes are not intended to send a signal, other nations will inherently update their existing beliefs about the state's cybercapability. Specifically, unit restructuring often results in an increased capacity because it achieves better integration of capabilities and coordination (Kostyuk 2019*b*: #18).

Moreover, because of the limitation of its design, this research was not able to delve into military culture or organizational factors that drive military innovation. Future qualitative studies should carefully evaluate how these factors contribute to the development of military cyberapparatuses. Lastly, researchers should also look at the capability within and outside of military agencies to investigate which agencies receive more weight when its comes to dealing with cybersecurity challenges that often require intergovernmental cooperation. The choice of making a specific ministry or agency responsible for cybersecurity is important because different agencies have different weights when it comes to intergovernmental cooperation meant to deal with security issues. "Prestige for historical reasons or legal prerogatives" drive this weight (Kostyuk 2019*b*: # 23).

Much of our current understanding of international politics rests on the assumption that state behavior is shaped by the threat of war and the pursuit of military capability. The empirical study of politics thus depends on measures of capability, which play a pivotal role in war causation, arms races, alliance formation, conflict duration, or crisis escalation, among

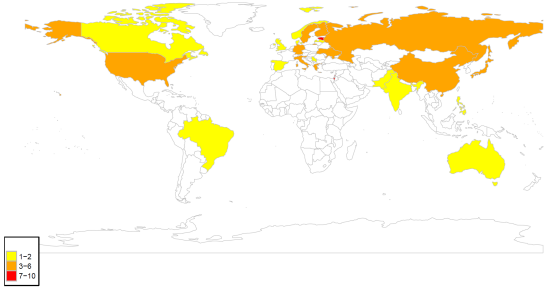
others. While future research on military cybercapacity can add more nuanced explanations of military effectiveness, innovation, force structure, alliance formation, and the outbreak of war, we should also consider important questions regarding norms for cyberwarfare, the obligations of states regarding the application of offensive cybercapabilities, and the applicability of existing laws of war and norms on the use of force in cyberspace. Uncontrolled capacity can lead to disastrous effect.

3.8 Appendix

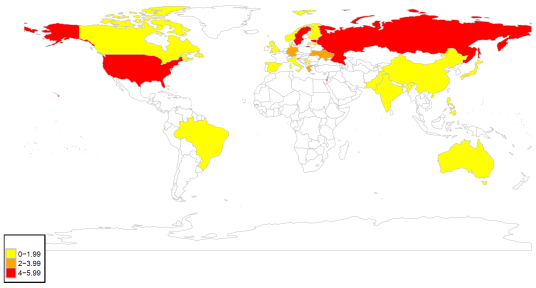
Elite Interviews: Causes of Military Cybercapability

To investigate the factors that drive a country's choice to create cyber offensive capabilities in the form of military units, I conducted sixty-four interviews with cybersecurity experts from twenty-five countries in 2018.[17] Most of these experts either have a current or past government affiliation. I personally conducted these interviews in person or via Skype or email. Figure 3.5a displays the number of interviews I conducted in each country. The most interviews I conducted in a given country was nine (in Estonia and Israel). Figure 3.5b displays the total duration of my interviews by country. My interviews, on average, lasted for about an hour, with the shortest interviews lasting for fifteen or thirty minutes. These

Figure 3.5: *Summary of the Interviews*



(a) Total Number of Interviews by Country



(b) Total Duration by Country (in hours)

[17] The IRB approval is #HUM00127749 (February 14, 2018).

interviews point a few common themes that I explore in the theoretical section of the main manuscript (Section 3.2).

Data

Data Sources: Threat Environment

Since countries can use military cybersecurity units to deal with conventional threats and digital threats, I consider both kinds of threats in my analysis.

To consider the effect of conventional military threats, I use Maoz (2005)'s data on Militarized Interstate Disputes (MID) to create the total number of MIDs that a country experienced in the year preceding its choice to cyber-militarize (`Total MIDs`). Gochman and Maoz (1984, 587) defines MIDs as "interactions between or among states involving threats to use military force, of military force, or actual uses of military force." Because the MID data treats incidents that involve police and border control as a use of force (e.g., disputes on the U.S.-Canadian border that involve fishing vessels), I exclude such events from the final dataset by removing events with an outcome labeled as "released (for seizure)."

I also considered two alternative datasets to serve as a proxy for a country's threat environment. The first dataset is Klein, Goertz and Diehl (2006)'s data on state rivalries, which has only been updated until 2001 and is not suitable for my analysis, which focuses on the 1999-2018 period. The second dataset is the International Crisis Behavior (ICB) data (version 12) that contains information on 476 international crises during 1918-2015 (Brecher, Wilkenfeld et al. 1997; Brecher et al. 2016). There are two notable difference between an MID and an international crisis: (1) perception, and (2) (the threat or) use of force. Perception is the key in determining whether the situation is defined as a crisis. One party might perceive a situation as an international crisis whereas an adversary might not perceive it as a crisis. While an MID evolves from "an explicit threat, display, or use of force" Gochman and Maoz (1984, 587), the threat or use of military force is not a necessary condition for a

crisis to occur. Indeed, political acts, such as "subversion, alliance formation by adversaries, diplomatic sanctions, severance of diplomatic relations, [or] violation of treaty," trigger about a quarter of foreign policy crises (Hewitt 2003, 671-672). These two distinctions indicate that the events in the ICB dataset is not a good proxy for understanding the threat environment in the context of this analysis.

Following Craig (2018), I use Valeriano and Maness 2018's Dyadic Cyber Incident Dataset (DCID) (version 1.5)[18] as an alternative way to measure a country's threat environment. Using this data, I create the following two variables: (1) the cumulative number of large, known cybercampaigns that a country experienced in all years preceding its change(s) of a domestic military cybersecurity apparatus (`Target`); and (2) the cumulative number of large, known cybercampaigns attributed to a country in all years preceding its change(s) of a domestic military cybersecurity apparatus (`Attacker`).

There are two main criticisms of any dataset of cyberoperations. The first one—typical for any conflict data—is reporting bias (Weidmann 2016). To address this concern, the DCID authors apply a well-established practice in conflict studies—the use of multiple sources to record an event. Despite this careful approach, reporting bias could be a valid concern for a dataset that collects information on daily cyberopations but less of an issue for the DCID data that records known, large cybercampaigns, defined as an accumulation of cyberattacks meant to achieve strategically important goals. Under reporting is less of an issue because it is difficult not to notice a large event. For instance, it is much easier to check the validity of the 2007 cybercampaign against Estonia than to find information on each individual cyberattack that Estonia experienced during the three-week-long cybercampaign. Moreover, it is hard not to notice a full-scale cybercampaign, especially when a significant amount of time has passed since the start of the campaign—between twenty and six years (i.e., the 2000-2016

[18] DCID is one of two available datasets on cyberoperations. I do not use the Council on Foreign Relations' Cyber Operations Tracker (COT)—the second dataset on cyberoperations—to conduct my robustness checks because the majority of incidents in this dataset contain events executed by non-state actors for criminal purposes and examples of governments using spyware to track actions of opposition groups.

period), for the attacks in DCID. Similarly, English-speaking outlets are more likely to cover a full-scale cybercampaign than individual, low-level cyberattacks. Overreporting is less of an issue because it is also much easier to use multiple sources to mistakenly record an individual cyberattack, which often lacks specific details, multiple times than to overreport large-scale cybercampaigns.

The second one, unique for cyberoperations, is the difficulty of their attribution. Cyber-attribution is no longer a technical problem but a costly political decision (Clark and Landau 2011; Rid and Buchanan 2015). Some nations have the capacity to attribute cybeoperations. Those nations that do not have such capacity often benefit from attribution by private companies that are always eager to go after large cybercampaigns—those in DCID—to increase their revenue. To address the possibility that a country might change its military cyberapparatus only when it discovers that it has been a target of cyberoperations from outside sources, I supplement the start and end dates of the DCID's cybercampaigns with the date of the campaigns' public discovery. To sum it up, despite its limitations, DCID data serve as a good proxy for a government's overall cyberthreat environment.

Data Sources: Military Alliances

The most popularly used datasets on military alliances are Leeds et al. (2002)'s Alliance Treaty Obligations and Provisions and Correlates of War (COW) Project's data on formal alliances (version 4.1) (Gibler 2008). Since the period I am interested in is quite recent, ATOP Alliance dataset, which contains a more detailed description of recent events and is more comprehensive, is more suitable for my analysis. Thus I use ATOP for my main analysis and cautiously proceed with running my robustness checks using COW Alliances. I use both datasets to create a weighted average effect of the allies' cybersecurity organizations on the country's choice of military cybersecurity organizations.

Leeds et al. (2002, 238)'s Alliance Treaty Obligations and Provisions data defines *alliances*

as "written agreements, signed by official representatives of at least two independent states, that include promises to aid a partner in the event of military conflict, to remain neutral in the event of conflict, to refrain from military conflict with one another, or to consult/cooperate in the event of international crises that create a potential for military conflict." The last observation in the data is coded as of 2016. I use ATOP to create a weighted average effect of the cybersecurity organizations adopted by a country's allies in a period prior the country's choice of cyber-militarization. For instance, `New Responsibilities Weighted by Allies` records the weighted average effect of the country's allies' decision to assign new cybersecurity responsibility to an existing military agency. `New Units Weighted by Allies`: records the weighted average effect of the country's allies' decision to create new a cybersecurity military agency.

Similarly to ATOP, Correlates of War (COW) Project's data on formal alliances (version 4.1) differentiates between a defense, neutrality, non-aggression, or entente (i.e., consultation) agreement (Gibler 2008). Even though COW Alliances and ATOP code the same type of alliances, they differ in a few notable ways. First, ATOP extends to 2016 and the last observation in COW is as of 2012. Second, COW lacks offensive agreements, but this does not present a challenge for this study. Third, some of the alliances in ATOP are not in COW. Fourth, ATOP covers allies of 186 countries during the studied period whereas COW covers only 148 countries. One of the explanations for this discrepancy could be that "Ten of the 745 alliances in the ATOP dataset, however, would not qualify for inclusion based on the COW list of independent states; at least one of the members of these ten alliances is a member of the international system according to Gleditsch and Ward but not according to COW" Leeds (2005, 8). As a result, ATOP is a more comprehensive data set during the time frame that my study explores.

United Nations General Assembly Voting data

Votes in the United Nations General Assembly (UNGA) have been commonly used to construct a measure of state foreign policy preferences (Bailey, Strezhnev and Voeten 2017; Ball 1951; Gartzke 1998; Lijphart 1963; Moon 1985; Russett 1966; Signorino and Ritter 1999). UNGA resolutions cover a variety of topics but Voeten, Strezhnev and Bailey (2017) grouped them into six main topics:

1. `ME`: votes related to the Palestinian conflict;
2. `NU`: votes related to nuclear weapons and nuclear material;
3. `DI`: votes related to arms control and disarmament;
4. `CO`: votes related to colonialism;
5. `HR`: votes related to human rights; and
6. `EC`: votes related to (economic) development.

Using this distinction, I create six categories: `Palestine`, `Nuclear`, `Disarmament`, `Colonialism`, `EconDev`, and `HumanRights`. These votes could be further grouped into two categories: (1) those that have a non-conflict angle (i.e., colonialism, human rights, and economic development) (`UN Partners (1)`) and (2) those that have a conflict angle (i.e., the Palestinian conflict, nuclear weapons, and arms control) (`UN Partners (2)`). These six categories constitute 92% of all resolutions adopted at the UN. I also create a category (`UN Partners (3)`) in which I place resolutions that do not fall into the six categories identified above.

Since there are many resolutions on a given subject in a given year, I distribute the votes between -1 and 1 ("yes"-"+1," "abstain"-"0," and "no"-"-1"), summarize them by topic and year, and divide by the total number of resolutions on a given topic in a given year. I use the obtained value to create the weighted average effect of the voting patterns at the UNGA on the country's choice to cyber-militarize. Similarly, I combine these issue variables

with `Assign` and `Create` to create the weighted average effect of the country's UN partners' choices of cybersecurity organizations on the country's choice of cyber-militarization. The UNGA country-level data was last updated in 2018.

Data Sources: Trade

I use the following three measures to identify the country's trading partners:

1. `Trading Partners (1)`: the amount of bilateral trade between two countries, taken from the World Bank ;
2. `Trading Partners (2)`: the number of signed bilateral investment treaties between two nations (Graham and Tucker 2019); and
3. `Trading Partners (3)`: the number of signed preferential trade agreements between two nations (Graham and Tucker 2019).

Similarly, I record the weighted average effect of cybersecurity units adopted by the country's trading partners in a period prior to the country developing its first military cybersecurity agency (`New Responsibilities/Units Weighted by Trading Partners (1/2/3)`). I use `New Responsibilities/Units Weighted by Trading Partners (1)` in my main analysis and `New Responsibilities/Units Weighted by Trading Partners (2)` and `New Responsibilities/Units Weighted by Trading Partners (3)` to run robustness checks.

Data Sources: Cultural Similarity

Using Graham and Tucker (2019)'s World Economics and Politics Dataverse (WEPD), I create the following two proxies for cultural similarity. First is a dummy variable that takes a value of "1" when two nations share the same official language. Second is a dummy variable that takes a value of "1" when two nations have similar colonial experiences. I

use both variables to create a weighted average effect of the cybersecurity organizations adopted by a country's linguistic and colonial partners in a period prior the country's choice of cyber-militarization:

- `New Responsibilities Weighted by Linguistic Partners`: records the weighted average effect of the country's linguistic partner's decision to assign a new cybersecurity responsibility to an existing military agency;
- `New Units Weighted by Linguistic Partners`: records the weighted average effect of the country's linguistic partner's decision to create a new cybersecurity military agency;
- `New Responsibilities Weighted by Colonial Partners`: records the weighted average effect of the country's colonial partner's decision to assign a new cybersecurity responsibility to an existing military agency;
- `New Units Weighted by Colonial Partners`: records the weighted average effect of the country's colonial partner's decision to create a new cybersecurity military agency.

Data Sources: Geography

To create a weighted average effect of the military cybersecurity organizations created by a country's geographic neighbors, I identify the country's geographic neighbors in the following five ways:

- the inverse distance between the two capitals (`Neighbors (1)`),
- the squared inverse distance between the two capitals (`Neighbors (2)`),
- the logarithmized inverse distance between the two capitals (`Neighbors (3)`),

- a dummy variable that identifies whether two countries share a land border or are separated by at most 100 miles of water (`Neighbors (4)`) (Stinnett et al. 2002), and
- a dummy variable that identifies whether two countries share a land border or are separated by at most 400 miles of water (`Neighbors (5)`) (Stinnett et al. 2002).[19]

Data Sources: Communication Channels and Expert Communities

Discussions related to national security and military capabilities tend to happen on bilateral and multilateral levels. To isolate such multilateral exchanges, I use Pevehouse et al. (2019)'s dyadic data that has information on countries' joint memberships in 534 IGOs between 1816 and 2014. Focusing on the 1999-2014 period, I choose only those IGOs whose primarily focus is security, defense, and peace. Some of these organizations have security as their main and only mission whereas others focus on other areas, in addition to promoting security and cooperation among its members. Here is the list of thirty-three IGOs that I selected from the IGO dataset:

1. *African Ministers' Council on Water* (AMCOW), formed "primarily to promote cooperation, security, social and economic development and poverty eradication among member states through the effective management of the continent's water resources and provision of water supply services";[20]
2. *Agency for the Prohibition of Nuclear Weapons in Latin America* (OPANAL);
3. *Arab Cooperation Council* (ACC), created by North Yemen, Iraq, Jordan, and Egypt in the 1989 and became instinct in the 1990s;
4. *Association of South East Asian Nations* (ASEAN);

[19] I have also considered using 200, 300, and 500 miles as my cut-off points but because these variables were perfectly separated with my dependent variables in some of my models, I decided to include these variables into my robustness checks.

[20] Taken from AMCOW' website: https: https://www.amcow-online.org/index.php?option=com_content&view=article&id=69%3Aabout-amcow&catid=34%3Aabout-amcow&Itemid=27&lang=en

5. *Baltic Peacekeeping Battalion* (BALTBAT);[21]
6. *Central European Initiative* (CEI);
7. *Collective Security Treaty Organization* (CSTO);
8. *Commonwealth of Independent States* (CIS);
9. *Commonwealth Secretariat* (ComSec) that focuses on "development, democracy and peace";[22]
10. *Community of Portuguese-Speaking Countries* (CPSC) that focuses on cooperation in all areas, including defense;
11. *Conference on Interaction and Confidence-Building Measures in Asia* (CICA);
12. *Council of the Baltic Sea States* (CBSS) that focuses on creating a safe and secure region;
13. *Euro Atlantic Partnership Council* (EAPC);
14. *European Institute for Peace* (EIP);
15. *Inter-American Defense Board* (IADefB);
16. *International Civil Defence Organization* (ICivDO);
17. *League of Arab States* (LOAS), currently the Arab League;
18. *Non-Aligned Movement* (NAM);
19. *North Atlantic Treaty Organization* (NATO);
20. *Organization for African Unity* (OAU);
21. *African Union* (AU);
22. *Organization for Security and Cooperation in Europe* (OSCE);

[21] For more information, see Sapronas (1999).
[22] *Source:* https://thecommonwealth.org/about-us/secretariat.

23. *Organization of the Islamic Conference* (OIC);
24. *Regional Centre on Small Arms and Light Weapons* (RECSA);
25. *Regional Commonwealth in the Field of Communications* (RCFC), focuses on the issues in the field of information and communication technologies (ICT);
26. *Shanghai Cooperation Organisation* (SCO);
27. *Secretariat of the Commission for East African Cooperation* (EAC);
28. *South Asian Association for Regional Cooperation* (SAARC);
29. *Union of the Mediterranean* (UM);
30. *United Nations* (UN);
31. *Warsaw Treaty Organization* (WPact), dissolved in 1991;
32. *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (Wassen); and
33. *Western European Union* (WEU).

I use the total number of IGOs out of this list of thirty-three to which countries have a joint membership to create a weighted average effect of cybersecurity organizations adopted by governments that share IGO memberships. Similarly, I distinguish whether governments with joint IGO membership assigned a new cybersecurity responsibility to an existing military agency (`New Responsibilities Weighted by IGO Partners`) or created a new military cybersecurity unit (`New Units Weighted by IGO Partners`) in the year prior to the year when the country makes changes to its military cyberapparatus.

Data Sources: Legitimacy, Prestige, or Modern Behavior

To measure the effect of prestige or modern behavior on the creation of a new cybersecurity military apparatus, I use thirty-three intergovernmental organizations (IGOs) that promote

security, defense, and peace, explained above, from Pevehouse et al. (2019)'s data. I have also considered controlling for the cumulative sum of new and assigned cybersecurity agencies created in the year prior to the country's development of its military cyberapparatus. However, because my survival analysis includes time-varying covariates and this variable is the same across all nations and only differs by year, I opted out of running my robustness checks using the variable that has no country-specific variation.

Summary Statistics and Correlation Plots

Figure 3.6 depicts the correlation plot for the diffusion variables with newly-created military units and controls. Table 3.4 shows the summary statistics for the main explanatory variables and controls. All variables besides `Democracy` have been re-scaled to make it easy to interpret the obtained results.

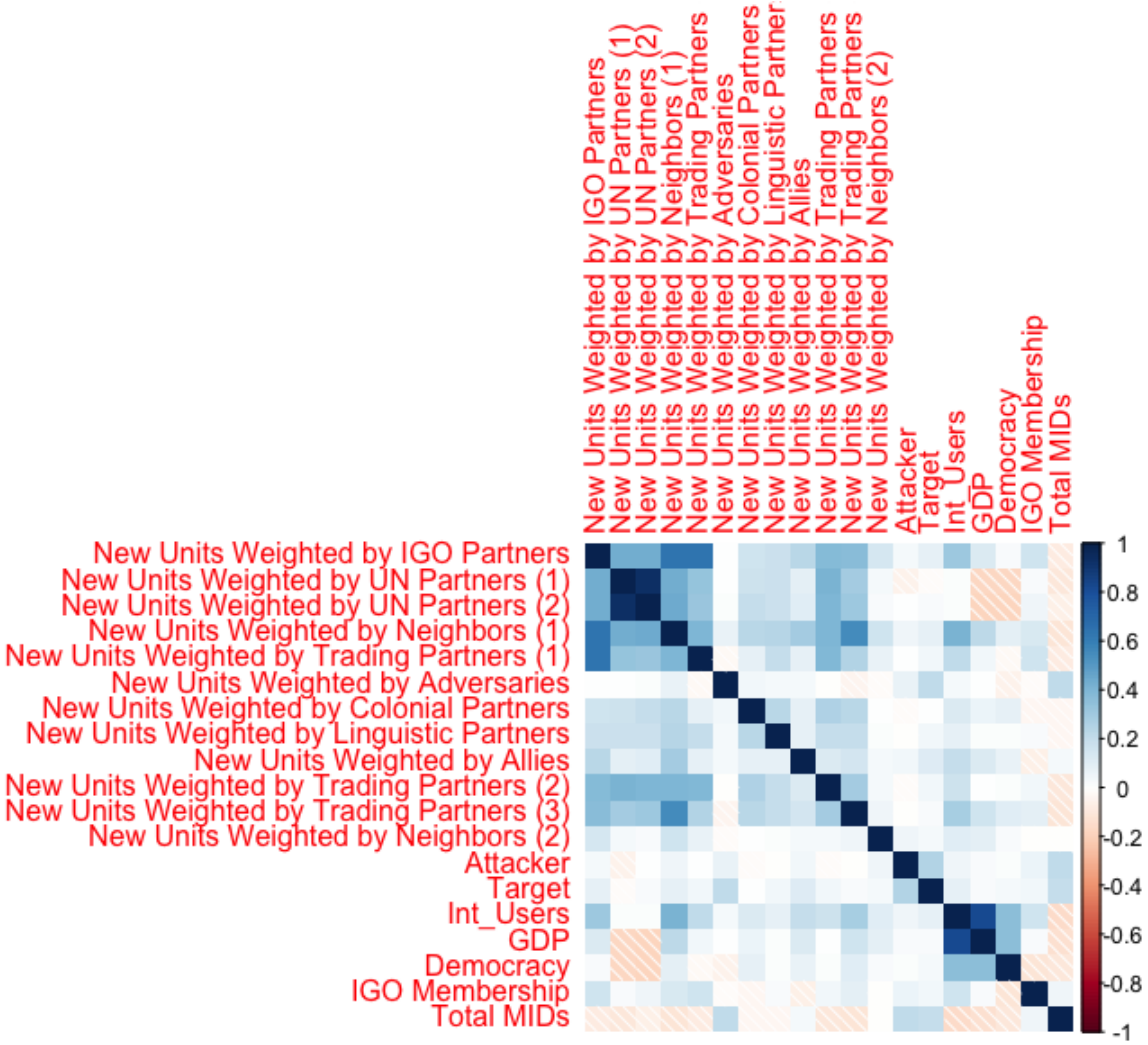
Empirical Strategy

Competing Risks Cox Proportional-Hazards Model. One assumption of the Cox Proportional-Hazards (CPH) model is that no two countries adopt policies at the same time. To "break" possible ties, I use the Efron approximation in my model as it is a tighter approximation to the exact marginal. Another assumption of the CPH model is that the hazard ratios do not vary over time. I use the Therneau and Grambsch nonproportionality test, which uses scaled Schoenfeld residuals, to test this assumption (Grambsch and Therneau 1994). Since some of variables violate this assumption (i.e., `New Units Weighted by UN Partners (1)`, `Attacker`, `GDP_PerCapita`), I interact these variables with the starting time (i.e., `tstart`) to address this issue (Therneau, Crowson and Atkinson 2020). Despite following this recommendation by the authors of the R package, the effect of these variables should be generally understood as an average effect over the entire studied period and not as a conditional effect over a particular period of time.

Table 3.4: *Summary Statistics*

	Minimum	*Median*	*Mean*	*Maximum*
New Responsibilities Weighted by IGO Partners (lag)	-0.6308	-0.6308	0.0000	12.3061
New Units Weighted by IGO Partners (lag)	-0.4848	-0.4848	0.0000	11.9438
New Responsibilities Weighted by UN Partners (1) (lag)	-0.9178	-0.8654	0.0000	2.9845
New Units Weighted by UN Partners (1) (lag)	-1.4824	-0.6836	0.0000	2.7759
New Responsibilities Weighted by UN Partners (2) (lag)	-0.9284	-0.5849	0.0000	2.8791
New Units Weighted by UN Partners (2) (lag)	-1.4622	-0.6394	0.0000	3.2785
New Responsibilities Weighted by Neighbors (1) (lag)	-0.5020	-0.4152	0.0000	29.2884
New Units Weighted by Neighbors (1) (lag)	-0.6243	-0.4881	0.0000	29.6857
New Responsibilities Weighted by Trading Partners (1) (lag)	-0.3636	-0.3636	0.0000	10.7431
New Units Weighted by Trading Partners (1) (lag)	-0.4655	-0.4655	0.0000	6.3528
New Responsibilities Weighted by Adversaries (lag)	-0.0730	-0.0730	0.0000	17.2849
New Units Weighted by Adversaries (lag)	-0.1330	-0.1330	0.0000	11.5740
New Responsibilities Weighted by Colonial Partners (lag)	-0.2243	-0.2243	0.0000	7.0749
New Units Weighted by Colonial Partners (lag)	-0.2243	-0.2243	0.0000	7.0749
New Responsibilities Weighted by Linguistic Partners (lag)	-0.1926	-0.1926	0.0000	20.3103
New Units Weighted by Linguistic Partners (lag)	-0.2725	-0.2725	0.0000	17.5567
New Responsibilities Weighted by Allies (lag)	-0.3061	-0.3061	0.0000	17.3049
New Units Weighted by Allies (lag)	-0.3586	-0.3586	0.0000	7.5303
New Responsibilities Weighted by Trading Partners (2) (lag)	-0.4439	-0.4439	0.0000	19.6833
New Units Weighted by Trading Partners (2) (lag)	-0.5430	-0.5430	0.0000	9.9334
New Responsibilities Weighted by Trading Partners (3) (lag)	-0.5026	-0.5026	0.0000	9.6377
New Units Weighted by Trading Partners (3) (lag)	-0.5398	-0.5398	0.0000	9.5450
New Responsibilities Weighted by Neighbors (2) (lag)	-0.1081	-0.1081	0.0000	11.6679
New Units Weighted by Neighbors (2) (lag)	-0.1373	-0.1373	0.0000	10.1527
Attacker (lag)	-0.1136	-0.1136	0.0000	22.0658
Target (lag)	-0.1541	-0.1541	0.0000	19.5390
GDP_PerCapita (log)	-2.3366	-0.0905	0.0000	2.4427
Int_Users (log)	-1.9551	0.2047	0.0000	1.3651
Democracy	0.0000	1.0000	0.5603	1.0000
IGO Membership (lag)	-2.6714	-0.5018	0.0000	3.2950
Total MIDs (lag, log)	-0.5003	-0.5003	0.0000	8.3295

Figure 3.6: *Correlation Plot: Yearly Data*



Moreover, while the Therneau and Grambsch non-proportionality test detects a number of specification errors in addition to non-proportionality, it may yield a false-positive test if the model is specified incorrectly (Therneau, Grambsch and Fleming 1990; Grambsch and Therneau 1994; Therneau and Grambsch 2000). I ran robustness checks that use the inverse hyperbolic sine function for continuous covariates to address that possibility.

Model Selection. Given that some of my predictors are highly correlated, as demonstrated

by Figure 3.6, I use Akaike's selection criteria to first select the control variables that best explain my variables of interest (`Assign` and `Create`). I start with a model that automatically includes clustering by country but selects between the type of the main explanatory variables (`New Responsibilities Weighted by Allies`, `New Units Weighted by Allies`) and control variables (`Target`, `Attacker`, `GDP_PerCapita`, `Int_Users`, `Democracy`, `IGO Membership`, and `Total MIDs`). Table 3.5 displays the AIC values for the best five models with the lower AIC value suggesting a better model fit. It confirms that the best model should include `New Units Weighted by Allies` and most of the earlier-defined controls (`Attacker`, `GDP_PerCapita`, `Int_Users`, `Democracy`, and `Total MIDs`). Even though `Target` and `IGO Membership` do not appear in the top five models, I proceed with including these controls in my subsequent analysis to avoid model overfit.

Table 3.5: *Model Selection: Control Variables*

ID	*# of Predictors*	*AIC*	*Model*
1	4	773.01	`New Responsibilities Weighted by Allies + Attacker + Int_Users + Total MIDs`
2	5	773.23	`New Responsibilities Weighted by Allies + Attacker + Int_Users + Total MIDs + Democracy`
3	5	773.28	`New Responsibilities Weighted by Allies + Attacker + Int_Users + Total MIDs + GDP_PerCapita`
4	6	773.69	`New Responsibilities Weighted by Allies + Attacker + Int_Users + Total MIDs + Democracy + GDP_PerCapita`
5	3	773.99	`Attacker + Int_Users + Total MIDs`

Next, I apply the AIC criteria to the diffusion variables that have a statistically significant effect in the models with individual diffusion variables (`IGO Partners`, `UN Partners (1)`, `UN Partners (2)`, `Neighbors (1)`, `Trading Partners (1)`, `Adversaries`, and `Linguistic Partners`). Similarly, each model under consideration automatically includes country-clustering and six original controls (`Attacker`, `GDP_PerCapita`, `IGO Memerbship`, `Int_Users`, `Target`, `Total MIDs`). I include the effects of both newly-created units and newly-responsible agencies by the country's neighbors (i.e., `Allies`, `UN Partners (1/2)`, `Neighbors (1)`, `IGO Partners`, `Adversaries`, `Linguistic Partners`,

and Trading Partners (1)). Table 3.6 displays the results, which recommend including the newly-created units and newly-responsible agencies by Allies, UN Partners (1) and (2), Adversaries, and Linguistic Partners. Since New Responsibilities/Units Weighted by UN Partners (1) and New Responsibilities/Units Weighted by UN Partners (2) highly correlated (Figure 3.6), I include only New Responsibilities/Units Weighted by UN Partners (1) in my models that consider cumulative effects of diffusion networks. Section 3.8 presents the obtained results.

Table 3.6: *Model Selection: All Diffusion Variables*

ID	*# of Predictors*	*AIC*	*Model*
1	13.00	762.62	clustering + original 6 + New Responsibilities/Units Weighted by UN Partners (2) + New Responsibilities/Units Weighted by Linguistic Partners + New Responsibilities/Units Weighted by Adversaries
2	11.00	762.75	clustering + original 6 + New Responsibilities/Units Weighted by UN Partners (2) + New Responsibilities/Units Weighted by Adversaries
3	15.00	762.84	clustering + original 6 + New Responsibilities/Units Weighted by UN Partners (2) + New Responsibilities/Units Weighted by Linguistic Partners + New Responsibilities/Units Weighted by Adversaries+New Responsibilities/Units Weighted by UN Partners (1)
4	13.00	763.00	clustering + original 6 + New Responsibilities/Units Weighted by UN Partners (2) + New Responsibilities/Units Weighted by Adversaries + New Responsibilities/Units Weighted by UN Partners (1)
5	13.00	764.95	clustering + original 6+ New Responsibilities/Units Weighted by UN Partners (2) + New Responsibilities/Units Weighted by Linguistic Partners + New Responsibilities/Units Weighted by Adversaries + New Responsibilities/Units Weighted by UN Partners (1)+ New Responsibilities/Units Weighted by Allies

Another way of checking the model fit is using the concordance statistic which "computes the agreement between an observed response and a predictor."[23] Popularized by Harrell Jr, Lee and Mark (1996), this technique became one of the most used measures of goodness-of-fit in survival models. Out of all the models, Model #2, which contains country-clustering, all original six controls (Attacker, GDP_PerCapita, IGO Memerbship, Int_Users, Target, Total MIDs), and newly-assigned and created units by all diffusion variables, does a better job of predicting which country is at risk of having an event (Assign or Create) at a

[23] *Source:* https://www.rdocumentation.org/packages/survival/versions/3.1-12/topics/concordance

particular time than other considered models. Results for Model #3 are very close to those for Model #2. Thus, I proceed with running my cumulative effects models with results recommended by AIC.

Table 3.7: *Model Selection: Concordance Statistics*

Model #	*Predictors*	*Concordance*	*St.error*
	`No Responsible Agency → Assign`		
1	clustering + 6 original controls	0.7786	0.0301
2	clustering + 6 original controls + newly-assigned and created units by all diffusion variables	0.8320	0.0263
3	clustering + 6 original controls + newly-assigned and created units by all diffusion variables recommended by AIC	0.8308	0.0257
4	clustering + 6 original controls + newly-assigned and created units by all diffusion variables recommended by AIC but `Ally`	0.8217	0.0240
5	clustering + 6 original controls + created units by all diffusion variables	0.8186	0.0257
	`No Responsible Agency → Create`		
1	clustering + 6 original controls	0.7887	0.0303
2	clustering + 6 original controls + newly-assigned and created units by all diffusion variables	0.8251	0.0269
3	clustering + 6 original controls + newly-assigned and created units by all diffusion variables recommended by AIC	0.8109	.02810
4	clustering + 6 original controls + newly-assigned and created units by all diffusion variables recommended by AIC but `Ally`	0.8104	0.0282
5	clustering + 6 original controls + created units by all diffusion variables	0.7996	0.0295

Robustness Checks

I conduct the following robustness checks.

Military Alliances. In addition to using ATOP data, I also use the Correlates of War (COW) Project's data on formal alliances (version 4.1) (Gibler 2008). As Table 3.11 demonstrates my results are not robust. This is not surprising, given that the COW Alliances data set contains a less comprehensive account of the formed alliances during the 1999-2018 period under the study. Specifically, as Section 3.8 explains, the data set ends in 2012, contains less detailed event descriptions, and fewer instances of the formed alliances even when COW Alliances' and ATOP's time periods overlap (1999-2012).

Distance. In order to identify a country's geographic neighbors, I use the following measures:

Table 3.8: *Effects of New Responsibility and New Unit (Binary, Year)*

(a) Part (a)

	(1)	(2)	(3)	(4)	(5)	(6)
	No Responsible Agency → Assign					
New Responsibilities Weighted by IGO Partners	0.135					
	(0.190)					
New Responsibilities Weighted by UN Partners (1)		0.145				
		(0.510)				
New Responsibilities Weighted by UN Partners (2)			−0.065			
			(0.470)			
New Responsibilities Weighted by UN Partners (3)				−0.054		
				(0.487)		
New Responsibilities Weighted by UN Partners (Disarmament)					−0.055	
					(0.512)	
New Responsibilities Weighted by UN Partners (Palestine)						−0.054
						(0.500)
New Units Weighted by IGO Partners	0.147					
	(0.205)					
New Units Weighted by UN Partners (1)		−1.215***				
		(0.483)				
New Units Weighted by UN Partners (2)			−1.101***			
			(0.454)			
New Units Weighted by UN Partners (3)				−1.058***		
				(0.452)		
New Units Weighted by UN Partners (Disarmament)					−0.655*	
					(0.454)	
New Units Weighted by UN Partners (Palestine)						−0.815**
						(0.493)
Attacker	1.121***	0.967***	1.050***	1.037***	1.014***	1.072***
	(0.376)	(0.365)	(0.364)	(0.362)	(0.365)	(0.380)
Int_Users	1.268**	1.158**	1.139**	1.141**	1.185**	1.167**
	(0.582)	(0.546)	(0.546)	(0.541)	(0.558)	(0.575)
Total MIDs	0.177	0.265	0.249	0.260	0.229	0.200
	(0.219)	(0.222)	(0.218)	(0.218)	(0.222)	(0.220)

Note: The dependent variable is Assign—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.

Table 3.8: *Effects of New Responsibility and New Unit (Binary, Year)*

(b) Part (b)

	(1)	(2)	(3)	(4)	(5)	(6)
	No Responsible Agency → Create					
`New Responsibilities Weighted by IGO Partners`	0.432**					
	(0.187)					
`New Responsibilities Weighted by UN Partners (1)`		−0.169				
		(0.547)				
`New Responsibilities Weighted by UN Partners (2)`			−0.433			
			(0.458)			
`New Responsibilities Weighted by UN Partners (3)`				−0.293		
				(0.477)		
`New Responsibilities Weighted by UN Partners (Disarmament)`					−0.139	
					(0.463)	
`New Responsibilities Weighted by UN Partners (Palestine)`						−0.728
						(0.570)
`New Units Weighted by IGO Partners`	−0.044					
	(0.284)					
`New Units Weighted by UN Partners (1)`		−0.578				
		(0.624)				
`New Units Weighted by UN Partners (2)`			−0.344			
			(0.524)			
`New Units Weighted by UN Partners (3)`				−0.430		
				(0.548)		
`New Units Weighted by UN Partners (Disarmament)`					−0.358	
					(0.548)	
`New Units Weighted by UN Partners (Palestine)`						−0.466
						(0.649)
`Attacker`	0.127	0.101	0.150	0.147	0.129	0.149
	(0.573)	(0.550)	(0.552)	(0.549)	(0.551)	(0.526)
`Int_Users`	1.321***	1.116**	1.084**	1.092**	1.131**	1.092**
	(0.603)	(0.583)	(0.585)	(0.583)	(0.590)	(0.595)
`Total MIDs`	0.532***	0.558***	0.540***	0.542***	0.549***	0.463***
	(0.202)	(0.206)	(0.202)	(0.203)	(0.205)	(0.207)
Observations	2,727	2,727	2,727	2,727	2,727	2,727
Additional Controls	✓	✓	✓	✓	✓	✓
Log Likelihood	−288.079	−284.061	−281.948	−282.934	−286.900	−287.426

Note: The dependent variable is `Create`—the country's decision to initiate the development of its military cyberapparatuses by creating a new cybersecurity agency.
*p<0.1; **p<0.05; ***p<0.01

Table 3.9: *Effects of New Responsibility and New Unit (Binary, Year) (Continued)*

(a) Part (a)

	(1)	(2)	(3)	(4)	(5)	(6)
	No Responsible Agency → Assign					
`New Responsibilities Weighted by UN Partners (Nuclear)`	0.139					
	(0.525)					
`New Responsibilities Weighted by UN Partners (Colonialism)`		−0.154				
		(0.481)				
`New Responsibilities Weighted by UN Partners (EconDev)`			−0.339			
			(0.385)			
`New Responsibilities Weighted by UN Partners (HumanRights)`				−0.097		
				(0.467)		
`New Responsibilities Weighted by Neighbors (1)`					0.247	
					(0.289)	
`New Responsibilities Weighted by Neighbors (2)`						0.101
						(0.147)
`New Units Weighted by UN Partners (Nuclear)`	−0.886**					
	(0.474)					
`New Units Weighted by UN Partners (Colonialism)`		−0.708***				
		(0.353)				
`New Units Weighted by UN Partners (EconDev)`			−0.470			
			(0.390)			
`New Units Weighted by UN Partners (HumanRights)`				−1.212***		
				(0.484)		
`New Units Weighted by Neighbors (1)`					0.348*	
					(0.190)	
`New Units Weighted by Neighbors (2)`						0.144**
						(0.074)
`Attacker`	1.043***	1.036***	1.094***	1.053***	1.096***	1.112***
	(0.362)	(0.371)	(0.371)	(0.360)	(0.363)	(0.365)
`Int_Users`	1.219**	1.136**	1.040*	1.167**	1.154**	1.165**
	(0.556)	(0.555)	(0.582)	(0.534)	(0.564)	(0.579)
`Total MIDs`	0.254	0.221	0.141	0.291	0.196	0.176
	(0.222)	(0.221)	(0.218)	(0.219)	(0.222)	(0.222)

Note: The dependent variable is `Assign`—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.
*p<0.1; **p<0.05; ***p<0.01

Table 3.9: *Effects of New Responsibility and New Unit (Binary, Year) (Continued)*

(b) Part (b)

	(1)	(2)	(3)	(4)	(5)	(6)
No Responsible Agency → Create						
New Responsibilities Weighted by UN Partners (Nuclear)	−0.118					
	(0.480)					
New Responsibilities Weighted by UN Partners (Colonialism)		−0.753				
		(0.536)				
New Responsibilities Weighted by UN Partners (EconDev)			−0.389			
			(0.353)			
New Responsibilities Weighted by UN Partners (HumanRights)				−0.497		
				(0.451)		
New Responsibilities Weighted by Neighbors (1)					0.727***	
					(0.245)	
New Responsibilities Weighted by Neighbors (2)						0.272***
						(0.107)
New Units Weighted by UN Partners (Nuclear)	−0.543					
	(0.552)					
New Units Weighted by UN Partners (Colonialism)		−0.451				
		(0.449)				
New Units Weighted by UN Partners (EconDev)			0.024			
			(0.438)			
New Units Weighted by UN Partners (HumanRights)				−0.288		
				(0.544)		
New Units Weighted by Neighbors (1)					0.157	
					(0.291)	
New Units Weighted by Neighbors (2)						0.090
						(0.120)
Attacker	0.118	0.104	0.184	0.141	0.166	0.205
	(0.555)	(0.549)	(0.543)	(0.557)	(0.569)	(0.538)
Int_Users	1.165**	1.071**	1.060**	1.120**	1.025**	1.093**
	(0.583)	(0.572)	(0.612)	(0.578)	(0.566)	(0.593)
Democracy	−0.006	−0.268	0.248	−0.098	0.072	0.140
	(0.449)	(0.477)	(0.427)	(0.469)	(0.436)	(0.430)
Total MIDs	0.580***	0.556***	0.499***	0.574***	0.613***	0.559***
	(0.208)	(0.209)	(0.202)	(0.205)	(0.209)	(0.206)
Observations	2,727	2,727	2,727	2,727	2,727	2,727
Additional Controls	✓	✓	✓	✓	✓	✓
Log Likelihood	−284.708	−281.831	−289.019	−280.212	−285.379	−287.554

Note: The dependent variable is Create—the country's decision to initiate the development of its military cyberapparatuses by creating a new cybersecurity agency.
*p<0.1; **p<0.05; ***p<0.01

Table 3.10: *Effects of New Responsibility and New Unit (Binary, Year) (Continued)*

(a) Part (a)

	(1)	(2)	(3)	(4)	(5)	(6)
	No Responsible Agency → Assign					
New Responsibilities Weighted by Neighbors (3)	1.755					
	(1.934)					
New Responsibilities Weighted by Neighbors (4)		−0.082				
		(0.146)				
New Responsibilities Weighted by Neighbors (5)			−0.110			
			(0.228)			
New Responsibilities Weighted by Trading Partners (1)				−0.275**		
				(0.240)		
New Responsibilities Weighted by Trading Partners (2)					0.148	
					(0.162)	
New Responsibilities Weighted by Trading Partners (3)						−0.113
						(0.194)
New Units Weighted by Neighbors (3)	4.524					
	(3.307)					
New Units Weighted by Neighbors (4)		0.134				
		(0.101)				
New Units Weighted by Neighbors (5)			−0.305*			
			(0.359)			
New Units Weighted by Trading Partners (1)				−0.129		
				(0.260)		
New Units Weighted by Trading Partners (2)					−0.660***	
					(0.343)	
New Units Weighted by Trading Partners (3)						−0.022
						(0.131)
Target	−0.366	−0.386	−0.426	−0.458	−0.381	−0.428
	(0.530)	(0.565)	(0.622)	(0.612)	(0.593)	(0.603)
Attacker	1.078***	1.135***	1.131***	1.117***	1.130***	1.127***
	(0.363)	(0.372)	(0.387)	(0.384)	(0.377)	(0.383)
Int_Users	1.159**	1.237**	1.257**	1.252**	1.370**	1.201**
	(0.550)	(0.589)	(0.593)	(0.590)	(0.591)	(0.596)
Total MIDs	0.237	0.174	0.197	0.195	0.183	0.163
	(0.223)	(0.221)	(0.220)	(0.222)	(0.222)	(0.220)

Note: The dependent variable is Assign—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.
*p<0.1; **p<0.05; ***p<0.01

Table 3.10: *Effects of New Responsibility and New Unit (Binary, Year) (Continued)*

(b) Part (b)

	(1)	(2)	(3)	(4)	(5)	(6)
	No Responsible Agency → Create					
`New Responsibilities Weighted by Neighbors (3)`	4.822***					
	(1.805)					
`New Responsibilities Weighted by Neighbors (4)`		0.165***				
		(0.080)				
`New Responsibilities Weighted by Neighbors (5)`			0.042			
			(0.143)			
`New Responsibilities Weighted by Trading Partners (1)`				0.368**		
				(0.125)		
`New Responsibilities Weighted by Trading Partners (2)`					0.184**	
					(0.173)	
`New Responsibilities Weighted by Trading Partners (3)`						0.250**
						(0.154)
`New Units Weighted by Neighbors (3)`	−6.037					
	(3.533)					
`New Units Weighted by Neighbors (4)`		0.152**				
		(0.110)				
`New Units Weighted by Neighbors (5)`			−0.088			
			(0.177)			
`New Units Weighted by Trading Partners (1)`				0.083		
				(0.276)		
`New Units Weighted by Trading Partners (2)`					−0.345	
					(0.354)	
`New Units Weighted by Trading Partners (3)`						−0.298
						(0.221)
`Attacker`	0.214	0.215	0.175	0.266	0.180	0.178
	(0.566)	(0.519)	(0.536)	(0.541)	(0.536)	(0.537)
`Int_Users`	1.024**	1.002**	1.132**	1.021**	1.128**	1.131**
	(0.574)	(0.601)	(0.605)	(0.603)	(0.609)	(0.609)
`Democracy`	0.135	0.296	0.202	0.245	0.233	0.288
	(0.429)	(0.427)	(0.426)	(0.427)	(0.422)	(0.427)
`Total MIDs`	0.511***	0.515**	0.526***	0.530***	0.524***	0.524***
	(0.211)	(0.205)	(0.204)	(0.202)	(0.204)	(0.204)
Observations	2,727	2,727	2,727	2,727	2,727	2,727
Additional Controls	✓	✓	✓	✓	✓	✓
Max. Possible R^2	0.217	0.217	0.217	0.217	0.217	0.217

Note: The dependent variable is `Create`—the country's decision to initiate the development of its military cyberapparatuses by creating a new cybersecurity agency.
*p<0.1; **p<0.05; ***p<0.01

Table 3.11: *Effects of New Responsibility and New Unit (Binary, Year) (Continued)*

(a) Part (a)

	(1)	(2)	(3)	(4)
No Responsible Agency → Assign				
New Responsibilities Weighted by Adversaries	0.112			
	(0.096)			
New Responsibilities Weighted by Linguistic Partners		−1.124		
		(0.846)		
New Responsibilities Weighted by Allies			−0.052	
			(0.187)	
New Responsibilities Weighted by Allies (COW)				0.027
				(0.120)
New Units Weighted by Adversaries	0.121			
	(0.107)			
New Units Weighted by Linguistic Partners		−1.823**		
		(0.856)		
New Units Weighted by Allies			0.474***	
			(0.141)	
New Units Weighted by Allies (COW)				0.199**
				(0.096)
Target	−0.503	−0.483	−0.449	−0.593
	(0.620)	(0.582)	(0.637)	(0.644)
Attacker	1.206***	1.162***	1.074***	0.149***
	(0.392)	(0.373)	(0.390)	(0.380)
GDP_PerCapita	0.201	0.364	0.259	0.226
	(0.380)	(0.383)	(0.380)	(0.374)
Int_Users	1.171**	0.966*	1.147*	1.078*
	(0.592)	(0.581)	(0.601)	(0.584)
Democracy	0.758	0.704	0.666	0.629
	(0.457)	(0.472)	(0.466)	(0.460)
IGO Membership	−0.039	−0.167	0.047	0.011
	(0.201)	(0.194)	(0.198)	(0.198)
Total MIDs	0.100	0.192	0.142	0.122
	(0.232)	(0.228)	(0.223)	(0.226)

Note: The dependent variable is `Assign`—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.
*p<0.1; **p<0.05; ***p<0.01

- the inverse distance between the two capitals (`Neighbors (1)`),
- the squared inverse distance between the two capitals (`Neighbors (2)`),
- the logarithmized inverse distance between the two capitals (`Neighbors (3)`),
- a dummy variable that identifies whether two countries share a land border or are separated by at most 100 miles of water (`Neighbors (4)`) (Stinnett et al. 2002), and
- a dummy variable that identifies whether two countries share a land border or are

Table 3.11: *Effects of New Responsibility and New Unit (Binary, Year) (Continued)*

(b) Part (b)

	(1)	(2)	(3)	(4)
No Responsible Agency → Create				
`New Responsibilities Weighted by Adversaries`	0.143**			
	(0.067)			
`New Responsibilities Weighted by Linguistic Partners`		0.017		
		(0.071)		
`New Responsibilities Weighted by Allies`			0.223***	
			(0.103)	
`New Responsibilities Weighted by Allies (COW)`				0.203
				(0.170)
`New Units Weighted by Adversaries`	0.117			
	(0.104)			
`New Units Weighted by Linguistic Partners`		−1.133		
		(0.686)		
`New Units Weighted by Allies`			0.138	
			(0.290)	
`New Units Weighted by Allies`				−0.054
				(0.140)
`Target`	0.060	−0.021	0.036	0.080
	(0.173)	(0.177)	(0.170)	(0.173)
`Attacker`	0.218	0.213	0.163	0.176
	(0.534)	(0.543)	(0.529)	(0.530)
`GDP_PerCapita`	0.317	0.284	0.265	0.197
	(0.409)	(0.395)	(0.398)	(0.406)
`Int_Users`	1.039**	0.997**	1.042**	1.140**
	(0.613)	(0.591)	(0.603)	(0.610)
`Democracy`	0.319	0.329	0.174	0.203
	(0.433)	(0.428)	(0.427)	(0.422)
`IGO Membership`	0.033	−0.117	−0.026	−0.093
	(0.207)	(0.207)	(0.197)	(0.212)
`Total MIDs`	0.428*	0.569***	0.530***	0.537***
	(0.218)	(0.210)	(0.206)	(0.204)
Observations	2,727	2,727	2,727	2,727
R^2	0.032	0.037	0.034	0.032

Note: The dependent variable is `Create`—the country's decision to initiate the development of its military cyberapparatuses by creating a new cybersecurity agency.
*p<0.1; **p<0.05; ***p<0.01

Table 3.12: *Effect of New Responsibility and New Unit (Binary, Year) (Continued)*

(a) Part (a)

	(1)	(2)	(3)
No Responsible Agency → Assign			
New Responsibilities Weighted by Regime Partners (1)	−0.611		
	(0.371)		
New Responsibilities Weighted by Regime Partners (2)		−0.391	
		(0.338)	
New Responsibilities Weighted by Regime Partners (3)			−0.246
			(0.346)
New Units Weighted by Regime Partners (1)	0.073		
	(0.573)		
New Units Weighted by Regime Partners (2)		−0.163	
		(0.480)	
New Units Weighted by Regime Partners (3)			0.144
			(0.589)
Target	−0.416	−0.424	−0.414
	(0.585)	(0.605)	(0.595)
Attacker	1.221***	1.132***	1.134***
	(0.400)	(0.384)	(0.382)
GDP_PerCapita	0.164	0.162	0.164
	(0.378)	(0.380)	(0.379)
Int_Users	1.245**	1.256**	1.255**
	(0.589)	(0.595)	(0.594)
Democracy	1.098	1.089	0.793
	(0.732)	(0.698)	(0.858)
IGO Membership	−0.073	−0.073	−0.065
	(0.196)	(0.198)	(0.198)
Total MIDs	0.181	0.168	0.172
	(0.221)	(0.220)	(0.221)

Note: The dependent variable is Assign—the country's decision to initiate the development of its military cyberapparatuses by assigning new cybersecurity responsibility to an existing agency.
*p<0.1; **p<0.05; ***p<0.01

separated by at most 400 miles of water (Neighbors (5)) (Stinnett et al. 2002).[24]

As Tables 3.9 and 3.10 demonstrate my results are not robust.

Regime Type. Using Gurr, Marshall and Jaggers (2010)'s Polity IV score, I implement three different cut-off points to identify nations that share the same regime type:

1. Regime Partners (1): a dummy variable that identifies whether two countries share the same regime, using Gurr, Marshall and Jaggers (2010)'s Polity IV score; nations

[24] I have also considered using 200, 300, and 500 miles as my cut-off points but because these variables were perfectly separated with my dependent variables in some of my models, I decided to include these variables into my robustness checks.

Table 3.12: *Effect of New Responsibility and New Unit (Binary, Year) (Continued)*

(b) Part (b)

	(1)	(2)	(3)
No Responsible Agency → Create			
New Responsibilities Weighted by Regime Partners (1)	−0.119		
	(0.267)		
New Responsibilities Weighted by Regime Partners (2)		0.097	
		(0.256)	
New Responsibilities Weighted by Regime Partners (3)			−0.031
			(0.248)
New Units Weighted by Regime Partners (1)	−0.385		
	(0.528)		
New Units Weighted by Regime Partners (2)		−0.098	
		(0.511)	
New Units Weighted by Regime Partners (3)			−0.076
			(0.681)
Target	0.047	0.045	0.052
	(0.169)	(0.169)	(0.169)
Attacker	0.265	0.187	0.195
	(0.543)	(0.527)	(0.530)
GDP_PerCapita	0.223	0.233	0.229
	(0.404)	(0.404)	(0.405)
Int_Users	1.134**	1.121**	1.126**
	(0.606)	(0.608)	(0.609)
Democracy	0.597	0.203	0.332
	(0.654)	(0.656)	(0.939)
IGO Membership	−0.049	−0.031	−0.032
	(0.202)	(0.202)	(0.202)
Total MIDs	0.535***	0.521***	0.517***
	(0.204)	(0.203)	(0.203)
Observations	2,727	2,727	2,727

Note: The dependent variable is Create—the country's decision to initiate the development of its military cyberapparatuses by creating a new cybersecurity agency.
*p<0.1; **p<0.05; ***p<0.01

that score a "4" or above receive a "1" (i.e., democracy) and those nations that score a "3" or below receive a "0" (i.e., autocracy);

2. Regime Partners (2): a dummy variable that identifies whether two countries share the same regime, using Gurr, Marshall and Jaggers (2010)'s Polity IV score; nations that score a "5" or above receive a "1" (i.e., democracy) and those nations that score a "4" or below receive a "0" (i.e., autocracy); and

3. Regime Partners (3): a dummy variable that identifies whether two countries share the same regime, using Gurr, Marshall and Jaggers (2010)'s Polity IV score; nations

that score a "6" or above receive a "1" (i.e., democracy) and those nations that score a "5" or below receive a "0" (i.e., autocracy).

My results demonstrate that none of the specifications for the regime type is correlated with the country's choice to develop its military cybersecurity apparatus (Table 3.12).

Trade. I use the following three measures to identify a country's trading partners:

1. `Trading Partners (1)`: the amount of bilateral trade between two countries, taken from the World Bank;
2. `Trading Partners (2)`: the number of signed bilateral investment treaties between two nations (Graham and Tucker 2019); and
3. `Trading Partners (3)`: the number of signed preferential trade agreements between two nations (Graham and Tucker 2019).

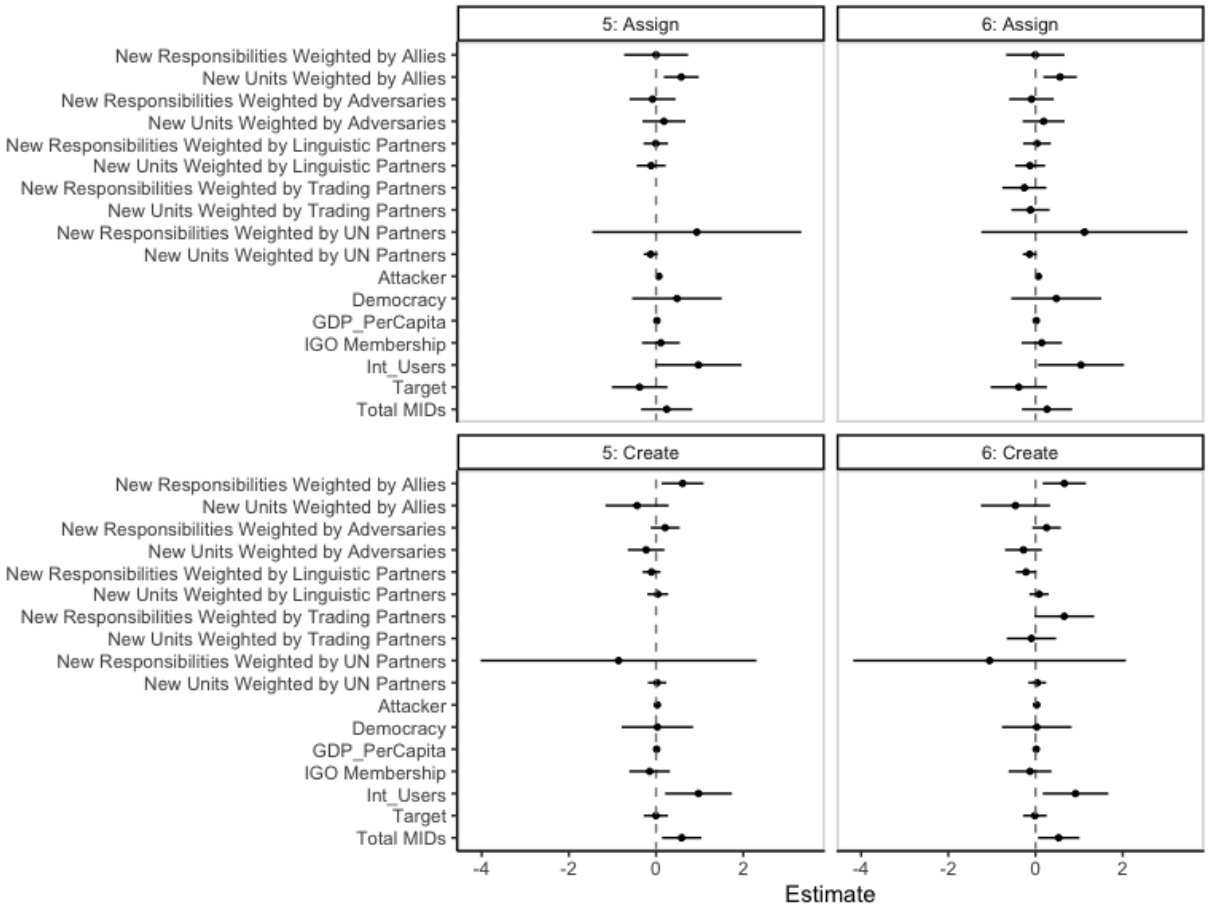
As Table 3.10, there is a positive correlation between the assignment of new responsibilities to existing military agencies by the country's trading partners and the country's decision to create a new military cybersecurity unit.

UNGA Resolutions. In addition to classifying UNGA resolutions into those on the subject of conflict (`UN Partners (1)`) and non-conflict (`UN Partners (2)`), I also apply my analysis to the UNGA resolutions on the six topics that contribute to these two categories as well as those resolutions that belong to neither of these two categories (`UN Partners (3)`). In particular, the UNGA resolutions on arms control and disarmament (`Disarmament`), nuclear weapons and nuclear material (`Nuclear`), and the Palestinian conflict (`Palestine`) are grouped into the `UN Partners (1)` category. The UNGA resolutions on colonialism (`Colonialism`), economic development (`EconDev`), and human rights (`HumanRights`) contribute to the `UN Partners (2)` category.

Most of these variables have either negative correlation or no correlation with `Assign` and `Create`. These results are not surprising, given that the UNGA resolutions on these various topics do not touch on the subject of cybersecurity and the proliferation of military cybercapacity. Thus, if the countries are busy with developing measures to deal with these others issues, they are less likely to devote their attention to the subject of military cybersecurity. The negative effect of the human rights resolutions is also not surprising. The subject of human rights violation has been often discussed along with a state's attempts to boost its cybercapacity. In particular, some political acitivists and civil society groups view an increase in state cybercapacity as new means to conduct surveillance and censorship against citizens. For instance, Brazilian social activists argue that the desire to monitor Brazilian citizens is one of the reasons why the government created its military department, called the Centre for Cyber-defense (CDCiber) (Muggan, Diniz and Glenny 2014). A threat of populous protest that often originated from abroad caused the country to increase its offensive cyber capability and CDCiber and Brazil's central intelligence agency (ABIN) to create social media monitoring platforms in the aftermath of the 2013 protest (Muggan, Diniz and Glenny 2014).

Cumulative Effect of Militarization. Suppose a country started developing its cyberapparatus in year t. In addition to considering whether a country's allies and adversaries started developing their military cyberapparatuses in year $t-1$, I use a binary variable that records whether the country's allies and adversaries started developing their military cyberapparatuses in any year prior to year $t-1$. Figure 3.7a demonstrates that signal complementarity between allies is robust, but the effect of the rivals' build-up of their military cyberapparatuses disappears. This result might suggest that countries perceive only recent development of military cyberapparatuses by their adversaries as threatening and have the urge to respond. With time, this urge fades away.

Figure 3.7: *Robustness Checks: Alternative Dependent Variable*



(a) Effect of Alternative "Neighbors" Measures on `Create`

Note: Dependent variable: `Create`—the country's decision to initiate the development of its military cyberapparatuse by creating a brand new unit. Results are from a Competing Risks Cox Proportional-Hazards Model. The reported values are the hazard ratios and their confidence intervals. There are 2,727 observations and 69 events. Each plot displays a weighted average effect of both assigning new cybersecurity responsibilities to existing military agencies and creating new military cybersecurity agencies. To create this effect, I record whether the country's allies and adversaries started developing its military cyberapparatus in any year prior to year $t-1$ (instead of in previous year only). See the Online Appendix for more details and a more details presentation of results. All results are based on two-tailed tests.

Chapter 4

Deterrence in the Cyber Realm: Public versus private cybercapacity

A number of detrimental cyberoperations that we have witnessed over the last two decades motivated nations to develop their cybercapacities. For instance, the Stuxnet worm, discovered in 2010, was used against the Iranian nuclear enrichment facility to slow down its nuclear weapons program. In 2014, a group with ties to the North Korean government hacked Sony Pictures Home Entertainment and used a malicious software to erase Sony's computer infrastructure. In 2015 and 2016, the Russian government cyberattacked Ukrainian electric power grids, as a result of which Ukrainian citizens remained without electricity for several hours. In 2016, the Russian government meddled in the U.S. presidential elections by mainly posting fabricated articles and disinformation on social media websites and hacking emails of the Clinton campaign officials and strategically releasing the obtained information. All these "strategic" attacks, according to the U.S. Department of Defense, detrimentally affected the target country's "economy and prosperity" (Fernandino 2018).

To deter such attacks, nations started implementing publicly observable proactive efforts aimed at signaling their offensive and defensive cybercapabilities. They started adopting new

legislation, doctrines, and strategies; creating new agencies responsible for cybersecurity; adding new roles related to cybersecurity to existing agencies (such as cyber-education programs within Ministries of Education); and adding cybersecurity components to military exercises. I define all these efforts as *public cyberinstitutions* (PCIs). PCIs are meant to deter adversaries from executing cyberattacks that cause significant damage to a country's prosperity and economy, but how effective are they at achieving that objective? Specifically, this research investigates a question that has been completely overlooked in the international relations literature until now: *Can PCIs deter adversaries from executing strategic cyberattacks?*

To answer this question, I develop an incomplete-information model in which a challenger considers attacking a defender. The challenger is not certain about the defender's cybercapacity and can only infer it from the defender's observable PCIs. Thus, the adversary's decision to attack is endogenous to the defender's type, and the defender has an incentive to over-invest in public cybercapacity in order to signal that it is stronger that it actually is.

This model leads to several insights. First, there are a large number of equilibria for which PCIs have no influence on the challenger. Second, I show that the target countries' strategic use of PCIs to deter their adversaries works only when two conditions are met: (1) the adversary believes that a country possesses significant cybercapabilities and that it would therefore be too costly to attack that country; and (2) the adversary is susceptible to the cost exacted by PCIs. This finding shows that PCIs influence an adversary's decision to attack only in limited cases. Despite that, weaker states over-invest in PCIs to signal higher cybercapacity than they possess, and strong cyber states over-invest so that their adversaries do not believe that they are weak states pretending to be strong.

Scarce data on cyberincidents and PCIs,[1] compounded by the secrecy surrounding

[1] Currently, there are only two published datasets on cyberincidents: Valeriano and Maness 2018's Dyadic

national security issues, make it difficult to undertake a rigorous empirical test of my model's findings. Instead, I use a series of interviews with cybersecurity experts, intelligence reports, and examples of attempted election interference to establish the empirical plausibility of my theory. The evidence I obtained through these means supports the theory's central conjecture that deterrence by PCIs works but only in limited cases.

This paper makes a number of theoretical contributions to the existing international-relations literature. First, it helps us better understand the nature of deterrence in the information age. My unique strategic logic of PCIs as a proxy for a country's cybercapacity represents a departure from existing literature. While most scholarly works on cyber-to-cyber deterrence focus on deterrence by punishment using cyberoperations (Baliga et al. 2018; Gartzke and Lindsay 2015; Lindsay 2013; Rid 2013; Valeriano and Maness 2014, 2018), this project presents a new theory that explains how PCIs can deter by both prevention and threat of punishment, by signaling an increase in both defensive and offensive cybercapabilities. This project also contributes to the literature on cross-domain deterrence (Gartzke and Lindsay 2019) by explaining situations in which countries use PCIs to deter their adversaries because non-cyber foreign policy options (i.e., economic sanctions, or diplomatic or military responses) are ineffective and/or costly.

Second, much of the literature on cybercoercion either focuses on intelligence and policy dilemmas confronting major powers or seeks to adapt existing theories of coercive diplomacy and deterrence to explain the strategic behavior of major powers in cyberspace (Borghard and Lonergan 2017; Brantly 2016; Gartzke 2013; Libicki 2009; Lindsay and Gartzke 2015; Nye Jr 2017; Valeriano and Maness 2018). I, instead, seek to explain the strategic behavior of weaker cyber states or middle powers when these states suspect a cyberattack. In these situations, middle powers often must rely on their own cybercapabilities because their allies are unlikely to help. Cyberdefenses are unique to each country and not easily transferable;

Cyber Incident Dataset and Kostyuk and Zhukov 2019's data on conflict in Ukraine. Datasets on cyberinstitutions are in the process of being developed (Kostyuk 2020*a*).

close allies are often reluctant to disclose information about their offensive cybercapabilities and/or commit cyberattacks on an ally's behalf (as compared with their willingness to offer military assistance during territorial invasions).

Third, this paper uses new sources to provide the first-ever theoretically informed explanation of how nations can use their cybercapabilities to deter state-sponsored interference campaigns. Most works on this relatively new phenomenon are limited to descriptive policy reports or formal accusations that trace evidence to potential perpetrators (Brattberg and Maurer 2018*a*; Cederberg 2018; Galante and EE 2018; Mueller 2019; USDepartmentOfJustice 2018*c*,*a*).

The literature on the "bargaining model of war" focuses on how private information and incentives to misrepresent, and commitment problems affected by power shifts explain costly armed conflict (e.g., Fearon 1995, Reiter 2003, Powell 2006). Like this literature, my model demonstrates that states tend to use costly signals and over-invest in their capabilities to make their adversaries misinterpret the existing balance of power (Morrow 1989*a*); states also tend to keep certain capabilities secret to obtain military advantage (Reiter 2003).

What is new about my model then? First, a different theoretical foundation drives a nation's decision regarding how to signal its cybercapacity. Unlike in the case of military capacity, states cannot launch parades to signal their cybercapacity. Satellite images are also unlikely to be useful to adversaries seeking to estimate a state's cyberstrength. An executed cyberattack may provide the target with a good estimate of the attacker's capabilities, but such an attack also de-values capability because it provides adversaries with instructions on how to fix flaws in their own networks and systems. The time-limited life-span and the dynamic nature of cyberoperations further complicate their signaling potential. While the basic parameters for most traditional weapons remain relatively static, strategically relevant features of certain cyberweapons might look quite different tomorrow (Libicki 2009). As a result, signaling cybercapacity via PCIs is more effective than signaling via cyberoperations

because it (1) preserves the value of a state's cyberoperations, which diminishes after use, and (2) provides the adversary with an immediate, often rough proxy for the state's cybercapacity. This logic demonstrates that a state makes this signaling choice not only to make the adversary overestimate its capability but also to preserve the value of its secret cyber arsenal.

Second, existing models focus only on whether and how investment in military capacity can deter a future attack or affect the likelihood of winning a war.[2] My theoretical foundation instead explains that sources of state cybercapacity are more diverse, lie beyond military and government, and extend to a state's private sector and even public-opinion management. While investing in military cybercapacity is important for deterrence by the threat of punishment, to deter adversaries by prevention, states might, for example, invest significant resources into building public awareness about the danger of cyberoperations and information operations, making potential election-interference campaigns harder.

Regarding the model, the closest works are Jackson and Morelli (2009), Powell (1993),[3] Meirowitz and Sartori (2008),[4] Debs and Monteiro (2014),[5] and Morrow (1989*a*).[6] But none of these models focus on a state's cybercapacity; instead, they explain how the state uses its conventional military capability to lead wars and/deter its opponents. Baliga et al. (2018)

[2] Some of these works include Debs and Monteiro (2014); Fearon (2018); Kydd (2000); Meirowitz and Sartori (2008); Morrow (1989*b*); Slantchev (2005).

[3] Using dynamic games, Jackson and Morelli (2009) and Powell (1993) examine how states simultaneously or sequentially invest in their arms. The authors explain guns-versus-butter and peace-versus-war effects of this choice. Unlike both models, mine assumes that an adversary is already armed at the time that it is contemplating an attack. Moreover, instead of the guns-versus-butter choice, I focus on how the defender chooses to allocate its resources between PCIs and covert cyberactivity in order to deter an adversary.

[4] Meirowitz and Sartori (2008, 33) begin with complete information and use imperfect information about states' choices to acquire arms in order to demonstrate how self-interests and strategy can drive states' decisions to acquire arms "in such a way as to create uncertainty about their military capability." While my model distinguishes between the defender's public and covert cybercapabilities, it involves incomplete information about a defender's type, not its choices.

[5] Similarly to Meirowitz and Sartori (2008), Debs and Monteiro (2014) focus on arming decisions that are not observable and how these decisions can lead to preventive wars. My model does not focus on preventive wars. Instead, it explains how observable PCIs can deter an adversary contemplating a cyberattack from executing this attack.

[6] Similar to Morrow (1989*a*), my model explains how the uncertainty about capabilities, and the divergence between observable and real capabilities, lead to conflict. But unlike Morrow (1989*a*)'s sequential bargaining model, with alternating offers by both states, my model focuses on how a state's allocation of resources to its PCIs allows an adversary to estimate a state's cybercapacity and decide whether to attack.

is the only other model that focuses on cyberdeterrence. In particular, this model explores how the state's inability to correctly attribute the origin of cyberoperations and to detect the fact that it has been cyberattacked affects this state's chances of deterring potential attackers. Unlike that model, where there is uncertainty over the signal's sender while the signal's quality is clear, my model investigates situations where the signal's sender is known but the signal's quality is unclear. I chose to approach the inferential problem differently from Baliga et al. (2018) because I look at the effect of PCIs—and not cyberattacks—that signal both offensive and defensive cybercapacity.

Lastly, similarly to works on counter-terrorism policies (Bueno de Mesquita 2007; Dragu 2011; Dragu and Polborn 2014; Faria 2006), my model explains whether and why nations might over-invest in public capacity and how effective these policies are. In addition to over-investing due to security concerns, states also over-invest in public counter-terrorism measures because of electoral pressure (Bueno de Mesquita 2007; Dragu and Polborn 2014), legal limits on executive power (Dragu and Polborn 2014), and a anti-terrorist agency's level of privacy protections (Dragu 2011), among other reasons. This paper explains that nations might over-invest in public cybercapability to deter their adversaries, who are unable to directly evaluate nations' actual cybercapability. This signaling choice helps nations preserve their secret cyber arsenals whose value diminishes after use and, at the same time, reach a wider audience. Because a weak state can appear strong by inflating PCIs, an optimal resource allocation between public and covert cybercapacity may not be sufficient to deter weak nations from mimicking PCIs of strong nations. Despite this race to over-invest in public cybercapacity, my model shows that this deterrence strategy works only in limited cases—a finding that resonates with Faria (2006)'s conclusion regarding the effectiveness of deterrence as a counter-terrorism policy.

4.1 Public Cyberinstitutions

I define *public cyberinstitutions* (PCIs) as *publicly observable efforts aimed at signaling a country's level of offensive and defensive cybercapability.*[7] I distinguish two types of PCIs. A state can: (1) create a new agency program, initiative, doctrine, strategy, or policy to address some aspect of cybersecurity or (2) add new cyber roles to existing agencies or new cyber provisions to existing policies. For instance, Sweden created the first type of PCI by establishing an agency responsible for psychological defense to "improve the ability of Swedish society to withstand pressure from a potential opponent" (*Sweden's Defense Policy: 2016 to 2020* 2015, 5). An example of the second type of PCI is the hack-back strategy that Germany considered, in preparation for the 2017 German elections, that would allow the country to response to a potential cyberattack in a real time (Schwirtz 2017).

While PCIs often do not reveal all the details about a new initiative or a program, unlike covert cyberactivity they allow an adversary to estimate the scope of the change and the potential resulting increase in the target state's cybercapacity. For instance, by adding voting machines to a list of critical infrastructure objects after the 2016 U.S. elections (Johnson 2017), the U.S. government signaled that it prioritized spending its resources on building better security for these machines, making them more difficult to hack. This information is important for an adversary considering a cyberattack because non-state actors tend to be important sources of state cybercapacity (Maurer 2018). For instance, *Presidential Policy Directive/PPD-21* (2013) introduced a collaboration program between the U.S. government and the U.S. private sector focused on critical infrastructure protection. According to the U.S. government, it planned through this program to "increase the volume, timeliness, and quality of cyberthreat information shared with U.S. private sector entities" that chose to participate in the program. Using the intelligence provided, the U.S. private sector would

[7] It is important to know that these efforts do not need to be observable to the public but they should be observable to potential adversaries.

"protect and defend [itself] against cyberthreats" (*Presidential Policy Directive/PPD-21* 2013).

I argue that public cyberinstitutions can deter by prevention and/or by threat of punishment. PCIs can deter by prevention because adversaries may infer that their attacks are likely to fail against the defenses implied by a PCI. A firewall, updated computer software, or a new program aimed at educating the public about cyberthreat and information threats are all examples of PCIs that can deter by prevention if they are perceived by an adversary to make hacking more difficult. The 2013 Executive Order 13636, which outlined a set of measures meant to provide better security for U.S. critical infrastructure objects against cyberthreats (Obama 2013), falls into this category. Other sorts of PCIs can deter by the threat of punishment. For instance, when the first French cyber offensive doctrine was released (*Public Elements of the Doctrine on Military Cyber Offensive* 2019), the French Defense Ministry stated that the country was "not afraid" of using cyber "weapons" in response to cyberthreats (Laudrain 2019). Finally, some PCIs can deter by both prevention and threat of punishment. The *U.S. Cyber Strategy* (2015, 3) uses deterrence by prevention by specifying the Department of Defense's (DoD's) role in defending its information networks, and it uses the threat of punishment by establishing a Cyber Mission Force that will be used to defend the United States against cyberattacks of "significant consequence."

There are two reasons why I investigate situations in which both deterrence mechanisms are at play. First, as the *U.S. Cyber Strategy* (2015)'s example demonstrates, one institution can signal both cyber offensive and defensive capability, making it hard to separate deterrence by the threat of punishment from deterrence by prevention. Second, when faced with a strategic cyberthreat, states tend to respond with multiple cyberinstitutions and, as a result, implement both types of deterrence at the same time to maximize their chances of success.

With main concepts defined, I will next venture into the relatively uncharted territory of modeling strategic cyberattack deterrence using public cyberinstitutions.

4.2 The Theory of Cyber Deterrence

The theory presented here examines the specific context in which a strong challenger ("he") contemplates a strategic cyberattack against a defender ("she").[8] When the challenger considers a cyberattack, he calculates the *value* he can gain from this attack (e.g., undermining democratic processes, in the case of election interference) and the *cost* he can incur. There are two types of costs. First is the cost of the defender's potential retaliation (e.g., using economic sanctions or cyberoperations). Second is the tendency of the value of cyberoperations, unlike military operations, to diminish in value after their first use (Libicki 2007). A tank, for example, can be successfully deployed many times over many years. Cyberattacks, on the other hand, often lose their effectiveness after their first use, even if the attack fails due to the defender's defenses. In using cyberattacks, the challenger risks the possibility that the defender might be able to develop protection against similar attacks in the future.

I argue that, for a challenger to decide to use a cyberattack against a defender, he must believe that the attack's value will outweigh its cost. What can change the attack's value and cost? Specifically, what can raise the cost enough to deter the challenger?

I argue that the costs from non-cyber foreign policy tools (i.e., diplomatic or military responses, or economic sanctions) will not change the value and cost because they have already been considered by the challenger in the initial decision-making process. These costs are easy to estimate using the defender's past history and are highly predictable based on the challenger's "prior beliefs about the defender's willingness" to use one of these options (Fearon 2002, 6). Moreover, given that the defender's capability in non-cyber foreign policy domains

[8] I employ the language from the traditional deterrence literature and refer to an adversary as a *challenger* and a defending state as a *defender*. The model makes an assumption that the defender attempts to deter her strongest challenger, as those challengers can potentially cause the most significant damage. If she is able to deter her strongest challenger, then all her other challengers will be deterred by default. Because the model focuses only on the strong challenger, I have omitted "strong" and refer only to a "challenger" for the remainder of the paper.

is unlikely to change rapidly, the challenger's estimate of the costs imposed by diplomatic responses and economic sanctions is likely to be fairly accurate. The challenger is also aware that military responses are costly and that it is therefore quite unlikely that the defender will launch a military strike in response to information operations or cyberoperations.[9]

Given that challengers are unlikely to be deterred by a fear of a diplomatic or military response, or by economic sanctions, the defender is left with cyber foreign policy tools to deter the challenger from executing cyberattacks. I argue that cyber foreign policy tools may raise the cost of a cyberattack for the challenger. Even if the challenger has a rough estimate of the defender's cybercapacity, the dynamic and time-limited nature of cyber tools makes it difficult for the challenger to determine the defender's cybercapacity with precision or certainty. Specifically, while the basic parameters for most traditional weapons remain relatively static, strategically relevant features of certain cyber weapons can change significantly over a very short period of time. Even though conventional platforms become obsolete over time, the life spans of cyberoperations are much shorter because they depreciate after their first use and because the defender might recognize and fix the vulnerability before the challenger is able to exploit it (Axelrod and Iliev 2014; Huntley 2018).

For deterrence to be successful, the defender must demonstrate two things: (1) resolve and (2) capability (Schelling 2008). Given that the defender knows she is facing a challenger contemplating a cyberattack, I assume the defender's resolve is high to use her capability to respond to the challenger in this high-stakes scenario (Press 2005).[10] In this scenario, deterrence depends on perceived, rather than actual, cyberstrength on the part of the defender (Jervis 1976). To understand how the defender can achieve the appearance of cyberstrength, we must first understand how a defender develops cybercapacity.

[9] For instance, the Israeli Defense Force bombing a building where the Hamas group allegedly operated is the first example when a state used a physical attack in response to cyberoperations (Newman 2019).

[10] This assumption allows me to explain the effect of the distribution of capabilities on deterrence. I relax this assumption and discuss how resolve can affect my model equilibria in Section 4.3.

Cybercapacity. All nations have limited resources that they can allocate to cybercapacity. For simplicity, I assume that, to maximize this capability, a government can divide these resources between PCIs, which publicly signal the defender's cyber offensive and defensive capability,[11] and *covert cyberactivity* (CCA), which involves *secret development of cybercapabilities and ongoing cyberoperations*.[12] Various programs, unknown to the challenger,[13] within intelligence agencies provide examples of covert cyberactivity.

There is a big difference between public and covert cybercapability in terms of a state's ability to send a signal about its overall cybercapacity. On the one hand, signaling cybercapacity via covert cyberoperations provides the challenger with a more accurate estimate of the defender's capability. But the difficulty of attributing the origin of cyberoperations and the time it takes to do so diminish the signal's value, which is further reduced by the time-limited life-span and the dynamic nature of cyberoperations. Signaling cybercapacity via PCIs, on the other hand, provides the defender's allies, adversaries, domestic and international audiences with an immediate, often rough proxy for the state's cybercapacity and preserves the value of a state's covert cyberoperations. For these reasons, a state can get more bang for its buck by signaling via PCIs.

It is important to note that this model does not exclude the possibility that countries can use cyberoperations to signal their capacity to an adversary. In my model, I incorporate this signaling into the challenger's prior beliefs regarding the defender's overall cybercapability. If the defender is strong and is able to leave non-malicious code in the challenger's systems, the challenger will be more likely to believe that the defender is strong. Weaker nations, on the other hand may not have this capability. Thus, their only way to signal their cybercapability may be to use PCIs. At the start of the game, I assume that such transparent covert

[11] Section 4.1 provides a detailed explanation of PCIs.

[12] Using primary evidence from my interviews, I assume that both PCIs and CCA are jointly optimal for the development of a defender's cybercapacity, and I opt to focus on the effect of public cyberinstitutions on deterrence. Section 4.6 gives an overview of my interviews.

[13] How much of the defender's CCA are unknown to the challenger depends on the challenger's (cyber and non-cyber) intelligence capability.

operations have already taken place. It is also worth noting that, just because a defender has the ability to access a challenger's systems and can leave non-malicious code to send a message, there is no guarantee that they will do so; it is possible that they would prefer to exploit this vulnerability at a later date. Thus, to signal their capability, they may instead use PCIs.

PCIs and CCA form the defender's overall cybercapacity, which does not necessarily increase solely through increased investment in her PCIs because such a strategy takes valuable resources away from CCA. For instance, a polished strategy document or newly-constructed headquarters is a poor substitute for covert cyberactivity like penetrating the challenger's electricity grid and preparing for a future attack that could be used for retaliation or for demonstrating the defender's cybercapacity. As a result, over-investment in PCIs at the expense of CCA can make a defender weaker. However, the relationship between the defender's overall cybercapacity and her chances at deterrence is not linear—i.e., an increase in one does not necessarily mean an increase in the other. Therefore, a defender with weak cybercapabilities might strategically invest more in PCIs if such an investment maximizes her chances at deterrence, even if it decreases her overall cybercapacity. I will now model this logic explicitly.

Game Overview

This is a game between a challenger (C, "he") and a defender (D, "she"). C considers executing a cyberattack against D. To deter C, D decides how to allocate her resources between public and private cybercapacity and, as a result, which level of PCIs to implement.

D has a *type* $\theta \in \{S, W\}$ that differs in the amount of resources a_θ available to her. The strong defender D_S has many more resources available to her than the weak defender D_W. θ is non-observable to the challenger.

The game starts with Nature's choice. Nature selects that $\theta = S$ with probability π

and that $\theta = W$ with probability $1 - \pi$. The model assumes that both players have a common prior belief and that π is the true probability that the defender is strong. Then D decides how to allocate her resources between PCIs and CCA. After D implements PCIs, C observes it, (possibly) updates his beliefs about D's type, and decides whether he wants to attack D. When C chooses whether to attack, he does so knowing the level of PCIs D implements, but not knowing D's type with certainty in most cases[14] because D's CCA is not completely observable. Section 4.6 displays this two-player game with incomplete information concerning D's type.

Defender. Suppose D has a units of resources available for cybercapacity. Let $I(r)$ denote the PCIs that D can develop with r units of resources and let $N(r)$ denote the CCA that D can develop with r units of resources. I assume that both I and N are increasing in r and that there are diminishing returns to investment in each (i.e. $I'(r)$, $N'(r) > 0$ and $I''(r)$, $N''(r) < 0$).

When D invests r units of resources into PCIs, D's overall cybercapability is $c(r) = I(r) + N(a - r)$. Since c is concave in r, a unique maximum exists.[15] The level of investment in PCIs $\hat{r}$ that maximizes overall capability $\hat{c}$ solves the equation

$$\hat{c} = max_{r\in[0,a]} c(r) = max_{r\in[0,a]} I(r) + N(a - r). \tag{4.1}$$

Let $\hat{I} = I(\hat{r})$ be the corresponding level of PCIs. Notice that $c'(\hat{r}) = I'(\hat{r}) - N'(a - \hat{r}) = 0$, or $I'(\hat{r}) = N'(a - \hat{r})$. Thus $\hat{r}$ can be viewed as an implicit function of a. Differentiating $\hat{r}$ with respect to a yields $\frac{\partial \hat{r}}{\partial a} = N''(a - \hat{r})/(I''(\hat{r}) + N''(a - \hat{r}))$, which is positive for all a, by the diminishing returns assumption. Thus $\hat{r}$ is increasing in a.

[14] C knows D's type in a separating equilibrium, discussed later in Propositions 3.

[15] Recall that cybercapacity is a proxy for the defender's ability to deter a challenger. When cybercapacity is maximized, so is the defender's chances at deterring the challenger from attacking her. D's cybercapacity does not necessarily increase simply by investing more in her PCIs because such a strategy takes valuable resources away from CCA. As a result, it is optimal for the defender to allocate her resources so that marginal returns are equal from $I(r)$ and $N(r)$.

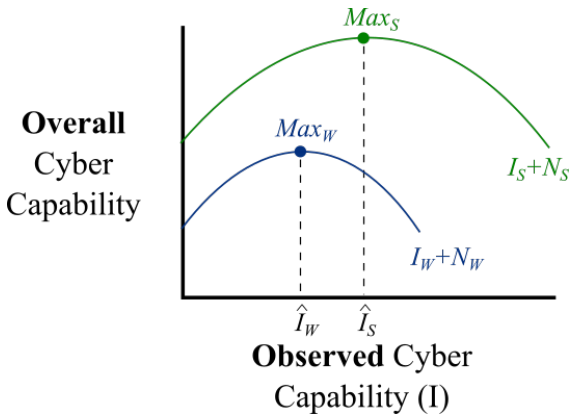


Figure 4.1: *Relationship between Defender's Type and Overall Cybercapacity as a Function of* I_θ

I and N are the same for both strong and weak nations. The two types differ only in the resources available for investment. Let us assume that D_S has two units of resources that she can invest in cybercapacity ($a_S = 2$) and D_W has one unit of resources ($a_W = 1$). When D_θ invests r units of resources into PCIs, D_θ's overall cybercapability is $c_\theta(r) = I(r)+N(a_\theta - r)$. As above, let $\hat{r}_\theta$ denote the level of investment in PCIs that maximizes c_θ, let $\hat{c}_\theta = c_\theta(\hat{r}_\theta)$, and let $\hat{I}_\theta = I(\hat{r}_\theta)$. Recall that $\hat{r}$ is increasing in a. Thus $\hat{r}_W < \hat{r}_S$. Finally, I assume that D_W is able to invest enough resources to attain $\hat{I}_S$.[16]

Because C is able to observe I, it will be convenient to interpret c as a function of I. Since I is a one-to-one function, r can be expressed as a function of I and so N can also be expressed as a function of I. It follows that c_θ can be expressed as a function of I, namely $c_\theta(I) = I + N(a_\theta - r(I))$. The graph of c_θ is shown in Figure 4.1. Here, the x-axis depicts D_θ's observed cybercapacity (I_θ) and the y-axis depicts D_θ's overall cybercapacity (c). Let $Max_\theta = (\hat{I}_\theta, \hat{c}_\theta)$ denote the maximum point of the graph of c_θ. Since $\hat{r}_W < \hat{r}_S$, we have that $\hat{I}_W < \hat{I}_S$. If $0 \leq r \leq 1$, then $c_W(r) = I(r) + N(1 - r) < I(r) + N(2 - r) = c_S(r)$ and so $c_W(I) < c_S(I)$ for all levels of PCIs that D_W can achieve. Thus, for each I, D_S has greater deterrence chances than D_W.

[16] Under this assumption, there will be five equilibria. If D_W cannot attain $\hat{I}_S$, there would only be two equilibria, in which PCIs have no influence (c.f. Proposition 1).

When D decides how to allocate her resources, she faces the following optimization problem:

$$min\, P(I) * Q(c) * L, \tag{4.2}$$

where P is the probability of an attack; Q is the probability that any attack is successful; and L is the loss to a successful attack.[17] P depends on the observed cybercapacity I, whereas Q depends on total cybercapacity c. If the type were known, then each type would invest $\hat{I}$ in PCIs as this level of investment would minimize both P and Q, and hence, the product in Equation 4.2. But, as I show later, in some instances the defender may have an incentive to deviate from this level of investment if doing so reduces the probability of an attack.

Challenger. C attacks D whenever his net gains from attacking outweigh his net gains from not attacking (Equation 4.3):

$$[\eta Q(c_S(I)) + (1-\eta)Q(c_W(I))]G > R. \tag{4.3}$$

Here, η is the posterior belief that the defender is strong. Q, as defined above, is the probability that the attack is successful that depends on D's total capability c, given the observed capability I. In the case of D_S, it is $c_S(I)$ and in the case of D_W, it is $c_W(I)$. G is the gain if the attack is successful. R is C's reservation utility ($R \geq 0$). Section 4.6 of Appendix 4.6 explains in details what goes into this calculation.

Solution Concept. The solution concept is Perfect Bayesian equilibrium, defined by the set of strategies and beliefs:

$$(\sigma_\theta, P(I), \eta(I)),$$

which are probability distributions that (1) D_θ implements each possible level of PCIs; (2) the probability that C attacks D_θ as a function of D_θ's PCIs that C observes; and (3) C's

[17] This choice involves important calculations that I present in Section 4.6.

posterior probability that D_θ is of a strong type, given PCIs he observes. Section 4.6 provides a detailed explanation of the equilibrium components.

Model Equilibria. In this section, I discuss the intuition behind the model equilibria and Section 4.6 provides all formal statements and proofs.

The equilibrium depends on the value of R relative to three cutoff values:

$$Q(c_S(\hat{I}_S))G < [\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G < Q(c_W(\hat{I}_W))G. \tag{4.4}$$

$Q(c_W(\hat{I}_W))G$ stands for C's gains from attacking D_W, given the probability that this attack is successful. $Q(c_W(\hat{I}_W))G$ is the largest out of the three values represented in Inequality 4.4 because it is the easiest to attack D_W. $Q(c_S(\hat{I}_S))G$ is the smallest value because the probability of successfully attacking D_S is the smallest. The value in the middle—$[\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G$—stands for C's gains from attacking D, given that with π probability he is facing D_S and with $1-\pi$ probability, he is facing D_W that pools with D_S and implements $\hat{I}_S$. $Q(c_W(\hat{I}_S)) < Q(c_W(\hat{I}_W))$ because D_W reduces her overall cybercapacity by pretending to be strong and, as a result, increases the probability of C's successful attack.

Figure 4.2 displays the same three cutoff values in relationship to R, depicted by a horizontal line. Let us understand how these relationships affect the type of equilibria that occur in each of these regions.

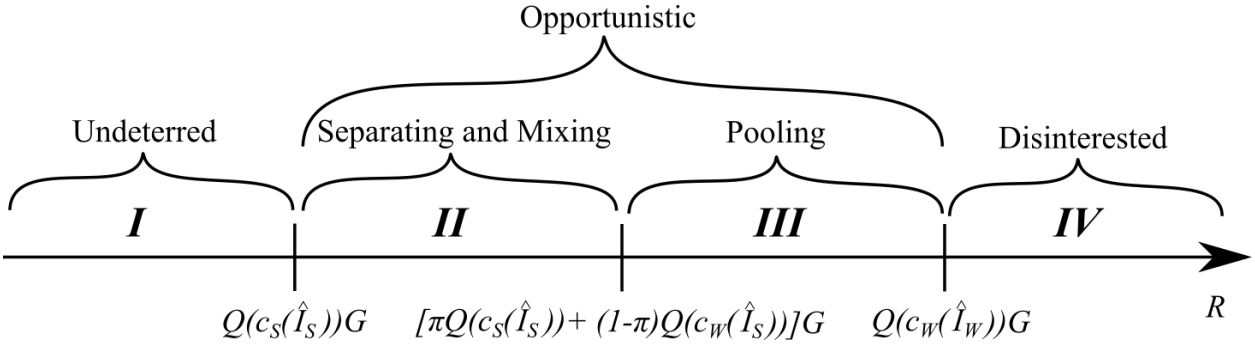


Figure 4.2: *Equilibria and Challenger's Types*

In Region IV where $Q(c_W(\hat{I}_W))G < R$, C's reservation value is higher than C's gain from attacking even if C knows that the defender is weak and implements $\hat{I}_W$. Since C never attacks ($\neg A$), I call him a *disinterested* challenger. In Region I where $R < Q(c_S(\hat{I}_S))G$, C's gains from attacking are higher than the reservation value even if C knows that the defender is strong and implements $\hat{I}_S$. Since C always attacks (A), I call him an *undeterred* challenger. In both regions, both types of the defender have no influence over C's behavior. As a result, they have no incentive to implement anything other than their optimal strategy ($D_\theta \rightarrow \hat{I}_\theta$). Proposition 1 summarizes both equilibria.

Proposition 1. Challenger's Decision to Attack Is Independent of Defender's Public cyberinstitutions.

(a) *If* $Q(c_W(\hat{I}_W))G < R$, D_θ *maximizes her cybercapacity and* C *never attacks. A representative equilibrium of the above unique equilibrium outcome is:* $\sigma_S(\hat{I}_S) = \sigma_W(\hat{I}_W) = 1$, *and* $P(\hat{I}_\theta) = 0$, $\eta(\hat{I}_S) = 1, \eta(\hat{I}_W) = 0$.

(b) *If* $R < Q(c_S(\hat{I}_S))G$, D_θ *maximizes her cybercapacity and* C *always attacks. A representative equilibrium of the above unique equilibrium outcome is:* $\sigma_S(\hat{I}_S) = \sigma_W(\hat{I}_W) = 1$, *and* $P(\hat{I}_\theta) = 1$, $\eta(\hat{I}_S) = 1, \eta(\hat{I}_W) = 0$.

The strategic use of PCIs to deter C occurs in the *signaling region* where there is both the *need* for and the *possibility* of deterrence. Here D_θ's PCIs can influence C, which will take different actions depending on the defender's true type. Specifically, the challenger will attack the defender if he knows that the defender is weak and will avoid attacking if he knows the defender is strong. I call this challenger *opportunistic*. In this region, depicted by Regions II and III in Figure 4.2, there are two pure strategy equilibria (Propositions 2- 3) and one mixed strategy equilibrium (Proposition 4), which depend on where R falls relative to $[\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G$.

If $[\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G < R < Q(c_W(\hat{I}_W))G$ (Region III of Figure 4.2), C will attack D_W if D_W implements $\hat{I}_W$. If D_W mimics D_S and plays $\hat{I}_S$, however, C has no way to tell which type he is facing and believes the defender is strong with probability of the prior π ($\eta = \pi$). At the prior belief, C does not attack. As a result, instead of implementing $\hat{I}_W$ to maximize her overall cybercapacity (point Max_W in Figure 4.3a) and face an attack with certainty, D_W strictly prefers pooling with D_S (point A in Figure 4.3a) and facing no attack. This pooling equilibrium holds only when the probability of the defender being strong (π) is high enough. Note that $[\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G$ is decreasing in π as $Q(c_S(\hat{I}_S)) < Q(c_W(\hat{I}_S))$. The minimum value of π for the pooling equilibrium to hold should be at least

$$\pi > \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}. \tag{4.5}$$

Proposition 2 presents this pooling equilibrium.

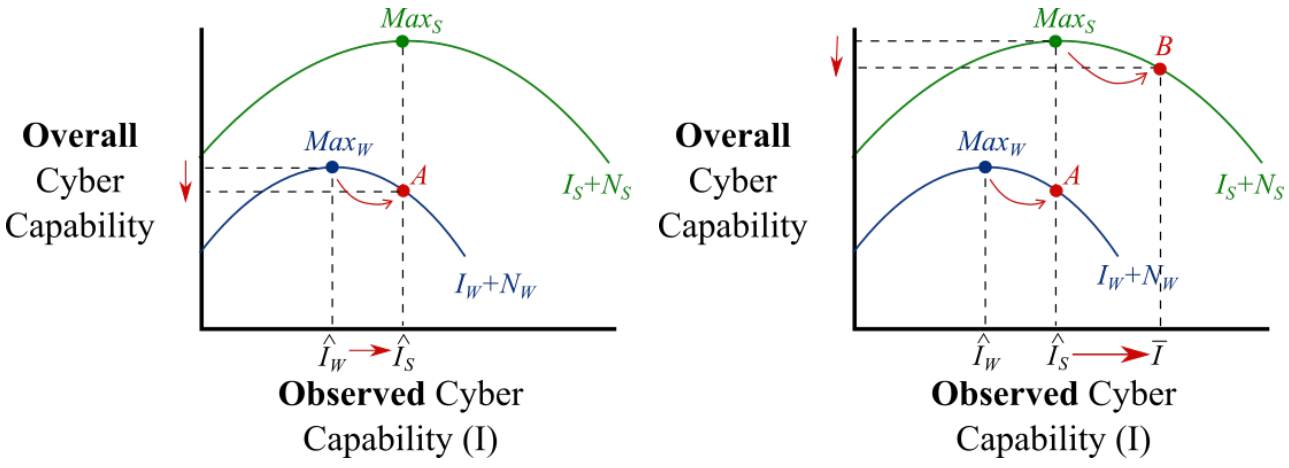
Proposition 2. POOLING EQUILIBRIUM. *If* $[\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G < R < Q(c_W(\hat{I}_W))G$ *and* $\pi > \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}$, D_θ *implements* $\hat{I}_S$ *and* C *attacks only when he sees* $\hat{I}_W$. *A representative equilibrium of the above unique equilibrium outcome is:* $\sigma_S(\hat{I}_S) = \sigma_W(\hat{I}_S) = 1$, $P(\hat{I}_W) = 1$, $\eta(\hat{I}_W) = 0$, *and* $P(\hat{I}_S) = 0$, $\eta(\hat{I}_S) = \pi$; *for any* $I \notin \{\hat{I}_S, \hat{I}_W\}$, $P(I) \in [0,1]$, $\eta(I) \in [0,1]$.[18]

If the probability of the defender being strong is low ($\pi < \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}$), C interprets pooling as weak and attacks when he sees $\hat{I}_S$. This happens if $Q(c_S(\hat{I}_S))G < R < [\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G$ (Region II of Figure 4.2). D_S is aware that D_W is trying to imitate her PCIs. As a result, D_S can take one of the two following actions. First, not wanting to be confused with D_W, D_S alters her behavior to clearly distinguish herself from D_W to ensure that C is deterred. Specifically, D_S spends enough resources to reach a level of PCIs that D_W cannot attain: $I > I_W(1)$ (recall that $I_W(1)$ is the maximum level

[18] It is important to note that off-the-equilibrium beliefs do not matter here because no D has an incentive to deviate from this equilibrium since C does not attack.

of PCIs that D_W can attain) or $\bar{I}$ (point B in Figure 4.3b). Observing $\bar{I}$, C knows that the defender is strong as D_W could not play that strategy. Not able to pool with D_S at $\bar{I}$, D_W implements her optimal strategy $\hat{I}_W$. Since separation is costly as it reduces D_S's overall capacity ($Q(c_S(\bar{I})) < Q(c_S(\hat{I}_S))$), for this equilibrium to hold C should not attack when he sees $\bar{I}$ even though he knows that D_S's overall capacity is reduced ($Q(c_S(\bar{I}))G < R$).

Proposition 3. SEPARATING EQUILIBRIUM. *If* $Q(c_S(\hat{I}_S))G < R < [\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G$, $\pi < \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}$, *and* $Q(c_S(\bar{I}))G < R$, D_W *implements* $\hat{I}_W$, D_S *implements* $\bar{I}$, *and* C *attacks only when he sees* $\hat{I}_W$. *A representative equilibrium of the above unique equilibrium outcome is:* $\sigma_W(\hat{I}_W) = \sigma_S(\bar{I}) = 1$, $P(\hat{I}_W) = 1$, $\eta(\hat{I}_W) = 0$, $P(\bar{I}) = 0$, *and* $\eta(\bar{I}) = 1$.



(a) Pooling Strategy

(b) Strategic Separation Strategy

Figure 4.3: *Defender's Pure Strategy Actions when Facing an Opportunistic Challenger*

Second, if D_S decides not to implement PCIs that D_W is not able to mimic ($I \leq I_W(1)$) because this will weaken D_S's defenses and invite an attack, then a pure strategy equilibrium does not exist with the strategies $\hat{I}_W$ and $\hat{I}_S$ in Region II of Figure 4.2. If both types implement $\hat{I}_S$, C attacks. As a result, D_W has no incentive to play $\hat{I}_S$ because since she is going to be attacked she does better allocating her resources optimally. If each type

implements $\hat{I}_\theta$, then C attacks $\hat{I}_W$ and D_W has an incentive to pool. While there exists no pure strategy equilibrium, there does exist a mixed strategy equilibrium where D_W mixes between $\hat{I}_W$ and $\hat{I}_S$ and C is indifferent between attacking and not.

D_W mixes with a probability that makes C indifferent between attacking and not:

$$\eta = \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}. \tag{4.6}$$

Since $0 < \eta < \pi$ in Region II of Figure 4.2, for this equilibrium to hold, $R < GQ(c_W(\hat{I}_S))$ and $R - GQ(c_W(\hat{I}_S)) < GQ(c_S(\hat{I}_S)) - GQ(c_W(\hat{I}_S))$. C attacks with a probability such that D_W is indifferent between implementing $\hat{I}_W$ and $\hat{I}_S$; it is when $P(\hat{I}_S)Q(c_W(\hat{I}_S))L = P(\hat{I}_W)Q(c_W(\hat{I}_W))L$. Since $P(\hat{I}_W) = 1$,

$$P(\hat{I}_S) = \frac{Q(c_W(\hat{I}_W))}{Q(c_W(\hat{I}_S))}, \tag{4.7}$$

which is less than one since the probability that C's attack is successful is lower if D_W plays her optimal strategy.

Because D_S gets attacked with some probability in this region, he would like to deviate to $\bar{I} > \hat{I}_S$. If $\bar{I} > I_W(1)$, then C will know that the defender is strong and has reduced her overall capacity by deviating to $\bar{I}$. As a result, D_S does not deviate to $\bar{I} > I_W(1)$ because it invites an attack ($Q(c_S(\bar{I}))G > R$). Moreover, D_S does not deviate to any $I < I_W(1)$ because I assume that both types are equally likely to play any out-of-the-equilibrium strategy, as a result, C's out-of-the-equilibrium belief is the prior π.

Proposition 4. Mixed Strategy Equilibrium. *If* $Q(c_S(\hat{I}_S))G < R < [\pi Q(c_S(\hat{I}_S)) + (1 - \pi)Q(c_W(\hat{I}_S))]G$, $\pi = \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}$, *and* $Q(c_S(\bar{I}))G > R$,

1. D_W *mixes between* $\hat{I}_W$ *and getting attacked with certainty and* $\hat{I}_S$ *and getting attacked with probability* $\eta = \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}$;
2. D_S *maximizes her overall cybercapacity;*

3. *C always attacks when he sees* $\hat{I}_W$ *and mixes between attacking and not attacking when he sees* $\hat{I}_S$ *with* $P(\hat{I}_S) = \frac{Q(c_W(\hat{I}_W))}{Q(c_W(\hat{I}_S))}$.

A representative equilibrium of the above unique equilibrium outcome is: $\sigma_S(\hat{I}_S) = 1$, $\sigma_S(\hat{I}_W) = 0$, $\sigma_W(\hat{I}_W) = \sigma_W(\hat{I}_S) = \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}$, $\sigma_S(\bar{I}) = \sigma_W(\bar{I}) = 0$, $P(\hat{I}_W) = 1$, $\eta(\hat{I}_W) = 0$, $P(\hat{I}_S) = \frac{Q(c_W(\hat{I}_W))}{Q(c_W(\hat{I}_S))}$, $\eta(\hat{I}_S) = \frac{R - GQ(c_W(\hat{I}_S))}{G(Q(c_S(\hat{I}_S)) - Q(c_W(\hat{I}_S)))}$, $P(\bar{I}) = 1$, $\eta(\bar{I}) = \mu$.

Table 4.1 lists assumptions and players' actions under different model equilibria. Additionally, it specifies whether the equilibria include any additional parameters that could be found in Propositions 2- 4.

4.3 Comparative Statics

As explained earlier in Section 4.2, the model has five equilibria (Figure 4.2). Each of these equilibria depends on the value of R in relationship to the cutoff points. If the value of R is high, C's gains from not attacking are greater than from attacking and we end up in Region IV (Proposition 1, part (a)). When the value of R decreases to Region III, D_W pools with D_S and C does not attack (Proposition 2). When the value of R becomes even lower, we end up in Region II, where there are two possible equilibria—separating and mixing. In the separating equilibrium, D_S implements the level of PCIs that D_W is not able to imitate. As a result, D_W implements $\hat{I}_W$ and gets attacked (Proposition 3). In the mixing equilibrium, D_W mixes between $\hat{I}_W$ and $\hat{I}_S$ and C mixes between attacking and not attacking (Proposition 4). When the value of R is the lowest, C's gains from attacking are greater than from not attacking and we end up in Region I (Proposition 1, part (a)).

But these equilibria do not only depend on the value of R, they also depend on the following model parameters: π, G, and $Q(c)$. Let us explore how the equilibria range shifts with a change in these parameters. Recall that Nature selects the defender's type θ. With probability π, Nature selects $\theta = S$, and with probability $1 - \pi$, Nature selects $\theta = W$.

Table 4.1: *Model Assumptions & Equilibria*

	Regions				
	I	**II**		**III**	**IV**
Assumptions	$R < Q(c_S(\hat{I}_S))G$	$Q(c_S(\hat{I}_S))G < R < [\pi Q(c_S(\hat{I}_S))+ (1-\pi)Q(c_W(\hat{I}_S))]G$		$[\pi Q(c_S(\hat{I}_S))+ (1-\pi)Q(c_W(\hat{I}_S))]G < R < Q(c_W(\hat{I}_W))G$	$Q(c_W(\hat{I}_W))G < R$
		no deviation to $\bar{I}$	deviation to $\bar{I}$		
Additional Parameters		✓	✓	✓	
D_S's actions	$\hat{I}_S$	$\hat{I}_S$	$\bar{I}$	$\hat{I}_S$	$\hat{I}_S$
D_W's actions	$\hat{I}_W$	mixes between $\hat{I}_W$ & $\hat{I}_S$	$\hat{I}_W$	$\hat{I}_W$	$\hat{I}_W$
C's actions	A	mixes between A and $\neg A$	A if $\hat{I}_W$	$\neg A$	$\neg A$
Equilibria		*Mixing*	*Separating*	*Pooling*	
Results	***PCIs have no effect***	***PCIs may deter***	***PCIs may deter***	***PCIs may deter***	***PCIs have no effect***

C–challenger; D–defender; R–C's reservation value; $Q(c)$–probability of C's successful attack; G–C's gains from attacking; π–C's prior belief that D is strong; D_S–strong defender; D_W–weak defender; $\hat{I}_S$–PCIs optimal for a strong defender; $\hat{I}_W$–PCIs optimal for a weak defender; $\bar{I} > \hat{I}_S > \hat{I}_W$; A–attack; $\neg A$–no attack; PCIs: Public cyberinstitutions.

When $\pi = 1$, $[\pi Q(c_S(\hat{I}_S)) + (1-\pi)Q(c_W(\hat{I}_S))]G = Q(c_S(\hat{I}_S))G$ and as a result Region II in Figure 4.2 disappears.[19] This result shows that with an increase in the probability of the defender being strong π, weak nations are more likely able to deter their adversaries by pretending that they are strong.

With an increase in C's gains G, the boundaries of all regions in Figure 4.2 shift to the right. As a result, Region IV shrinks because some weak types that were able to deter C by maximizing their overall capacity will start pooling. Similarly, Region II absorbs some portion of Region III because some weak types that were able to deter by pooling in Region III will now start mixing and some strong types will separate themselves from weak types. Lastly, Region I where deterrence is not possible will expand. This result shows that with an increase in C's gains from attacking, it becomes much more difficult to deter C. We observe the same set of changes with an increase in the probability of C's successful attack $Q(c)$.

Now, let us examine how real-world factors can cause these changes in parameters, resulting in equilibria shifts. The probability of C's successful attack $Q(c(I))$ is a function of D's overall capacity, which is a function of D's PCIs. In other words, how D decides to allocate her resources between PCIs and CCA determines how successful C's attack will be. Among a plethora of factors that can affect D's resource allocation, I focus on public opinion and the influence of D's alliances. I also consider how the influence of D's alliances and D's resolve affect C's gains G.

Public Opinion. Seventy percent of Americans expect that the U.S. public infrastructure and financial systems will experience significant cyberattacks in the next five years (Smith 2018). To address this potential concern of voters, politicians can over-invest in PCIs to "signal to their domestic audience that they are taking actions to solve the problem" (Kostyuk 2019*b*: #50). This sub-optimal resource allocation might make people feel more secure and guarantee leaders' reelection (Gelpi, Reifler and Feaver 2007; Gronke, Koch

[19] Note that if $\pi = 0$, then there are still four regions in Figure 4.2, since $Q(c_W(\hat{I}_S)) < Q(c_W(\hat{I}_W))$.

and Wilson 2003).[20] But the effectiveness of these measures is often doubtful (Bueno de Mesquita 2007). An increase in public cybercapacity results in a decrease in overall capacity, causing an increase in the probability of a successful attack. Corollary 1 summarizes this counter-intuitive result.

Corollary 1. PUBLIC OPINION: *With an increase in pro-PCI sentiment among the population, D may implement a higher level of PCIs, leading to a decrease in D's overall cybercapacity and an increase in the probability of C's successful attack.*

Alliances. The presence of a strong ally for the defender can increase chances of extended deterrence (Danilovic 2001; Huth and Russett 1988; Leeds 2003; Weede 1983) because the combined military capacity of an alliance can reduce the challenger's gains (Benson, Meirowitz and Ramsay 2014; Leeds 2003; Morrow 1994; Smith 1995; Yuen 2009; Zagare and Marc Kilgour 2003). The larger this combined capacity, the lower the challenger's gains or decreasing the probability of successful attack (Danilovic 2001; Fearon 1992; Huth and Russett 1988; Leeds 2003; Weede 1983). This will shift all equilibria in Figure 4.2 to the left, expanding the regions where deterrence can work.

Additionally, pressure from alliances can often explain a state's decision to aggregate its military capabilities (Schweller 1994; Sweeney and Fritz 2004). As a result, a strong ally can also affect the defender's resource allocation. For example, despite the fact that Estonia mostly faces cybercrime, influence operations, and ransomware attacks as opposed to state-sponsored cyberattacks (*Annual Cyber Security Assessment 2017 Estonian Information System Authority* 2017, 9), the country prioritizes full operationalization of its cyber command to be on par with its North Atlantic Treaty Organization (NATO) allies (*National Defence Development Plan 2017-2026* 2017). Strong allies often provide resources to their weaker partners to increase the latter's capacity. To appear strong and satisfy their

[20] Variation in regime type affects the extent to which public opinion matters on leaders' decisions to use force (Baum 2004; Berinsky 2009; Holsti 2004).

allies, weaker partners may choose to over-invest in PCIs to appear strong. Such resource misallocation will shift all equilibria in Figure 4.2 to the right, reducing the regions where deterrence can work. As a result, pressure and assistance from allies have an ambiguous effect on deterrence. Corollary 2 summarizes this counter-intuitive result.

Corollary 2. ALLY SUPPORT: *An increase in D's ally influence, either in the form of support or pressure, has an ambiguous effect on deterrece. On the one hand, it might lead to a decrease in C's gains, reducing the probability of C's attack. On the other hand, it might lead to an increase in D's level of PCIs, leading to a decrease in D's overall cybercapacity and an increase in the probability of C's successful attack.*

This ambiguous effect of alliances may depend largely on the credibility of mutual defense commitments. If the credibility is low or seemingly conditional, as recent President Trump's remark on NATO allied defense spending seemed to suggest (Haltiwanger 2019), then incentives to over-invest are more likely. These incentives to over-invest might be particularly true for the cyberrealm, where allies may disagree much more on what kinds of responses are appropriate, leading even to a stronger case that alliances are not likely to help deterrence much.

Resolve. As discussed in Section 4.2, for deterrence to be successful, D must demonstrate her resolve and capability (Schelling 2008). My model presents a simple case that assumes that D has a high resolve to use her capability to respond to C. What happens if we relax this assumption? If we view resolve as a parameter of C's gains G, an increase in resolve will reduce G, shifting all equilibria in Figure 4.2 to the left and, as a result, expanding the regions where deterrence can work. Corollary 3 summarizes this result.

Corollary 3. DEFENDER'S RESOLVE: *An increase in D's resolve might lead to a decrease in C's gains from attack, reducing the probability of C's attack.*

While these equilibria shifts are plausible, they are unlikely. Resolve, in a reduced form, is a

country's reputation for defending itself over years. It is an observable feature. The country cannot have resolve without demonstrating it, as summarized by *Dr. Strangelove*: "the... whole point of the doomsday machine... is lost... if you keep it a secret!"

4.4 Evidence

The novelty, secrecy, and sensitivity of the topic of cyber deterrence prevents me from conducting a rigorous empirical test of my findings. Instead, this paper aims to demonstrate the empirical plausibility of my theory and provide support for my model equilibria, using elite interviews and case studies of elections.

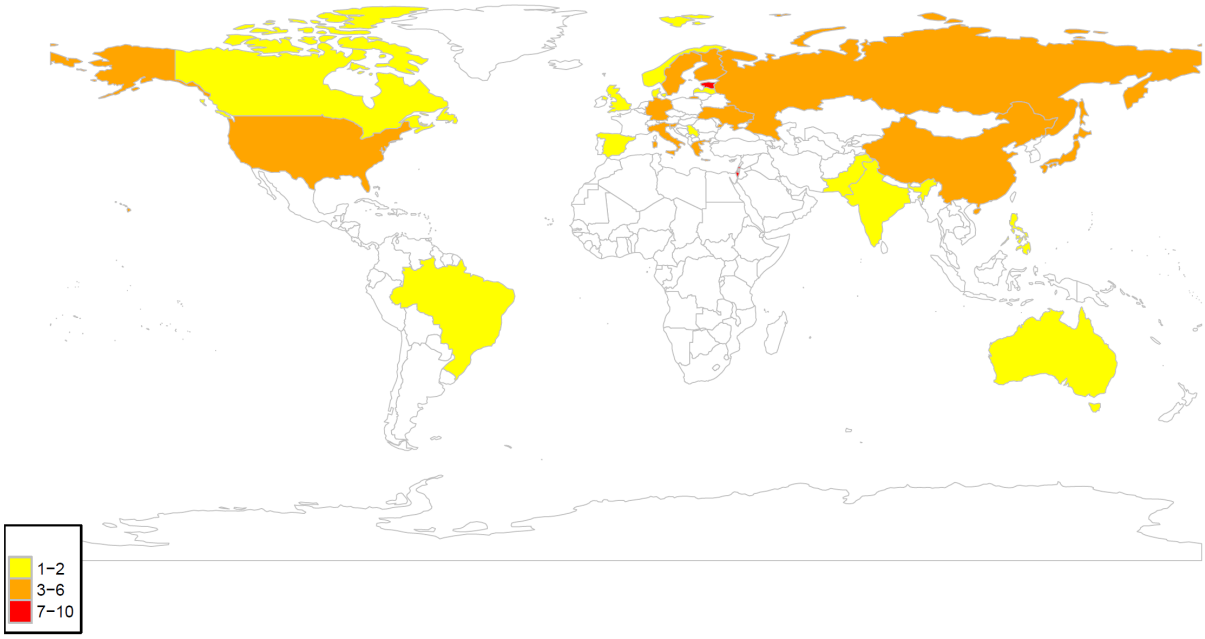
Interviews

I conducted sixty-five interviews with cybersecurity experts from twenty-five countries most of whom were either current or former government employees.[21] Figure 4.4 displays the number of interviews that I conducted in-person or via video calls or emails between February and December of 2018. In Israel and Estonia, I was able to conduct nine interviews during this time.[22]

My interviewees pointed to two trends in the defender's behavior. First is pooling behavior among weak cyber nations where instead of developing cybercapabilities solely for intelligence collection, for instance, these weaker cyber countries start developing offensive cybercapabilities within their militaries. The main purpose of this "loud" signal, contrary to quiet cyber intelligence operations, is "to signal the country's readiness to go beyond its national borders to punish cyber aggressors" (Kostyuk 2019*b*: #11). However, careful examination of these public signals shows that the stated capability is not always present. For instance, when asked for concrete details about the recruitment and training of cyber

[21] I received an IRB approval to conduct my interviews on February 14, 2018 (Study #HUM00127749).
[22] This section provides only a brief overview of the main trends from my interviews. Section 4.6 elaborates on these trends.

Figure 4.4: *Number of Interviews per Country (February-December 2018)*



soldiers, silence, vague responses, or the excuse that many countries were finding it difficult to recruit cyber warriors into their forces followed (Kostyuk 2019*b*: #11, #20, # 35, #49). This discrepancy between stated and actual capabilities may hint that countries use easy to observe but difficult to verify public cyberinstitutions to make their adversaries overestimate their existing cybercapabilities in the hopes of deterring them from attacking.[23]

Second is a strategic separation of strong cyber nations where despite their significant cybercapabilities, cyber powers continue to invest in their public cyberinstitutions to differentiate themselves from weaker nations. For instance, Russia has established information warfare units (Reuters 2017) and is committed to invest between $200 million and $250 million USD per year to significantly strengthen its offensive cybercapabilities, and to create a cyber-deterrent that "will equate to the role played by nuclear weapons" (Gerden 2016). Such additional investments and multiple public cyberinstitutions signal "mostly failure" of the already implemented efforts (Kostyuk 2019*b*: #20). If deterrence had

[23] Other reasons why a country might prioritize developping PCIs over CCA include an appeal to public, cooperation with allies, and prestige (Kostyuk 2019*b*).

worked and the country was ready and confident in its ability to defend itself in cyberspace, it would not need "to make [any additional] noise" (Kostyuk 2019*b*: #20).

My interviewees profess the belief that deterrence is working in the case of strategic cyberattack scenarios but remain skeptical of cyberinstitutions as an effective deterrent mechanism, citing the difficulty of demonstrating this effect empirically as a major challenge. They point to two signs of successful deterrence. First, the decision to design cyber weapons with more care and precision shows that states have started practicing some restraint as more nations become cyber-dependent (e.g., built-in restrictions in the WannaCry and NotPetya attacks) (Kostyuk 2019*b*: #48, 49). Second, cyber powers have changed their cyber strategies. With an increase in China's reliance on the Internet, resulting in an increase in China's own cybervulnerability, the country has changed its cyber force posture from brinkmanship to calibrated escalation, signaling to its adversaries that it wants to avoid full-scale retaliation (Cunningham 2018).

Case Studies of Elections

My theory is agnostic regarding the type of a strategic cyberattack that a nation prefers to deter. As one way to demonstrate that my theory holds, I draw evidence from illustrative examples from elections (Section 4.4 and Section 4.4 from Appendix 4.6). I focus on the presence or absence of *state-directed*[24] election-interference campaigns because such campaigns constitute a prominent subset of strategic cyberattacks. After the interference in the 2016 U.S. elections, many nations added election protections to their top national-security priorities. Given that 169 nations will have either presidential or parliamentary elections in the next four years, and that all of these nations are vulnerable to potential election-interference campaigns, the importance of understanding how to deter such campaigns will only continue to grow.

[24] Section 4.6 defines types of actions can constitute *election interference* as well as the various levels of involvement a state can have in such actions.

My comparative case study method focuses on Kremlin-directed attempts to influence electoral campaigns in Western democracies. I choose the most similar cases for my comparison (George 2019); they share the same cyber-capable attacker (Russia), have similar targets (Western democracies), use the same methods (cyber and information operations executed by the same set of actors), have the same purpose (election interference), and have similar time frames (2016-2018). They differ, however, in the level of cyberinstitutions that the targets implement.

My model predicts that Moscow is deterred when it overestimates its target's cybercapacity as a result of observing the target's cyberinstitutions. This can be seen in the 2017 Swedish election. In the other two scenarios, public cyberinstitutions had no effect on the Kremlin's decision whether to attack. In the German 2017 elections, a combination of non-cyber factors shifted Russia's cost-benefit calculus in favor of not attacking even before cyberinstitutions were put in place (Section 4.6). In the U.S. 2016 elections, Moscow was willing to pay any cost and risk any potential U.S. (cyber and/or non-cyber) retaliation for an influence campaign that could help create a global authoritarian fraternity (Section 4.6).

2018 Swedish National Elections: Opportunistic Challenger & Pooling Equilibrium

The 2018 Swedish national elections provide support for the pooling equilibrium in which the challenger is opportunistic (Region III in Figure 4.2). By investing significant resources into PCIs, Sweden, as a middle power, was able to create an impression that it possessed significant cyber defenses and offenses and, as a result, was able to deter the Russian government from interfering in the 2018 Swedish elections.

Why did Russia consider interfering in the Swedish electoral process? Sweden's non-alignment policy has always served as a guarantee of Russia's security. Recently, however, Sweden shifted its military non-alignment position by strengthening its

international defense cooperation with NATO (Kunz 2015). In response, Russia's defense minister Sergei Shoigu described Sweden's involvement in NATO activities as "worrying" and added that "such steps...[were] forcing us to take response measures" (*Russia Concerned by Efforts to Draw Finland, Sweden Into NATO - Defense Minister* 2018). Military actions and/or economic sanctions are possible response measures, although to date, Russia has pursued neither of these. The Ukrainian and Syrian conflicts, combined with NATO-Swedish defense cooperation (even if it falls short of collective defense) are most likely responsible for preventing Russia from taking a military approach.

Russia is, on the other hand, a mastermind of influence campaigns and has been preparing a strong foundation for such a campaign on the Swedish population for some time. Starting in 2014, the Swedish information landscape witnessed an increase in disinformation campaigns, led by trolls, bots, and Kremlin-sponsored media outlets, such as *Sputnik International* (Kragh and Åsberg 2017, 774). Even after the Sweden-targeted version of *Sputnik International* was terminated in the spring of 2016, other cyberoperations and information campaigns aimed at influencing the Swedish public opinion continued. Russian actors were behind a series of distributed denial-of-service (DDoS) attacks[25] against Swedish news sites and a disinformation campaign about NATO in the Swedish media.[26] Moreover, in 2016, the Swedish authorities reported an increase in information campaigns aimed at "polarizing Swedish society, undermining stability, and spreading falsehoods" leading up to the 2018 Swedish elections (Cederberg 2018, 5). A 2018 U.S. Senate report confirms this by providing evidence that Sweden remained one of the few "favorite target[s] of the Kremlin's propaganda machine" (*Putin's Assymetric Assault on Democracy in Russia and Europe* 2018, 109).

These ongoing cyber and information operations were bolstered by a political climate of anti-immigration sentiment in both the Swedish parliament and populace. Immigration

[25] These attacks flood a website with multiple requests, making it crash.
[26] See https://www.documentcloud.org/documents/4627057-16-2517-CKK-2017-09-15-State-Production-3.html

has always been a contentious issue in Swedish politics, recently exacerbated by the Syrian refugee crisis. Over the last five years, Sweden, a country of ten million, has welcomed 165,000 asylum-seekers from the Middle East (Cerrotti 2017). To demonstrate how polarizing the topic of immigration is in Swedish politics and among its population, let us look at the Sweden Democrats party. Using immigration as one of its agenda items, the far-right Sweden Democrats became the third largest party in the Swedish parliament in 2018 after having occupied only two seats in 2010 (Johnson and Evans 2018). The party's anti-immigration stance and the divide in the general population over the immigration issue presented the perfect environment for the Kremlin's influence campaigns.

However, by 2018, in the immediate lead-up to the election, Kremlin-linked disinformation campaigns seemed to fade, and there was no outright election interference (Cederberg 2018). Why? What stopped Russia from interfering in the Swedish elections?

I argue that the Swedish government's persistence, drive, and transparency in establishing public cyberinstitutions aimed at protecting its elections most likely convinced Russia that an interference campaign would have been too costly. Even prior to Russia's 2016 U.S.-election interference, the Swedish government took significant publicly observable steps to improve its cyber defense and offense in order to deter future information operations and cyberoperations. Having witnessed Russia's interference in the U.S. elections, Sweden, assuming that its 2018 election would be the Kremlin's next target, preemptively substantially increased their already ongoing efforts.

Swedish defense started with clearly defined priorities. As early as 2015, Sweden's Defense Policy named protection of democracy as one of the country's security objectives (*Sweden's Defense Policy: 2016 to 2020* 2015)—an objective reiterated in *National Cybersecurity Policy* (2017). The documents laid out a series of measures aimed at creating better cyber defenses to "raise the threshold [of] attacking Sweden" (*National Cybersecurity Policy* 2017, 19). Importantly, Sweden has designated its election systems as critical infrastructure.

The government also increased the budgets of existing agencies to include election protection into their scope, and it established new agencies, forums, and programs to protect against election interference and disinformation campaigns. The Swedish government's crisis preparation and response agency became the main authority for election coordination. Through a special Cabinet decision, the Swedish Civil Contingencies Agency (MSB), together with the Swedish Security Services and the Election Authority, was tasked with coordinating election protection. The Swedish Agency for Public Management became responsible for "coordinating Swedish public agencies which could carry out 'psychological defense"' (SverigesRadio 2017) during peacetime to "improve the ability of Swedish society to withstand pressure from a potential opponent" (*Sweden's Defense Policy: 2016 to 2020* 2015, 5).

Swedish security services (SÄPO), the Swedish Police Authority, the Election Authority, and MSB established a high-level national forum, responsible for briefing election administrators on potential threats (Cederberg 2018). Having created a confidential report using past cases of election interference, this forum traveled throughout the country to educate local election administrators about how better to protect against these cyberthreats (Cederberg 2018, 15). Similar education campaigns were undertaken by media outlets and political parties (SverigesRadio 2017) and were also carried out in schools (Roden 2017). To prepare for total defense awareness, including in a cyber emergency, MSB produced a pamphlet titled "If Crisis or War Comes" and "sent it to all 4.7 million Swedish households" (Brattberg and Maurer 2018*a*, 29). During all this preparation, SÄPO and other governmental agencies were relatively open and transparent about the initiatives they undertook to address potential interference. Such clear communication might have increased public awareness and the likelihood that Swedes would practice better cyber hygiene (Brattberg and Maurer 2018*a*).

In addition to building better defenses, Sweden invested significant resources in improving

the cybercapabilities of its intelligence agencies to detect external threats and of its military forces to respond to them (Rettman and Kirk 2018). The National Defense Radio Establishment (FRA) and the Military Intelligence and Security Service (MUST) — both responsible for signals intelligence—installed special detection and warning systems to guard against foreign powers hacking into sensitive agencies. In preparation for elections, the government increased expenditure on signals intelligence and added to it new projects that included "the development of advanced offensive smart technologies and tools that have the capacity to weaponize counter-strike actions against...perpetrators" (O'Dwyer 2018).

Sweden also strengthened its military posture. For the first time in more than two decades, the Swedish government decided to substantially increase its defense budget, some of which was to be spent on active cybercapabilities (*Sweden's Defense Policy: 2016 to 2020* 2015, 4-5). The country re-introduced military conscription, with some of these new recruits contributing to the cyber work force. Most importantly, during the country's preparatory efforts to deal with any potential election interference by foreign powers, Sweden's Prime Minister Stefan Löfven emphasized the country's military cyber offensive capability and the government's willingness to use it. For instance, when discussing a three-point plan to stop foreign powers from influencing the 2018 Swedish elections, Löfven publicly claimed that the Swedish Armed Forces were capable of carrying out "active operations in the cyber environment" (SverigesRadio 2017). At a security conference in January 2018, Löfven clearly communicated the country's willingness to act in case of election interference: "To those thinking about trying to influence the outcome of the elections in our country: Stay away!" (as quoted in Cederberg (2018, 11)).

These public cyberinstitutions, put in place before elections, made the Kremlin overestimate Sweden's cybercapacity and, as a result, deterred Moscow from interfering in the 2018 Swedish elections.

Alternative Explanations. There are other factors that, at face value, could have deterred Russia from interfering. Upon closer inspection, however, these factors probably did not play such a role. First is NATO's military capabilities. The NATO-Sweden cooperation defense pact prioritizes security in the Baltic Sea region and the "develop[ment of] interoperable capabilities and maintain[ance of] the ability of the Swedish Armed Forces to work with those of NATO and other partner countries in multinational peace-support operations" (*Relations with Sweden* 2018). In other words, this pact is meant to protect Sweden from a physical invasion by Russia (akin to those in Ukraine and Georgia) but not from election interference.

Second is the threat of Western economic sanctions. The ineffectiveness of these sanctions in changing Moscow's behavior in Ukraine and Syria suggest that they are unlikely to have deterred the Kremlin from executing its plan. Third is Russia's lack of interest in interfering. This explanation contradicts evidence from a U.S. government report that outlines preparatory influence operations aimed at undermining the 2018 Swedish elections (*Putin's Assymetric Assault on Democracy in Russia and Europe* 2018). In the same vein, Cederberg (2018) argued that Russia prioritized the planning of an interference campaign into the 2018 U.S. elections. But, according to former Director of National Intelligence Daniel Coats, there was no vote tampering during the 2018 U.S. elections other than "influence activities and messaging campaigns" by "Russia, and other foreign countries, including China and Iran" meant "to promote their strategic interests" (Coats 2018).

Last is Sweden's actual cybercapacity. Though Russia may have believed that, instead of using pooling to merely appear strong, Sweden had, in fact, become a strong cyber nation, this would have been a misperception on Russia's part. As time passed after the 2018 Swedish elections, it became clear that Sweden was, in fact, not as cyber-strong as their public cyberinstitutions suggested. In particular, there was a discrepancy between the Swedish government's publicly announced commitments and the implementation of these commitments (Cederberg 2018, 29). For instance, despite the Swedish government's

announcements, not only was no psychological defense agency created prior to the elections, the government did not even appoint an investigator responsible for determining this agency's scope. Moreover, government initiatives did not always translate into more resilient defense cybercapability. Even though Sweden's security agencies had been publicly working with political parties and media outlets to increase their awareness of how to deal with cyberthreats and information threats, the information these agencies presented was not necessarily useful in addressing these threats. Similarly, despite Sweden's relatively small population, no studies have measured whether or how Sweden's public awareness campaigns translated into behavioral change. Kostyuk and Wayne (2020) demonstrate that public fails to engage in safer online behavior even though they intended to do so after they were exposed to a cyberattack. Having ruled out the above factors, it appears that Sweden was able to deter Russia from interfering in its 2018 elections by using public cyberinstitutions to make the Kremlin overestimate Sweden's cybercapacity.

4.5 Discussion and Implications

This study has revealed several important patterns of the strategic use of public cyberinstitutions to deter challengers that differ by their type. When the challenger is *disinterested*, he has no interest in attacking the defender, giving the false impression of deterrence success. When the challenger is *undeterred*, he has decided to attack the defender even before observing her PCIs, giving the false impression of deterrence failure. Both scenarios demonstrate that even if PCIs provide the challenger with information about the defender that he did not previously possess, not all challengers will base their decision to attack on this information. Inadequate signaling or a variety of other factors, such as domestic politics, budgetary and legal constraints, or organizational and strategic culture might explain the challenger's choice to attack.

When the challenger is *opportunistic* and only attacks the defender if he perceives

her as cyber weak and avoids attacking if he perceives her as cyber strong, PCIs can indeed play a strategic role. To deter this challenger, weak cyber nations might choose to over-invest their limited resources into public cyberinstitutions and under-invest in covert cyberactivity to appear strong. Strong cyber nations, in their turn, over-invest their limited resources into PCIs to distinguish themselves from weak cyber nations pretending to be cyber strong. This sub-optimal resource allocation, which makes the defender weaker in her overall cybercapacity, can be worthwhile because it may deter the challenger. These results have important theoretical and policy implications.

First, they shed light on a theoretical debate surrounding cyber deterrence. Similar to Tor (2017), this article stresses the need to re-think our reference to absolute nuclear deterrence as a matrix of deterrence success for cyberoperations. Countries do not create cybercapacity to deter low-level cyberoperations; instead, their goal is to stop adversaries from executing strategic cyberattacks, which can cause detrimental damage to the country's economy, prosperity, and security. As the cyberthreat landscape grows and changes, states tend to update their definitions of strategic cyberattacks to reflect this change. Less than a decade ago, for instance, countries focused only on the protection of their critical infrastructure (*Presidential Policy Directive/PPD-21* 2013). Following the 2016 U.S. elections, many nations added election protection to their top national security priorities (*National Cybersecurity Policy* 2017).

As countries constantly re-define what constitutes strategic cyberattacks, adversaries become more creative in the execution of cyberoperations aimed at achieving their strategic goals. For example, in response to Russia's meddling in the 2016 U.S. elections, the U.S. government took steps to protect its 2018 elections, including sanctions. In response to this measure, Russian bots and trolls adjusted their behavior and started operating during the election off-season. For instance, there was a spike in Russian bot and troll tweets in the summer after the 2016 U.S. election (Roeder 2018). These influence campaigns, even if

conducted during election off-seasons, shape public opinion and might affect public voting behavior. Emerging digital technologies, such as artificial intelligence, bring a new set of challenges that governments should be prepared to address. "Deep learning" technology, a method in which computers learn how to solve certain tasks based on the analysis of large information sets, allows to automatically create fake images and videos that are indistinguishable from real content.

Second, over-investment in PCIs demonstrates that states are changing their deterrent tactic. Over the last two decades, states have mainly invested in their CCA to deter adversaries. But this tactic is inefficient because it is: (1) costly due to the diminishing value of cyberoperations after their first use; and (2) ineffective due to the difficulty of cyberattribution. As my findings demonstrates, over-investment in PCIs—in limited cases—allows weak cyber nations to deter their strong adversaries. But it is not clear how long this tactic will be effective. With time, weak cyber nations attempting to imitate strong cyber nations are more likely to be exposed as weak nations and their cyberinstitutions will become less effective in deterring adversaries.

As a result, states should take the signaling of cybercapacity via PCIs with a grain of salt. While PCIs serve as a cyberthreat assessment barometer because they allow a challenger to estimate a defender's ability to conduct cyberoperations, the defender's willingness to use these operations, and the scope of the defender's potential retaliation, this assessment is not precise. To better estimate the defender's cybercapacity, in addition to PCIs, challengers should examine other indicators, such as economic and technological achievements and the defender's reliance on the private sector for cybercapacity. This cumulative approach used to estimate cybercapacity will help governments better evaluate options that minimize the risk of escalation.

My approach of studying deterrence by PCIs is not without limitations. My model oversimplifies real-world scenarios by making assumptions to identify the causal effect of

PCIs on deterrence chances. Specifically, my model views the challenger's decision to attack and the defender's choice to establish PCIs as a one-time decision. In practice, PCIs present a state's cumulative effort to boost its cybercapacity. Similarly, influence campaigns, for example, are composed of many small campaigns that span an extended period. As a result, it is not easy to distinguish between situations in which deterrence by PCIs fails to deter election interference and those in which PCIs were not even considered by the challenger. This is because it is hard to determine how much updating-of-beliefs took place during different stages of the influence campaign.

Moreover, my model equates the defender's probability of successfully retaliating against the challenger with the probability that her cyber defenses hold because PCIs often tend to signal an increase in both offensive and defensive cybercapabilities (Schneider 2019). Future iterations of this model should explore scenarios when it is not the case. For instance, when PCIs only signal an increase in offensive cybercapability, the threat of cyber retaliation might not deter a country that does not have many cyber targets, like North Korea. PCIs that only signal an increase in cyber defenses might deter countries that view attacking well-protected targets as too costly. As a result, by practicing both the deterrence by prevention and by the threat of punishment, the country maximizes its chances at deterrence because it increases the cost of attacking for all attackers.

"If deterrence fails, it is usually because someone thought he saw an 'option' that the... government had failed to dispose of, a loophole that it hadn't closed against itself" (Schelling 2008, 44). By building offensive cybercapabilities, government officials seem to assume that "cybercapabilities alone have a deterrent effect without taking into consideration the strategic requirements that come with deterrence by the threat of punishment, namely credibly holding assets at risk and signaling desired behavior while being willing to face consequences in case of an escalation" (Schulze and Herpig 2018). As my model demonstrates, successful deterrence depends on both a defender's cybercapacity and a challenger's type. Some challengers may

remain undeterred due to a lack of political will in the defending nation to launch a retaliatory cyberattack against an adversary as formidable as, say, Russia or China. In these cases, the potential consequences of entering an escalation cycle with such an adversary may be perceived to be too great to risk. Thus, to maximize the desired deterrent effect of publicly flexing their cyber muscles, nations must explicitly spell out their cybersecurity strategies in order to close the loopholes that adversaries can exploit. Until they do, the pessimistic view of cyber deterrence will persist.

4.6 Appendix

Election Interference

In this section, I define what types of actions can constitute *election interference* as well as the various levels of involvement a state can have in such actions.[27] Specifically, a state can use cyberoperations and/or information operations to interfere in elections. Cyberoperations are conducted via the Internet to collect sensitive information (i.e., cyberespionage) and/or disrupt or degrade the work of a computer, program, or an infrastructure system (e.g., computer-based attacks against an electric power grid, computerized voting machines, etc.). Information operations, by contrast, which are used to influence public opinion in ways that can affect election outcomes (e.g., via propaganda or "fake news"), though often disseminated via the Internet (e.g., on social media platforms), can also be spread by more conventional (non-computer-based) media. Table 4.2 lists a few examples of cyberoperations and information operations that the state can use to influence an election outcome (Galante and EE 2018).

First, a state can use cyberoperations to distort data or system functionality via infrastructure exploitation. For example, the Russian state used cyberoperations to

[27] I use "election interference" and "influence campaign" interchangeably in this paper.

compromise voter-registration and campaign-finance databases in thirty-nine states during the 2016 U.S. elections (Riley and Robertson 2017). Second, a state can use cyberoperations to manipulate votes by changing vote tallies, input, or transmission. For example, a few days before the 2014 Ukrainian elections, the Russian state destroyed key electronic files of Ukraine's Central Election Commission's computer programs that monitor the tallying of votes.

A state can also use information operations to execute (either independently or in combination) the following three actions: false-front engagement, sentiment amplification, and fabricated content. False-front engagement involves the fabrication of a public identity by an individual member of a group in order to use that identity to interact with others. Sentiment amplification involves "the dissemination and prominence of a specific viewpoint" (Galante and EE 2018, 5). Fabricated content involves the spread of false information. To amplify the effect of each of these techniques, a state often uses all three simultaneously. For instance, the Internet Research Agency (IRA)—a Russian company whose owner, Yvgeniy Prigozhin, has ties to Putin—created social media accounts under assumed American identities in order to disseminate incorrect claims that would exploit and amplify divisive political sentiments in the United States (USDepartmentOfJustice 2018*c*).

A state can use both cyberoperations and information operations to influence elections. For instance, in the case of strategic publications, a state uses cyberoperations to illicitly obtain sensitive data, such as internal communications, and then strategically releases them to tarnish the reputation of electoral candidates. After having obtained sensitive information through the 2015 U.S. Democratic National Committee (DNC) hack, the Russian state published this information on DCLeaks.com and WikiLeaks to damage Hillary Clinton's candidacy.

In addition to the six types of actions outlined above that are used to influence elections, I distinguish three possible levels of state involvement in influence campaigns (Table 4.2).

First, at the highest level of involvement, a state can direct a campaign. Examples of state-directed interference include the cyberoperations in the 2014 Ukrainian and 2016 U.S. elections that were attributed to Advanced Persistent Threat (APT) 28 — part of the Russian military's main intelligence directorate, the GRU (Alperovitch 2016). Second, at a lower level of involvement, a state can encourage interference by ensuring that a third party has knowledge of the "state's objectives [and] can partake with reasonable assurance that these efforts will be viewed favorably" (Galante and EE 2018, 6). For instance, prior to the 2016 Brexit referendum, the IRA operated an extensive social media pro-Brexit campaign, but no evidence confirmed that the Kremlin directed this campaign. Third and finally, a state can have no involvement in an election-interference campaign even though the interference is aligned with state objectives. For example, the interference into the 2017 French elections seemed to align with the objectives of the Russian state, but the French National Agency for the Security of Information Systems (ANSSI) confirmed that the Kremlin was not behind the interference and presented the simplicity of the attacks as evidence pointing to an actor with lower cybercapacities than the Russian state (*France says no trace of Russian hacking Macron* 2017).

Table 4.2: *Types of Election Interference*

		Level of State Involvement		
		State-directed	*State-encouraged*	*State-aligned*
Cyberoperations	*Infrastructure Exploitation*	✓		✓
	Vote Manipulation	✓		
Information Operations	*False Front Engagement*		✓	
	Sentiment Amplification		✓	✓
	Fabricated Content	✓	✓	
Cyberoperations & Information Operations	*Strategic Publication*			✓
		2014 U.S. elections	*2016 U.K. referendum*	*2017 French elections*
		Election examples		

This paper focuses on examples of *state-directed* attempts to interfere into foreign elections

by using cyberoperations and information operations.

Game Model in Details

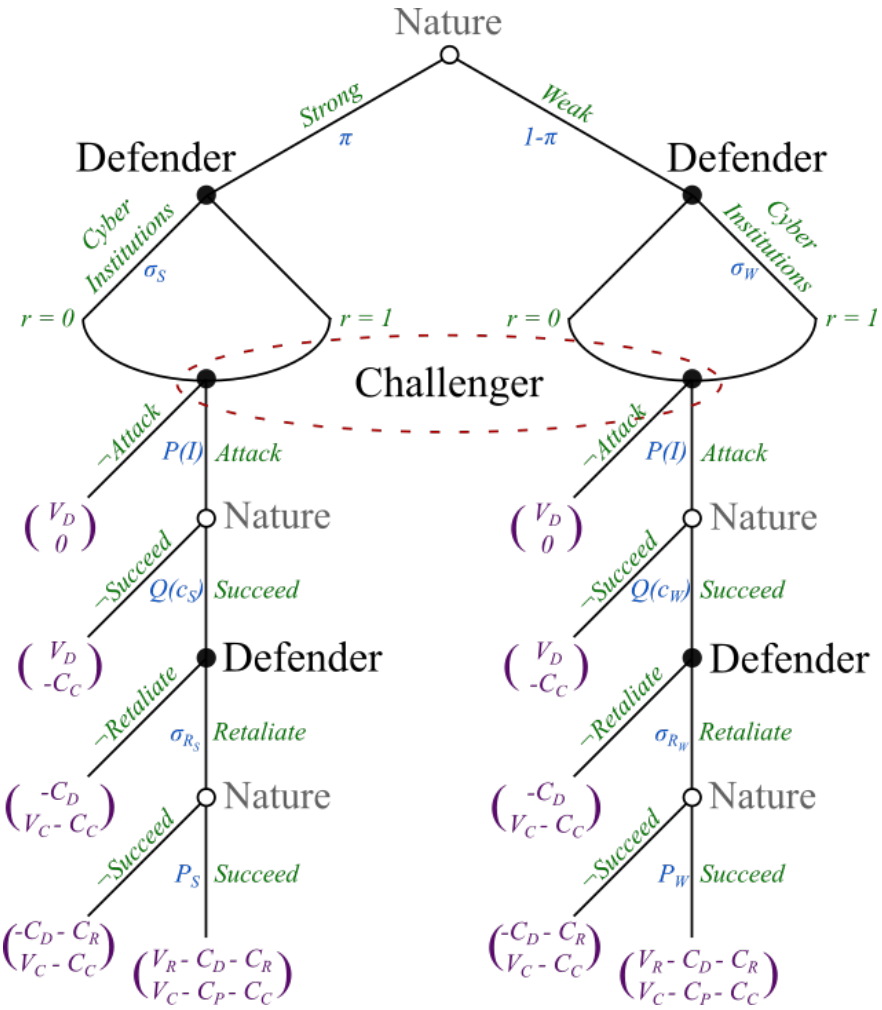
Extensive Form Game Tree of Deterrence by Public Cyberinstitutions. Figure 4.5 displays my two-player game with incomplete information concerning the defender's type. In the first stage, Nature selects that $\theta = S$ with probability π and that $\theta = W$ with probability $1 - \pi$. The model assumes that both players have a common prior belief and that π is the true probability that the defender is strong. In the second stage, D_θ decides how to allocate her resources between PCIs and CCA and the level of PCIs she implements. After D_θ implements PCIs, C observes it, (possibly) updates his beliefs about whether D_θ is strong (η), and decides whether he wants to attack D_θ; the decision to attack also depends on the probability that his attack would succeed and the probability that D_θ would retaliate. The model assumes that even though C cannot observe θ directly, he has a prior belief of θ, derived from, for example, past cyberoperations attributed to the defender and the defender's technological and scientific abilities. When C chooses whether to attack, he does so knowing the level of PCIs D_θ implements, but not knowing D_θ's type with certainty because D_θ's CCA is not completely observable.

If C does not attack the game ends. If C decides to attack D_θ, his attack can either succeed or fail. The probability of a successful attack is determined by D_θ's overall cybercapacity and how she distributes her resources between her public and private cybercapacity. In the next stage, Nature selects that C's attack is successful with probability $Q(c_\theta)$ and that C's attack is not successful and with probability $1 - Q(c_\theta)$. If C's attack does not succeed, the game ends. If C's attack succeeds, D_θ must decide whether to retaliate against C.[28] If D_θ does not retaliate, the game ends. If D_θ retaliates, Nature selects that

[28] The defender knows who the challenger is because the model operates in a closed system with two players and cyber attribution is no longer a challenge. I do not model the cyber attribution challenge for the following two reasons: (1) a state's decision to attribute cyberoperations is no longer a technical challenge but is instead a political decision (Rid and Buchanan 2015; Soldatov and Borogan 2017); and (2) Baliga

D_θ's retaliation is successful with probability P_θ and that D_θ's retaliation is not successful with probability $1 - P_\theta$. The probability of a successful retaliation is determined by D_θ's overall cybercapacity and how she distributes her resources between her public and private cybercapacity. Regardless of whether or not the retaliation is successful, the game ends.

Figure 4.5: *Extensive Form Game Tree of Deterrence by Public Cyberinstitutions*



Defender's Choices & Payoffs. If D successfully deters C and C decides not to attack, D receives value from deterring C, $V_D \in [0, 1]$. If D does not deter C using her PCIs, she pays the cost of being attacked, $C_D \in [0, 1]$. C's choice of action is endogenous to D's PCIs, which

et al. (2018) models the feasibility of deterrence when the cyber attribution challenge is present.

signals to C the defender's type, her cybercapacity, and how damaging retaliation will be if C attacks this type and/or how good D_θ's cyber defenses are, allowing C to estimate how costly it will be for him to break these defenses. C wants to avoid attacking D_S because her retaliation will do more damage to C than will retaliation by D_W and/or it will be much costlier to break D_S's defenses than to break D_W's defenses.

If C attacks, D_θ's cyber defenses may or may not be sufficient to stop this attack from getting through. C's probability of successful attack (Q) depends on D_θ's cybercapacity ($Q \equiv Q(c)$). The model assumes Q is decreasing in c and $Q \in [0,1]$. I define $Q_S = Q(\hat{c}_S)$ and $Q_W = Q(\hat{c}_W)$ as the lowest probabilities that C successfully attacks D_S and D_W. If C's attack is successful, D_θ decides whether to retaliate. If D_θ retaliates, she pays the cost of attempted retaliation, $C_R \in [0,1]$, which incorporates the cost of using cyberoperations whose value diminishes after their first use, regardless of whether retaliation is successful. If retaliation is successful, D_θ additionally receives value from successful retaliation, $V_R \in [0,1]$.[29] The probability that this retaliation is successful (P) depends on D_θ's cybercapacity ($P \equiv p(c)$). The model assumes that P is increasing in c and $P \in [0,1]$. I define $P_S = p(\hat{c}_S)$ and $P_W = p(\hat{c}_W)$ as the greatest probabilities that D_S and D_W successfully retaliate against C.

Challenger's Choices & Payoffs. C attacks D_θ whenever his net gains from attacking outweigh his net gains from not attacking. Equation 4.1 explains when it is the case and what goes into this calculation.

$$P_B V_C - P_B \sigma_{R_\theta} P_A C_P - C_C > R, \tag{4.1}$$

where P_B is C's expectation that D_θ's cyber shields will fail against his attack, having observed D_θ's PCIs; $V_C \in [0,1]$ is the value that C receives from successfully attacking D_θ; σ_{R_θ} is the probability that D_θ retaliates against C as a function of whether C attacks D_θ, having observed her PCIs; P_A is C's expectation that D_θ will retaliate successfully having

[29] Because D_θ's main goal is to deter C, the model assumes that $V_D > V_R$.

observed D_θ's PCIs; $C_P \in [0,1]$ is C's expected cost from D_θ's retaliation; $C_C \in [0,1]$ is C's expected cost from attacking D_θ that incorporates the cost of using cyberoperations whose value diminishes after their first use. R is C's reservation utility, which represents C's net gains from not attacking D_θ ($R \geq 0$).

C's expectation that D_θ's cyber shields will fail against his attack, having observed D_θ's PCIs as

$$P_B = \eta(I)Q(c_S(I)) + (1 - \eta(I))Q(c_W(I)), \tag{4.2}$$

where $Q_S = Q(\hat{c}_S)$ and $Q_W = Q(\hat{c}_W)$ are the lowest probabilities that C successfully attacks D_S and D_W, respectively, or the highest probabilities that D_S's and D_W's cyber defenses successfully hold against C's attack. In Equation 4.1, D_θ's cybercapacity serves as a proxy for C's expectation of how unbreakable D_θ's defenses are — the larger C's expectation of D_θ's cybercapacity, the more likely C is to believe that D_θ's cyber defenses will hold against his attack and, as a result, the more deterred C will be from attacking D_θ. Equation 4.1 also demonstrates the difference between my model of cyber deterrence and the model of deterrence by non-cyber means — in the former, even if C's attack is not successful, D_θ's retaliation is assumed.

C's expectation that D_θ will retaliate successfully having observed D_θ's PCIs as

$$P_A = \eta(I)p(c_S(I)) + (1 - \eta(I))p(c_W(I)), \tag{4.3}$$

where $P_S = p(\hat{c}_S)$ and $P_W = p(\hat{c}_W)$ are the greatest probabilities that D_S and D_W, respectively, successfully retaliate against C. Similarly, in Equation 4.1, D_θ's cybercapacity serves as a proxy for C's expectation of D_θ's retaliation — the larger C's expectation of D_θ's cybercapacity, the more likely C is to believe that D_θ will retaliate against C after being attacked, and the more damaging C believes this retaliation will be. As a result, the larger the expectation of D_θ's cybercapacity, the more deterred C will be from attacking her.

Because the challenger observes the same PCIs to estimate the probability of D_θ's retaliation and the probability that D_θ's defenses withstand his attack, I assume that $P_A = P_B$ and refer to both probabilities as P_A. Similarly, I assume that $P_S = Q_S$ and $P_W = Q_W$ and refer to both probabilities as P_S and P_W.

Solution Concept. An equilibrium to the model is defined by the set of strategies and beliefs:

$$(\sigma_\theta, \sigma_{R_\theta}, P(I), \eta),$$

which are probability distributions that (1) D_θ implements each possible level of PCI; the probability that (2) D_θ retaliates against C as a function of whether C attacks this type, having observed her PCI;[30] (3) the probability that C attacks D as a function of D's PCI that C observes; and (4) C's posterior probability that D is of a strong type, given PCI he observes.

The solution concept is Perfect Bayesian equilibrium $(\sigma_\theta, \sigma_{R_\theta}, P(I), \eta)$, which has four components. First, σ_{R_θ} is the probability distribution over $[0, I_\theta(1)]$ for each type of D, θ. $\sigma_{R_\theta} > 0$ only if this probability maximizes D_θ's expected payoff, given C's decision to attack her having observed D's PCI ($P(I) : [0, I_S(1)] \rightarrow [0, 1]$). D retaliates against C when net gains from retaliation are at least as good as net gains from non-retaliation. D's expected payoff is shown in Equation 4.4.

$$\sigma_{R_\theta}(I) > 0 \Leftrightarrow I \in \arg\max_I \left[(1-\sigma_{R_\theta})(-C_D) + \sigma_{R_\theta} \left[p(c_\theta)[V_R - C_D - C_R] + (1-p(c_\theta))(-C_D - C_R) \right] \right] \tag{4.4}$$

Second, there is a probability distribution σ_θ over $[0, I_\theta(1)]$ for each type of D, θ. $\sigma_\theta > 0$ only if this probability maximizes D_θ's expected payoff, given C's decision to attack her having observed D's PCI ($P(I) : [0, I_S(1)] \rightarrow [0, 1]$). D's expected payoff is shown in Equation 4.5.

[30] I excluded D_S's and D_W's probabilities of retaliation from the solution concept in Chapter 4 because these probabilities are incorporated into C's gains.

$$\sigma_\theta(I) > 0 \Leftrightarrow I \in \arg\max_I \Bigg[P(I) \Big[Q(c_\theta) \Big[\sigma_{R_\theta} [p(c_\theta)[V_R - C_D - C_R] + (1 - p(c_\theta))(-C_D - C_R)] + (1 - \sigma_{R_\theta})(-C_D) \Big] + (1 - Q(c_\theta))V_D \Big] + (1 - P(I))V_D \Bigg] \quad (4.5)$$

Third, C attacks D with positive probability ($P(I) : [0, I_S(1)] \to [0, 1]$) when net gains from attacking are at least as good as net gains from not attacking, given his expectations of D's type:

$$P(I) \in \arg\max_{P(I)\in[0,1]} \Bigg[(1 - P(I))R + P(I) \Big[P_B \Big[\sigma_{R_\theta} [P_A(V_C - C_P - C_C) + (1 - P_A)(V_C - C_C)] + (1 - \sigma_{R_\theta})(V_C - C_C) \Big] + (1 - P_B)(-C_C) \Big] \Bigg] \quad (4.6)$$

In Condition 4.6, $P_A = \eta(I)p(c_S(I)) + (1 - \eta(I))p(c_W(I))$ and $P_B = \eta(I)Q(c_S(I)) + (1 - \eta(I))Q(c_W(I))$. Since Condition 4.6 is a linear function of $P(I)$, $P(I)^* \in \{0, 1\}\, \forall P_A \neq \bar{P}$ and $\forall P_B \neq \bar{P}$.

Fourth, C updates his posterior beliefs (η: $[0, I_S(1)] \to [0, 1]$) about D's type using Bayes' Rule

$$\eta(I) = \frac{q\sigma_S}{q\sigma_S + (1 - q)\sigma_W}, \quad (4.7)$$

$\forall I$ such that $\sigma_S(I) + \sigma_W(I) > 0$.

Proofs

I am using the following definitions in the proofs:

- Let's define $I(r) = I$, then $r = I^{-1}(I)$.
- $c_\theta(I) \equiv I(r) + N(a_\theta - r) = I + N(a_\theta - r(I))$ is D_θ's cybercapacity if she chooses I_θ, expressed in terms of I;

- $I_{\sigma_\theta} \equiv \{I : \sigma_\theta > 0\}$ is set of PCI for D_θ that will be chosen with positive probability under strategy σ_θ;
- $I_\theta(\bar{P}) \equiv \{I : p(c_\theta(I)) > \bar{P}\}$ is the set of PCI for D_θ that leads to the probability of D_θ's successful retaliation that is higher than $\bar{P}$.[31]

Due to the characteristics of this game, there might exist a lot of equilibria. Therefore, I introduce the notion of *outcome equivalence*. Two equilibria — $(\sigma_\theta, \sigma_{R_\theta}, P(I), \eta)$ and $(\sigma'_\theta, \sigma'_{R_\theta}, P(I)', \eta')$—are outcome-equivalent if the expected payoffs of each player are the same under these two equilibria (Fudenberg and Tirole 1991). The game has a unique equilibrium outcome if any two equilibria are outcome-equivalent. Therefore, I can pick one representative equilibrium if the game has a unique equilibrium outcome.

Defender's choice to retaliate. Examining D's choice to retaliate, I have the following utilities:

$$EU_D(\neg Retaliate) = -C_D, \text{and}$$

$$EU_D(Retaliate) = P_\theta(V_R - C_D - C_R) + (1 - P_\theta)(-C_D - C_R)$$

D is indifferent between retaliating and not retaliating when $EU_D(Retaliate) = EU_C(\neg Retaliate)$, i.e.,

$$P_\theta(V_R - C_D - C_R) + (1 - P_\theta)(-C_D - C_R) = -C_D$$

$$P_\theta V_R - P_\theta C_D - P_\theta C_R - C_D - C_R + P_\theta C_D + P_\theta C_R = -C_D$$

$$P_\theta V_R = C_R, \tag{4.8}$$

where

- P_θ is the probability that D_θ successfully retaliates, which is determined by D_θ's overall cybercapacity and how she distributes her resources at Stage 1,

[31] As mentioned earlier, this could be also viewed as the probability that D_θ's cyber defenses hold.

- V_R is the value that D_θ receives from successful retaliation,
- C_D is D_θ's cost of being attacked, and
- C_R is the cost that D_θ pays for retaliating.

Equation 4.8 derives the defender's choice to retaliate, depicted in Lemma 1.

Lemma 1. A defender retaliates if her value from retaliation, given the probability that retaliation is successful, is greater than her cost ($P_\theta V_R > C_R$).

Being weak implies that P_θ is low, as a result, V_R should be much larger that C_R for D_W to retaliate. D_W often does not have significant cybercapacity and given that D_W faces a strong challenger, I assume that $C_R < V_R$. As a result, I assume that D_W does not retaliate when attacked.[32] On the contrary, D_S gains significant value from retaliation. Not only does she punish C, she also deters other potential challengers from cyberattacking her. As a result, I assume that hyD_S always retaliates when attacked.

Challenger's choice to attack. Examining C's choice of action, I have the following utilities:

$$EU_C(\neg Attack) = R, \text{and}$$

$$EU_C(Attack) = P_B\Big[\sigma_{R_\theta}\big[P_A(V_C - C_P - C_C) + (1-P_A)(V_C - C_C)\big] + (1-\sigma_{R_\theta})(V_C - C_C)\Big]$$
$$+ (1-P_B)(-C_C) == P_B\Big[\sigma_{R_\theta}\big[P_AV_C - P_AC_P - P_AC_C + V_C - C_C - P_AV_C + P_AC_C\big] +$$
$$+ (1-\sigma_{R_\theta})(V_C - C_C)\Big] + (1-P_B)(-C_C) =$$
$$= P_B\Big[\sigma_{R_\theta}\big[-P_AC_P + V_C - C_C\big] + (1-\sigma_{R_\theta})(V_C - C_C)\Big] + (1-P_B)(-C_C) =$$
$$= P_B\Big[-\sigma_{R_\theta}P_AC_P + \sigma_{R_\theta}V_C - \sigma_{R_\theta}C_C + V_C - C_C - \sigma_{R_\theta}V_C + \sigma_{R_\theta}C_C\Big] + (1-P_B)(-C_C) =$$
$$= -P_B\sigma_{R_\theta}P_AC_P + P_BV_C - P_BC_C - C_C + P_BC_C = -P_B\sigma_{R_\theta}P_AC_P + P_BV_C - C_C$$

[32] In Section 4.3, I discuss when it is not the case—D_W has a high resolve and retaliates.

C is indifferent between attacking and not attacking when $EU_C(Attack) = EU_C(\neg Attack)$, i.e.,

$$- P_B \sigma_{R_\theta} P_A C_P + P_B V_C - C_C = R \tag{4.9}$$

If D_θ does not retaliate ($\sigma_{R_\theta} C_P = 0$), then

$$P_B V_C - C_C = R,$$

meaning that C is indifferent between attacking or not if his gains from this attack is the same as the value from his reservation point. Solving for P_B, we obtain

$$P_B = \frac{C_C + R}{V_C} \tag{4.10}$$

If D_θ retaliate ($\sigma_{R_\theta} C_P \neq 0$), then

$$P_B V_C - P_B \sigma_{R_\theta} P_A C_P - C_C = R, \tag{4.11}$$

meaning that C is indifferent between attacking or not if his value from this attack minus the costs of potential retaliation and of an attack is the same as the value from his reservation point. Because the model assumes that $P_A = P_B$,

$$P_A V_C - P_A^2 \sigma_{R_\theta} C_P - C_C = R, \text{or}$$

$$P_A^2 \sigma_{R_\theta} C_P - P_A V_C + C_C + R = 0$$

Solving this for P_A, we obtain

$$P_A = \frac{V_C \pm \sqrt{V_C^2 - 4\sigma_{R_\theta} C_P (C_C + R)}}{2\sigma_{R_\theta} C_P}$$

Without loss of generality, I assume C's reservation utility, R, is equal to 0. As a result,

$$P_A = \frac{V_C \pm \sqrt{V_C^2 - 4\sigma_{R_\theta} C_P C_C}}{2\sigma_{R_\theta} C_P}. \tag{4.12}$$

Because P_A is a probability, two clarifications should be made about Equation 4.12. First, I assume that $V_C^2 \geq 4\sigma_{R_\theta} C_P C_C$, so that both solutions are real numbers. Second, because all

values in this equation are distributed between 0 and 1, I only focus on the positive solution of Equation 4.12 and I denoted it by $\bar{P}$. $\bar{P}$ can be interpreted as the cut-off point for D's successful retaliation probability when C is indifferent between attacking and not attacking.

Equations 4.10-4.12 derive conditions when C uses a cyberattack against D_θ. Specifically, Lemma 2 defines the critical value at which the challenger is indifferent between attacking and not attacking.

Lemma 2. *A critical value of P_A for which the challenger is indifferent between attacking and not attacking is:*

(a) $\bar{P} = \frac{C_C+R}{V_C}$, if $\sigma_{R_\theta} C_P = 0$, and

(b) $\bar{P} = \frac{V_C+\sqrt{V_C^2-4\sigma_{R_\theta} C_P(C_C+R)}}{2\sigma_{R_\theta} C_P}$, if $\sigma_{R_\theta} C_P \neq 0$.

C's choice of action only depends on the relationship between his critical value of being indifferent between attacking or not attacking $\bar{P}$ and his perceived probability of D's successful retaliation against him, P_A, given that he observes PCI. Here, $P_A = p_S(I)\eta(I)+p_W(I)(1-\eta(I))$, where $\eta(I)$ is C's belief that D is strong type and $p_\theta(I) = p(c_\theta(I))$ is D_θ's successful retaliation probability, given the cybercapacity that D_θ obtains, having implemented PCIs. Because this cybercapacity is not always optimal, $p_\theta \leq \hat{P}_\theta$, where $\hat{P}_\theta$ is D_θ's maximum probability of successful retaliation.

Let's consider how the model equilibria change based on the values of P_A and $\bar{P}$. Specifically, we have the following three conditions:

1. If $P_A > \bar{P}$, C does not attack
2. If $P_A = \bar{P}$, C mixes between attacking and not attacking
3. If $P_A < \bar{P}$, C attacks

Because P_A stands for both P_S and P_W, let's now consider how these equilibria change based on the relationship of values of P_S and P_W and $\bar{P}$. Specifically, there are five possible regions:

1. If $P_S > P_W > \bar{P}$, C does not attack
2. If $P_S > \bar{P} > P_W$, C attacks when he sees $\hat{I}_W$ and does not attack when he sees $\hat{I}_S$
3. If $P_S < P_W < \bar{P}$, C always attacks
4. If $P_S > \bar{P} = P_W$, C mixes between attacking and not attacking when he sees $\hat{I}_W$ and does not attack when he sees $\hat{I}_S$
5. If $P_S = \bar{P} > P_W$, C does not attack when he sees $\hat{I}_W$ and mixes between attacking and not attacking when he sees $\hat{I}_S$

Now I consider each of these regions to derive the model equilibria.

Case 1: $\bar{P} < \hat{P}_W < \hat{P}_S$**.** I am going to show that in this region the unique equilibrium outcome is: C does not attack, D_θ get her first-best outcomes—D_θ deters C and D_θ does not retaliate.

First, I consider potential separating equilibria in which $\mathcal{I}_{\sigma_S} \cap \mathcal{I}_{\sigma_W} = \emptyset$. Then I know C's belief $\eta(I)$ is

$$\eta(I) = \begin{cases} 1, & \text{for } I \in \mathcal{I}_{\sigma_S} \\ 0, & \text{for } I \in \mathcal{I}_{\sigma_W} \\ [0,1], & \text{o.w. (off the equilibirum path).} \end{cases}$$

The corresponding on-path P_A is

$$P_A = \begin{cases} p(c_S(I)), & \text{for } I \in \mathcal{I}_{\sigma_S} \\ p(c_W(I)), & \text{for } I \in \mathcal{I}_{\sigma_W}. \end{cases}$$

Since $\bar{P} < \hat{P}_W < \hat{P}_S$, $\mathcal{I}_\theta(\bar{P}) \neq \emptyset$, for both types of D. Each type's best response is choosing any level of PCI within the set $\mathcal{I}_\theta(\bar{P})$ which leads to $P_A > \bar{P}$. Hence, C does not attack on

the equilibrium path. Both types of D get their first-best outcomes and have no incentives to deviate. Therefore, it is a equilibrium.

Second, I consider equilibria in which $\mathcal{I}_{\sigma_S} \cap \mathcal{I}_{\sigma_W} \neq \emptyset$. Then I know C's belief $\eta(I)$ is

$$\eta(I) = \begin{cases} \frac{q\sigma_S(I)}{q\sigma_S(I)+(1-q)\sigma_W(I)}, & \text{for } I \in \mathcal{I}_{\sigma_S} \cup \mathcal{I}_{\sigma_W} \\ [0,1], & \text{otherwise} \end{cases}.$$

The corresponding on-equilibrium path P_A is $P_A = p_S(I)\eta(I) + p_W(I)(1-\eta(I))$. I know that if both types of D choose PCI from their own $\mathcal{I}_{\sigma_\theta}$ set, then for any belief $\eta(I)$, $P_A = p_S(I)\eta(I) + p_W(I)(1-\eta(I)) \Rightarrow P_A > \bar{P}\eta(I) + (1-\bar{P})\eta(I) \Rightarrow P_A > \bar{P}$. Hence C does not attack. Both types of D get their first-best outcomes and have no incentives to deviate. A representative equilibrium of the above unique equilibrium outcome is: $\sigma_S(\hat{I}_S) = \sigma_W(\hat{I}_W) = 1$, $\sigma_{R_S}(\hat{I}_S) = \sigma_{R_W}(\hat{I}_W) = 0$, and $P(\hat{I}_\theta) = 0$, $\eta(\hat{I}_S) = 1, \eta(\hat{I}_W) = 0$. This case proves Proposition 1 part (a) of Chapter 4.

Case 2: $\hat{P}_W < \bar{P} < \hat{P}_S$**.** In this case, D_W has an incentive to imitate D_S. I consider two different assumptions in this case. I define $H \equiv \mathcal{I}_S(\bar{P}) \cap (I_W(1), I_S(1)]$. If $H = \emptyset$, D_W can imitate PCI in H. If $H \neq \emptyset$, D_W cannot imitate any PCI in H because it is beyond her capability for any $I \in (I_W(1), I_S(1)]$, while choosing $I \in H$ is both doable and profitable for D_S.

Case 2.1: $H = \emptyset$. Under this assumption, there is no separating equilibria. Suppose there exists a separating equilibrium in which $\mathcal{I}_{\sigma_S} \cap \mathcal{I}_{\sigma_W} = \emptyset$. Then we know C's belief $\eta(I)$ is

$$\eta(I) = \begin{cases} 1, & \text{for } I \in \mathcal{I}_{\sigma_S} \\ 0, & \text{for } I \in \mathcal{I}_{\sigma_W} \\ [0,1], & \text{o.w. (off equilibirum path).} \end{cases}$$

The corresponding on-path P_A is

$$P_A = \begin{cases} p(c_S(I)), & \text{for } I \in \mathcal{I}_{\sigma_S} \\ p(c_W(I)), & \text{for } I \in \mathcal{I}_{\sigma_W}. \end{cases}$$

Let's consider D_W's strategy. Because $p(c_W(I)) < \bar{P}$ for any $I \in \mathcal{I}_{\sigma_W}$, C attacks D_W. In order for this to be an equilibrium, $p(c_S(I)) < \bar{P}$ for all $I \in \mathcal{I}_{\sigma_S}$, otherwise D_W will deviate to $\mathcal{I}_{\sigma_S}$. That is, $\mathcal{I}_{\sigma_S} \cap \mathcal{I}_\theta(\bar{P}) = \emptyset$. In particular, $\hat{I}_S \notin \mathcal{I}_{\sigma_S}$. Then, $\sigma'_S(\hat{I}_S) = 1$ is a profitable deviation for D_S. Specifically, D_S's expected utility when she deviates to $\mathcal{I}_{\sigma_S}$ is:

$$EU_{D_S}(\sigma'_S) = P(I)'\Big[Q(c_S(\hat{I}_S))\Big[\sigma'_{R_S}\big[p(c_S(\hat{I}_S))[V_R - C_D - C_R] + (1 - p(c_S(\hat{I}_S))(-C_D - C_R)\big] + (1 - \sigma'_{R_S})(-C_D)\Big] + (1 - Q(c_S(\hat{I}_S)))V_D\Big] + (1 - P(I)')V_D$$

$$EU_{D_S}(\sigma'_S) = P(I)'\Big[Q(c_S(\hat{I}_S))\Big[\sigma'_{R_S}\big[p(c_S(\hat{I}_S))V_R - p(c_S(\hat{I}_S))C_D - p(c_S(\hat{I}_S))C_R - C_D - C_R + p(c_S(\hat{I}_S))C_D + p(c_S(\hat{I}_S))C_R\big] - C_D + \sigma'_{R_S}C_D\Big] + (1 - Q(c_S(\hat{I}_S)))V_D\Big] + (1 - P(I)')V_D$$

$$EU_{D_S}(\sigma'_S) = P(I)'\Big[Q(c_S(\hat{I}_S))\Big[\sigma'_{R_S}p(c_S(\hat{I}_S))V_R - \sigma'_{R_S}C_D - \sigma'_{R_S}C_R - C_D + \sigma'_{R_S}C_D\Big] + (1 - Q(c_S(\hat{I}_S)))V_D\Big] + (1 - P(I)')V_D$$

$$EU_{D_S}(\sigma'_S) = P(I)'\Big[Q(c_S(\hat{I}_S))\Big[\sigma'_{R_S}p(c_S(\hat{I}_S))V_R - \sigma'_{R_S}C_R - C_D\Big] + V_D - Q(c_S(\hat{I}_S))V_D\Big] + (1 - P(I))'V_D$$

$$EU_{D_S}(\sigma'_S) = P(I)'\Big[Q(c_S(\hat{I}_S))\sigma'_{R_S}p(c_S(\hat{I}_S))V_R - Q(c_S(\hat{I}_S))\sigma'_{R_S}C_R - Q(c_S(\hat{I}_S))C_D + V_D - Q(c_S(\hat{I}_S))V_D\Big] + (1 - P(I))'V_D$$

$$EU_{D_S}(\sigma'_S) = P(I)'Q(c_S(\hat{I}_S))\sigma'_{R_S}p(c_S(\hat{I}_S))V_R - P(I)'Q(c_S(\hat{I}_S))\sigma'_{R_S}C_R - P(I)'Q(c_S(\hat{I}_S))C_D - P(I)'Q(c_S(\hat{I}_S))V_D + V_D$$

If D_S does not deviate and C attacks, then:

$$EU_{D_S}(\sigma_S) = Q(c_S(\hat{I}_S))\Big[\sigma_{R_S}\big[p(c_S(\hat{I}_S))[V_R - C_D - C_R] + (1 - p(c_S(\hat{I}_S))(-C_D - C_R)\big] + (1 - \sigma_{R_S})(-C_D)\Big] + (1 - Q(c_S(\hat{I}_S)))V_D$$

$$EU_{D_S}(\sigma_S) = Q(c_S(\hat{I}_S))\sigma_{R_S}p(c_S(\hat{I}_S))V_R - Q(c_S(\hat{I}_S))\sigma_{R_S}p(c_S(\hat{I}_S))C_R - Q(c_S(\hat{I}_S))C_D + V_D - Q(c_S(\hat{I}_S))V_D$$

Because $P(I)' \in \{0, 1\}$, $EU_{D_S}(\sigma'_S) \geq EU_{D_S}(\sigma_S)$. Because $c_S(\hat{I}_S) > c_S(I)$ for any $I \in \mathcal{I}_{\sigma_S}$,

$$EU_S(\sigma'_S) > \int_{I \in \mathcal{I}_{\sigma_S}} Q(c_S(\hat{I}_S))\sigma'_{R_S}p(c_S(\hat{I}_S))V_R\sigma_S(I)dI - \int_{I \in \mathcal{I}_{\sigma_S}} Q(c_S(\hat{I}_S))\sigma'_{R_S}C_R\sigma_S(I)dI - \int_{I \in \mathcal{I}_{\sigma_S}} Q(c_S(\hat{I}_S))C_D\sigma_S(I)dI - \int_{I \in \mathcal{I}_{\sigma_S}} Q(c_S(\hat{I}_S))V_D\sigma_S(I)dI + V_D$$

Now, let's consider potential pooling equilibria in which $\mathcal{I}_{\sigma_S} \cap \mathcal{I}_{\sigma_W} \neq \emptyset$. Let's pick any $\bar{I} \in \mathcal{I}_{\sigma_S} \cap \mathcal{I}_{\sigma_W}$, $\eta(\bar{I}) = \frac{q\sigma_S(\bar{I})}{q\sigma_S(\bar{I}) + (1-q)\sigma_W(\bar{I})}$.

1. Suppose $P_{A(\bar{I})} < \bar{P}$, i.e., $P(\bar{I}) = 1$. Then at least one type of D has an incentive to deviate. For example, if $\bar{I} \neq \hat{I}_S$, then $\hat{I}_S$ gives D_S a higher expected payoff than $\bar{I}$. A profitable deviation would be shifting the probability assigned to $\bar{I}$ to $\hat{I}_S$,

$$\sigma'_S(I) = \begin{cases} \sigma_S(I), & \text{for } I \notin \{\bar{I}, \hat{I}_S\} \\ 0, & \text{for } I = \bar{I} \\ \sigma_S(\bar{I}) + \sigma_S(\hat{I}_S), & \text{for } I = \hat{I}_S \end{cases} .$$

   It is easy to check that $\sigma'_S(I)$ indeed is a strategy (a probability distribution,

$\int_I \sigma'_S(I)dI = 1$). Using the definition of D_S's expected payoff, we have:

$$EU_{D_S}(\sigma'_S) - EU_{D_S}(\sigma_S) = \Bigg[P(I)'\Bigg[Q(c_S(\hat{I}_S))\Big[\sigma'_{R_S}\big[p(c_S(\hat{I}_S))(V_R - C_C - C_R) + p(c_S(\hat{I}_S))(-C_D - C_R)\big] + (1 - \sigma'_{R_S})(-C_D)\Big] + (1 - Q(c_S(\hat{I}_S)))V_D\Bigg] + (1 - P(I)')V_D\Bigg] - \Bigg[Q(c_S(\bar{I}))\Big[\sigma_{R_S}\big[p(c_S(\bar{I}))(V_R - C_C - C_R)\big] + (1 - p(c_S(\bar{I}))(-C_D - C_R)\Big] + (1 - \sigma_{R_S})(-C_D)\Bigg] + (1 - Q(c_S(\bar{I})))V_D\Bigg]\sigma_S(\bar{I})$$

This is because:

$$EU_{D_S}(\sigma_S) = \int \sigma_S(I)\Bigg[P(I)\Bigg[Q(c_S(I))\Big[\sigma_{R_\theta}\big[p(c_S(I))(V_R - C_C - C_R) + (1 - p(c_S(I)))(-C_D - C_R)\big] + (1 - \sigma_{R_\theta})(-C_D)\Big] + (1 - Q(c_S(I)))V_D\Bigg] + (1 - P(I))V_D\Bigg]dI$$

$$EU_{D_S}(\sigma'_S) = \int \sigma_S(I)'\Bigg[P(I)\Bigg[Q(c_S(I))\Big[\sigma_{R_\theta}\big[p(c_S(I))(V_R - C_C - C_R) + (1 - p(c_S(I)))(-C_D - C_R)\big] + (1 - \sigma_{R_\theta})(-C_D)\Big] + (1 - Q(c_S(I)))V_D\Bigg] + (1 - P(I))V_D\Bigg]dI$$

Let's assume

$$\Bigg[P(I)\Bigg[Q(c_S(I))\Big[\sigma_{R_\theta}\big[p(c_S(I))(V_R - C_C - C_R) + (1 - p(c_S(I)))(-C_D - C_R)\big] + (1 - \sigma_{R_\theta})(-C_D)\Big] + (1 - Q(c_S(I)))V_D\Bigg] + (1 - P(I))V_D\Bigg] = m(I).$$

$\sigma_S = \sigma_S^{'}$, for all $I \neq \bar{I}, \hat{I}_S$.

$$EU_{D_S}(\sigma_S^{'}) - EU_{D_S}(\sigma_S) = \int \sigma_S(I)^{'} m(I) dI - \int \sigma_S(I) m(I) dI =$$
$$\int_{I \neq \bar{I}, \hat{I}_S} \sigma_S(I)^{'} m(I) dI + \int_{I \in \bar{I}, \hat{I}_S} \sigma_S(I)^{'} m(I) dI - \int_{I \neq \bar{I}, \hat{I}_S} \sigma_S(I) m(I) dI -$$
$$\int_{I \in \bar{I}, \hat{I}_S} \sigma_S(I) m(I) dI = \int_{I \in \bar{I}, \hat{I}_S} \sigma_S(I)^{'} m(I) dI - \int_{I \in \bar{I}, \hat{I}_S} \sigma_S(I) m(I) dI =$$
$$\sigma_S^{'}(\bar{I}) m(\bar{I}) + \sigma_S^{'}(\hat{I}_S) m(\hat{I}_S) - \sigma_S(\bar{I}) m(\bar{I}) - \sigma_S(\hat{I}_S) m(\hat{I}_S) =$$
$$0 + \big[\sigma_S(\bar{I}) + \sigma_S(\hat{I}_S)\big] m(\hat{I}_S) - \sigma_S(\bar{I}) m(\bar{I}) - \sigma_S(\hat{I}_S) m(\hat{I}_S) =$$
$$\sigma_S(\bar{I}) m(\hat{I}_S) + \sigma_S(\hat{I}_S) m(\hat{I}_S) - \sigma_S(\bar{I}) m(\bar{I}) - \sigma_S(\hat{I}_S) m(\hat{I}_S) = \sigma_S(\bar{I}) \big[m(\hat{I}_S - m(\bar{I}))\big].$$

Because $P(I) \in \{0, 1\}$,

$$EU_{D_S}(\sigma_S^{'}) - EU_{D_S}(\sigma_S) \geq \Bigg[Q(c_S(\hat{I}_S)) \Big[\sigma_{R_S}^{'} \big[p(c_S(\hat{I}_S))(V_R - C_C - C_R)$$
$$+ p(c_S(\hat{I}_S))(-C_D - C_R)\big] + (1 - \sigma_{R_S}^{'})(-C_D)\Big] + (1 - Q(c_S(\hat{I}_S)))V_D\Bigg]$$
$$- \Bigg[Q(c_S(\bar{I})) \Big[\sigma_{R_S} \big[p(c_S(\bar{I}))(V_R - C_C - C_R)\big] +$$
$$(1 - p(c_S(\bar{I}))(-C_D - C_R)\Big] + (1 - \sigma_{R_S})(-C_D)\Big] + (1 - Q(c_S(\bar{I})))V_D\Bigg] \sigma_S(\bar{I})$$

Because $c_S(\hat{I}_S) > c_S(\bar{I})$, $EU_{D_S}(\sigma_S^{'}) - EU_{D_S}(\sigma_S) > 0$. Hence, $\sigma_S^{'}(I)$ is a profitable deviation.

The above logic applies to the case $\bar{I} \neq \hat{I}_W$ as well. But $\bar{I}$ cannot be $\hat{I}_S$ and $\hat{I}_W$ at the same time. Therefore, at least one of D_S and D_W has an incentive to deviate.

2. Suppose $P_{A(\bar{I})} > \bar{P}$, i.e., $P(I)(\bar{I}) = 0$. D_S and D_W get the first-best outcomes and have no incentive to deviate. As long as there exists some I such that $P_{A(\bar{I})} > \bar{P}$, I could have pooling equilibria. Now let's find a sufficient condition for this. Define $g(I) = p_S(I)q + p_W(I)(1 - q)$, then $g(I) = p_S(I)q + p_W(I)(1 - q) = p(c_S(I))q +$

$p(c_W(I))(1-q) = p(I + (1 - I_S^{-1}(I))n)q + p(I + (1 - I_W^{-1}(I))n)(1-q)$. One sufficient condition is

$$\max_{I \in [0, I_W(1)]} g(I) > \bar{P} \tag{4.13}$$

If Inequality 4.13 is satisfied, then there exists a set $\mathcal{I}_g \equiv \{I \in [0, I_W(1)] : g(I) > \bar{P}\}$. Hence a representative pooling equilibrium is: $\sigma_S(I_1) = \sigma_W(I_1) = 1$, $\sigma_{R_\theta}(I_1) = 0$, $P(I_1) = 0$, $\eta(I_1) = \pi$, and $P(I) \in [0,1]$, $\eta(I) \in [0,1]$ for $I \neq I_1$, where I_1 is a number in $\mathcal{I}_g$. This case proves Proposition 2 of Chapter 4.

Case 2.2: $H \neq \emptyset$. Under this assumption, $\eta(I) = 1$ for any $I \in H$. Therefore, $P_{A(I)} = p_S(I)\eta(I) + p_W(I)(1 - \eta(I))$ and $p_S(I) > \bar{P}$, for any $I \in H$. As long as D_S chooses PCI in H, she get her first best outcome and D_W cannot imitate D_S and implements $\hat{I}_W$. Since C does not attack D_S, there is no need for D_S to consider retaliation against C ($\sigma_{R_S} = 0$). As assume earlier, D_W does not retaliate, even though she is attacked.

Hence there exists a separating equilibrium outcome. A representative equilibrium is: $\sigma_S(I_0) = 1, \sigma_W(\hat{I}_W) = 1, \sigma_{R_S}(I_0) = 0, \sigma_{R_W}(\hat{I}_W) = 0, P(I_0) = 0, P(\hat{I}_W) = 1, \eta(I_0) = 1, \eta(\hat{I}_W) = 0$, where I_0 is any number in H. This case proves Proposition 3 of Chapter 4. The existence of pooling equilibria shall follow Case 2.1 (part 2).

Case 3: $\hat{P}_W < \hat{P}_S < \bar{P}$. In this case, $\mathcal{I}_\theta(\bar{P}) = \emptyset$ for D_θ. Hence, for any PCI and for $\eta(I)$, $P_{A(I)} = p_S(I)\eta(I) + p_W(I)(1 - \eta(I))$. If $\hat{P}_W < \hat{P}_S < \bar{P}$, $p_S(I)\eta(I) + p_W(I)(1 - \eta(I)) < \bar{P}\eta(I) + (1 - \bar{P})\eta(I) \Rightarrow P_{A(I)} < \bar{P}$, meaning that C attacks when observing any I. Then, D_θ's expected payoff is

$$Q(c_\theta)\Big[\sigma_{R_\theta}\big[p(c_\theta)(V_R - C_P - C_R) + (1 - p(c_\theta))(-C_D - C_R)\big] + (1 - \sigma_{R_\theta})(-C_D)\Big] + (1 - Q(c_\theta))V_D$$

D_θ maximizes $p(c_\theta(I))$ to maximize her expected payoff. I have defined that $\hat{I}_\theta = \text{argmax}\, c_\theta(I)$, since $p(\cdot)$ is a increasing function, $\hat{I}_\theta = \text{argmax}\, p(c_\theta(I))$. As mentioned earlier, D_θ retaliates when $p(c_\theta(\hat{I}_\theta))V_R > C_R$. Therefore, for any equilibrium

$\sigma_S(\hat{I}_S) = \sigma_W(\hat{I}_W) = 1$, $\sigma_{R_S}(\hat{I}_S) = 1$, $\sigma_{R_W}(\hat{I}_W) = 0$, $P(I) = 1$ for any I, $\eta(\hat{I}_S) = 1, \eta(\hat{I}_W) = 0$. This case proves Proposition 1 part (b) of Chapter 4.

Case 4: $\bar{P} = \hat{P}_W < \hat{P}_S$. If $\bar{P} = \hat{P}_W < \hat{P}_S$,

$$C : \begin{cases} \text{mixes} & I = \hat{I}_W, \\ \text{does not attack} & I = \hat{I}_S. \end{cases}$$

In this situation D_W has an incentive to deviate to some $I'_W = \hat{I}_S$ and not to be attacked by C.

Case 5: $\hat{P}_W < \bar{P} = \hat{P}_S$. If $\hat{P}_W < \bar{P} = \hat{P}_S$,

$$C : \begin{cases} \text{attacks} & I = \hat{I}_W, \\ \text{mixes} & I = \hat{I}_S. \end{cases}$$

If $I \in [0, I_W(1)]$ and if D_W implements $\hat{I}_W$, she will be attacked. To avoid that, D_W has an incentive to mimic D_S. Thus, while there does not exist a pure strategy equilibrium in this region, there exists a mixed strategy equilibrium where D_W mixes between $\hat{I}_W$ and $\hat{I}_S$ and C is indifferent between attacking and not.

D_W mixes with probability that makes C indifferent between attacking or not:

$$\bar{P} = \frac{\sqrt{V_C^2 - 4\sigma_{R_\theta} C_P (C_C + R)}}{2\sigma_{R_\theta} C_P},$$

as demonstrated by Equation 4.12.. C attacks with probability such that D_W is indifferent between implementing $\hat{I}_W$ and getting attacked with certainty, and implementing $\hat{I}_S$ and getting attacked with some probability. To calculate this probability, let's assume that C attacks when he observes $\hat{I}_S$ with probability α. If D_W does not imitate D_S, she receives

$$EU_{D_W}(\hat{I}_W, \hat{I}_S) = -V_D + \hat{P}_W(V_R - C_D - C_R).$$

But, if D_W imitates D_S, then

$$c_W(\hat{I}_S) = \hat{I}_W(\hat{I}_W^{-1}(\hat{I}_S)) + N(1 - \hat{I}_W^{-1}(\hat{I}_S)) = \hat{I}_S + N(1 - \hat{I}_W^{-1}(\hat{I}_S)).$$

This is because solving for the level of r, such that a weak type mimics a strong type, I get: $I_W(r) = \hat{I}_S \rightarrow r = \hat{I}_W^{-1}(\hat{I}_S)$. As a result, D_W imitates D_S, when

$$\bar{P}_2 = \mathcal{P}(c_W(\hat{I}_S)). \tag{4.14}$$

Then,

$$EU_{D_W}(I_W^{'} = \hat{I}_S, \hat{I}_S) = (1-\alpha)(0)+\alpha[-V_D+\bar{P}_2(V_R-C_D-C_R)] = \alpha[-V_D+\bar{P}_2(V_R-C_D-C_R)].$$

D_W's payoff from mimicking D_S is

$$\alpha[-V_D + \bar{P}_2(V_R - C_D - C_R)].$$

Her payoff from not mimicking D_S is

$$-V_D + \hat{P}_W(V_R - C_D - C_R).$$

When

$$\alpha = \frac{V_D - \hat{P}_W(V_R - C_D - C_R)}{V_D - \bar{P}_2(V_R - C_D - C_R)}, \tag{4.15}$$

D_W mixes between $\hat{I}_W$ and $\hat{I}_S$. In this case, D_S will not imitate D_W because C attacks D_W. Here we have a *mixed strategy separating equilibrium*, where $\sigma_S(\hat{I}_S) = 1, \sigma_W(\hat{I}_W) = \sigma_S(\hat{I}_S) = \frac{\sqrt{V_C^2 - 4\sigma_{R_\theta} C_P(C_C+R)}}{2\sigma_{R_\theta} C_P}, \sigma_{R_S}(\hat{I}_S) = \frac{V_D - \hat{P}_W(V_R-C_D-C_R)}{V_D - \bar{P}_2(V_R-C_D-C_R)}$, $\sigma_{R_W}(\hat{I}_W) = 0, P(I) = \frac{V_D - \hat{P}_W(V_R-C_D-C_R)}{V_D - \bar{P}_2(V_R-C_D-C_R)}, \eta(\hat{I}_S) = \frac{\sqrt{V_C^2 - 4\sigma_{R_\theta} C_P(C_C+R)}}{2\sigma_{R_\theta} C_P}, \eta(\hat{I}_W) = 0$. This case proves Proposition 4 of Chapter 4.

■

Elite Interviews: Public Cyberinstitutions as a Deterrent

Overview of the Interviews. I personally conducted sixty-five interviews with cybersecurity experts from twenty-five countries in-person or via Skype or email, to control for potential interviewer effects and maintain consistency across interviews. While in total, I contacted 231 experts in 47 countries, many were reserved to speak to me even off the record because of the sensitivity of the topic of cybercapacities for the following three reasons. First, many governments have been developing so-called "cyber weapons" for a while but have not publicly announced such efforts. Second, governments are reluctant to admit that their deterrent efforts were failing and the insecurity of their system. Third, even though the governments announced the development of their cyberinstitutions, they did not want anyone to find out that they were not able to fulfill their proposed plans. A strong governmental control in autocratic regimes might explain hesitation to engage in an interview with me even among non-governmental experts. It took my about 44 hours to conduct all interviews, with the duration between 15 minutes and 3 hours, and a median of 1 hour and mean of 1.48 hours.
Anecdotal Evidence from Interviews. I first examine the defender's behavior and then take a look at the challenger's choice of actions.

The fact that more than one hundred of the world's militaries are said to have some sort of an organization or a unit to address "cyber warfare" might be suggestive of two trends. First is these countries' deterrent intent. When a country starts developing its offensive cybercapability, the most natural fit is to place its offensive cyberoperations within its signals intelligence (SIGINT) agencies because these agencies are the most equipped to deal with "cyber" (Kostyuk 2019*b*: #3). Such a move signals that the country is in the process of utilizing the advantages of cyberspace to primarily collect intelligence. If a country proceeds to the next step and starts creating offensive cybercapabilities within its military, it signals its capability and intent to use its offensive cybertools to go beyond its national

borders to punish cyber aggressors (Kostyuk 2019*b*: #11). Contrary to cyberintelligence, which includes quiet penetration operations that aim to stay undetectable in adversarial networks as long as possible, this *loud* signal of readiness to attack is meant to deter potential perpetrators. A recent U.S. Department of Defense's (DoD) strategy of "active defense," defined as "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy" (*US DoD Active Defense* 2019), is an example of such a public cyberinstitution meant to deter adversaries.

Second is pooling behavior of these nations (Singer and Friedman 2014). Without providing specific details regarding the capabilities of the created units, nations hope to hide their low cybercapacities behind these cyberinstitutions and convince their adversaries that their cybercapacities are real and growing. While there are many examples of this pooling behavior, let us take a quick look at Norway, which created its cyber command back in 2012 (Kostyuk 2019*b*: #4, #15). Despite an eagerness to invest in its offensive cybercapabilities, Norway has not made much progress in the development of these capabilities. A desire to be "forward leaning," which one interviewee describes as a typical Norwegian feature, likely explains why the country was so quick to document its plan to create a cyber military unit (Kostyuk 2019*b*: #11), but it does not explain why the country has been slow in implementing this plan. Instead, the country's desire to pool with strong cyber nations is a more plausible explanation for this behavior.

Norway is not an exception in this regard. During the last few years, many countries have become eager to announce the creation of offensive cybercapacities within their governments' militaries and the adjustment of their cyber doctrines to reflect this change. For instance, the pacifistic nature of the German and Japanese constitutions does not prevent these nations from developing cyber military units and from slowly shifting their cyber defensive postures to more offensive ones (Matsubara 2018; Schulze and Herpig 2018). Recently, French armed forces minister Florence Parly unveiled the country's first doctrine for offensive

cyberoperations (*Public Elements of the Doctrine on Military Cyber Offensive* 2019), stating that France is "not afraid" of using cyber "weapons" in response to cyberthreats (Laudrain 2019).

Careful examination of these public actions and declarations may lead to the conclusion that the stated capability is not always present. For example, with plans to establish military cyberunits, countries tend to report how many cyber soldiers these units will have in a three- or five-year period. While militaries often rely on contractors for the development of a computer code, these contractors are forbidden to execute actual operations on behalf of military. As a result, these newly recruited cyber soldiers should possess at least some basic computer skills to be able to execute cyberoperations against enemies. When asked for concrete details about the recruitment and training of cyber soldiers, silence, vague responses, or the excuse that many countries were finding it difficult to recruit cyber warriors into their forces followed (Kostyuk 2019*b*: #11, #20, # 35, #49).

There are two possible explanations of this discrepancy between stated and actual capabilities. First, it can hint that countries use public cyberinstitutions, which are easy to observe but difficult to verify, as their main strategy of signaling their cybercapacity and resolve in hopes that their adversaries overestimate their true cyber arsenals and intentions. Second, it can be the common maturation trend within militaries in which doctrine and organizational outpaces operations capabilities. China, for example, has an aspirational doctrine since 2001 but took a few years to build up operational capabilities to be able to implement that doctrine in 2005. This is when it make its military cyber organizations/doctrine public.

While many nations create cyberinstitutions to pool with so-called *cyber powers*,[33] these powers, in their turn, implement a more significant level of cyberinstitutions to differentiate themselves from weaker cyber nations. For instance, Russia established information warfare

[33] China, Iran, Israel, North Korea, Russia, the United Kingdom, and the United States (Vavra 2017).

units (Reuters 2017) and has committed between $200 million and $250 million USD per year to significantly strengthen its cyber-offensive capabilities and to create a cyber-deterrent that "will equate to the role played by nuclear weapons" (Gerden 2016). The U.S. DoD's 2017 cyber budget of $6.7 billion USD was devoted to "strengthening cyber defenses and increasing options available in case of a cyber-attack" (U.S.DepartmentOfDefense 2016). Even though its exact number remains unknown, some of this budget was spent on the implementation the U.S. cyber strategy of active defense or on the establishment of other cyberinstitutions. If deterrence had worked and the country was ready and confident in its ability to defend itself in cyberspace, it would not need "to make [any additional] noise" (Kostyuk 2019*b*: #20). Multiple efforts — more investment in cyberinstitutions, in this case — can simply signal "mostly failure" of the already implemented efforts (Kostyuk 2019*b*: #20).

Now, let us examine *how such actions affect the challenger's decisions.* My interviewees were rather skeptical—in line with the model's results—of cyberinstitutions as an effective deterrent mechanism, citing the difficulty of demonstrating this effect empirically as a major challenge. Because cybersecurity is a relatively new area of national security, and most information about decision-making processes regarding this area remains classified, there is no publicly-available evidence suggesting that policy-makers, for example, have decided not to attack a country in cyberspace because they were afraid of that country's potential cyber response. We can assume that U.S. adversaries became more concerned about their networks after Snowden, Stuxnet, and Shadow Brokers, for instance, revealed the skill and organizational capacity of the National Security Agency (NSA). But, an official confirmation of this assumption is lacking.

My interviewees professed the belief that deterrence is working in the case of strategic cyber-attack scenarios—blackouts attacks, for example. They point to two signs of successful deterrence. First, the decision to design cyber weapons with more care and precision shows that states have started practicing some restraint as more nations become cyber-dependent.

Supporting this explanation, one of my interviewees pointed to the built-in restrictions in the WannaCry and NotPetya attacks as "evidence that government agencies might be restraining themselves" (Kostyuk 2019*b*: #48). Without these restrictions, the consequences of these operations could have been more devastating (Vanderburg 2017). Second, cyber powers have changed their cyber strategies. With an increase in China's reliance on the Internet, resulting in an increase in China's own cyber vulnerability, the country has changed its cyber force posture from brinkmanship to calibrated escalation, signaling to its adversaries that it wants to avoid full-scale retaliation (Cunningham 2018).

Election Examples

In Chapter 4, I present the case of the 2018 Swedish elections where PCIs deterred the Kremlin from interfering into this election (Section 4.4). Here, I focus on the two cases where PCIs had not effect on the Kremlin's decision of whether to attack. In the German 2017 elections, a combination of non-cyber factors shifted Russia's cost-benefit calculus in favor of not attacking even before PCIs were put in place (Section 4.6). In the U.S. 2016 elections, Moscow was willing to pay any cost and to risk any potential U.S. (cyber or non-) retaliation for its influence campaign that could help create a global authoritarian fraternity (Section 4.6).

2017 German Federal Elections: Disinterested Challenger

The 2017 German federal elections provide support for the equilibrium in which the challenger is disinterested (Region IV in Figure 4.2). I argue that *German cyberinstitutions had no effect on Russia's decision to stay away from the 2017 German federal elections*. Instead, a combination of non-cyber factors shifted Russia's cost-benefit calculus in favor of not attacking even before PCIs were put in place.

The history of cyberoperations and information operations attributed to the Kremlin a few years prior to the elections demonstrate that the Russian state had interest in

German elections interference. Information operations started in 2013, when three key German-language Kremlin-linked propaganda outlets — *Sputnik Deutsch*, *RT Deutsch*, and *NewsFront Deutsch* — entered the German market (Nimmo 2017) and were later joined by trolls[34] and bots.[35] The 2015 and 2016 cyberoperations against the parliament and political parties demonstrate that Moscow was also eager to obtain sensitive information for potential future use (Herpig 2017). But value from these efforts for an effective influence campaign were overwhelmed by potential costs resulting from the following factors.

First, Germany's balanced media systems, the lack of polarization among the German public, Germany's multiparty and proportional system, and a "gentleman's agreement" between major political parties not to use any information leaked as a result of cyberattacks made it difficult for Moscow to sow confusion in the public (Schwirtz 2017). Second, the only clear beneficiary of these campaigns was the Alliance for Germany (AfD)—the rest of parties supported the sanction regime against Moscow. But when AfD entered the race, they only had between eight and ten percent of vote, which was not enough to gain the majority. Third, the use of old-fashioned paper ballots on the local level afforded Germany with an accurate recount in the event that digitized votes used on the federal level were compromised (Herpig 2017). Lastly, high-level deterrent rhetoric by German politicians referencing a deterioration of the relationship between the two countries if interference occurred likely played a part.[36] Although Putin and Merkel's relationship has eroded over time, alienating Germany—an important bridge between the West and Russia—was not in Russia's interest.

If not these factors, what other factors could have stopped Russia from election interference? Brattberg and Maurer (2018*b*) and Schwirtz (2017) suggest that a failure to

[34] A troll is someone who argues for extreme views without credible sources.

[35] An automated program that runs over the Internet.

[36] During its spring 2017 visit to Moscow, the "Chancellery emissary delivered a stern warning"; in May, Merkel herself issues a warning to Putin, by saying "she assumes 'German parties will be able to decide their election campaign among themselves"'(Beuth et al. 2017); and in June, German President Frank-Walter Steinmeier warned Moscow that "Were [it] to interfere in the election of the Bundestag, then the share of commonalities will necessarily decrease further. That would be damaging for both sides" (as quoted in Brattberg and Maurer (2018*b*, 18)).

influence the 2017 French presidential elections made the Kremlin re-think its approach, since it lost the element of surprise. While quite plausible, the evidence later revealed interference into the French elections was not directed by the Kremlin, although it was aligned with its objectives (Galante and EE 2018).

2016 U.S. Election: Undeterred Challenger

The 2016 U.S. presidential elections provide support for the equilibrium in which the challenger is *undeterred* (Region I in Figure 4.2). Having witnessed the worldwide impact of the mass disclosures of the U.S. government's treatment of private data, Moscow was willing to pay any cost and to risk any potential U.S. (cyber or non-) retaliation for its influence campaign that could help create a global authoritarian fraternity. Having made up its mind before or in 2014, the Russian government was an unstoppable tank moving towards its target and not U.S. cyberinstitutions could have stopped the Kremlin from executing its plan.

Moscow's online campaigns and the Russian intelligence-gathering mission that began in 2014 demonstrate the seriousness of Russia's intentions in implementing its democracy containment doctrine (USDepartmentOfJustice 2018*c*). Specifically, the Russian influence campaign took root back in 2014, when the Internet Research Agency (IRA) began operating a social media campaign, "designed to provoke and amplify political and social discord in the United States" (Mueller 2019, 4). With time, this campaign evolved into "a targeted operation that...favored candidate Trump and disparaged candidate Clinton" (Mueller 2019, 4). In addition to these overt online operations, the Russian government also used covert cyberattacks to achieve its goal. For example, in July 2015, Russia's General Staff Main Intelligence Directorate (GRU) gained access to the Democratic National Committee (DNC) networks; in March 2016, they began cyberoperations aimed to compromise email accounts of Democratic Party officials; and in June 2016, they released content of the stolen data

using WikiLeaks and DCLeaks.com (*Assessing Russian activities and intentions in recent US elections* 2017, 2).

When planning this influence campaign, Moscow likely contemplated between its value and cost. Its lowest value was "undermin[ing] public faith in the U.S. democratic process" and its highest value was "harm[ing Secretary Clinton's] electability and potential presidency" that could have resulted in the change in the U.S. foreign policy (*Assessing Russian activities and intentions in recent US elections* 2017, ii). Even its lowest value was far greater than any costs Russia could envision paying.

If caught, Moscow knew that it faced potential retaliation by the world's military and cyber power. This retaliation, aligned with U.S. foreign policy tools, could have taken one of the following forms: diplomacy, economy, nuclear, and/or military (cyber and non-). Diplomatic retaliation was the least of Russia's worries considering the existing tension between the two countries. Moscow expected that, if elected, Clinton would only exacerbate this tension. The cost of additional economic sanctions—in addition to those that the country already faced for the Ukrainian conflict—was marginal. Moreover, nuclear and military responses to cyber and information operations were off the table.

At the time when the Russian government was about to start its influence campaign, it was not clear whether the U.S. government had the political will to retaliate against the Kremlin using cyber means. If the Kremlin was accused of interference, it could simply cite the difficulty of attributing the origin of cyberoperations to deny their involvement or to blame patriotic hackers for executing these operations, as it has done in the past (Rid 2013). In this case, a U.S. cyber response against the Kremlin might not have been justifiable. Moreover, Washington might have been hesitant to retaliate because of the high U.S. Internet connectivity that created a vast cyberattack surface providing plenty of targets if Russia chose to respond. Lastly, U.S. cyber defenses were not strong enough to deter Russia by prevention because, in 2014, the U.S. government was working on protecting

its own network and critical infrastructure objects from cyberoperations, and had yet to realize the danger of information campaigns.

This evidence demonstrates that there was a significant gap between the value and cost of the Kremlin's influence campaign at its start in 2014. In the following two years, the Kremlin likely felt that military and economic options were unlikely to add any additional costs because Washington was unlikely to change its view on these foreign policy tools. Because Moscow was aware that Washington was building its cyberinstitutions to increase its defenses and improve its offense, the Kremlin must have contemplated the additional cyber costs that it would incur during the influence campaign.

There were a few possible sources of additional costs. The first source was better defenses from cyberoperation and information operations. Washington's cyberinstitutions implemented prior to 2014, meant to deter by prevention, could have given the Kremlin an idea of Washington's best possible defense. *Presidential Policy Directive/PPD-21* (2013), for instance, which focused on critical infrastructure protection might have sent two signals. First, because it did not cover voting machines as part of critical infrastructure, Moscow might have interpreted this as a signal that the government was not paying attention to election infrastructure protection. Second, because critical infrastructure protection was a rather new direction in U.S. cyber policy, Russia might have assumed that Washington, with its vast bureaucracy, would continue working in this direction over the next few years. Because a swift change in U.S. cyber policy was quite unlikely, the Kremlin was, to some extent, confident that Washington was not going to spend significant resources on educating political campaign leaders and the public about the danger of cyberthreats and disinformation operations. But even if it did, the short-term impact of these efforts were quite uncertain, only slightly raising the already relatively low costs of the Kremlin's information operations.

The second source is retaliation via launching an information campaign or executing

cyberattacks. Both options were rather costly and ineffective and would have resulted in relatively minimal costs for the Kremlin. Washington was unlikely to attempt information operations because of Kremlin's tight control of Russia's print, online, and social media and because of Russia's treatment of information as a weapon, allowing its military to respond to such information threats (*Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* 2011).

Similarly, even if Washington spent the necessary time and resources on targeting Russia's critical infrastructure, the damage that Russia experienced would have been limited. For example, it is impossible to hack Russia's entire power grid system at once because most stations are manually controlled and can be restored by flipping a switch. Moreover, the Kremlin periodically tests the "cyber robustness" of all potential targets and does not use U.S. equipment to avoid the risk of Washington's remote-access backdoor (Ryabikova 2019).[37] But, in these hypothetical scenarios, the main question remains: was Washington willing even to consider any of these options for retaliation via cyberspace, given the U.S. high Internet connectivity?

In short, the potential worst-case scenario costs that Moscow faced were lower than the value it would gain by election interference. Thus, the Kremlin's interference campaign was never going to be deterred by U.S. cyberinstitutions.

[37] A *backdoor* is an undocumented portal that allows an attacker to enter the system.

Chapter 5

Limitations and Future Research

5.1 Public Cyberinstitutions: Causes and Effects

This dissertation asks two important questions that have been overlooked by existing scholarship: *What drives the development of public cyberinstitutions (PCIs)?* And *what their effects are?*

To answer the first question, this dissertation delves into the creation of national cybersecurity strategies and the development of military cyberapparatuses—two examples of PCIs that lie on opposite sides of the state cybercapacity spectrum. National cybersecurity strategies, which signal the country's defensive capability, outline a set of basic, initial measures that a country plans to implement to address cybersecurity: public education about the dangers of cyberthreats, technical means to respond to cybercrime, and international cooperation, among others. Similar to the creation of national cybersecurity strategies, the development of military cyberapparatus signals defensive capability, but in a narrower sense. They signal a country's ability to protect its military's networks and systems and, in some cases, objects of national critical infrastructure. More importantly, these agencies signal the country's offensive capability. As a result, the development of a military cyberapparatus

is more a profound, resource- and expertise-intensive step than the creation of a national cybersecurity strategy.

Since these two types of capabilities serve different purposes, the factors that contribute to their development also differ. This dissertation shows that state preferences on cybersovereignty have an important role to play in the spread of national cybersecurity strategies whereas alliance politics plays an important role in the case of the development of military cyberapparatuses. In particular, when developing its first national cybersecurity strategy, a country considers the strategies adopted by nations that share its views on cybersovereignty. When developing its military cyberapparatus, the country complements its allies' behavior. This research also demonstrates irrelevance of any other type of network (i.e., adversaries, neighbors, trading partners, countries that voted similarly on various UNGA resolutions, countries that have joint membership in various intergovernmental organizations, countries that share a colonial past or with the same official language) that could capture the global spread of cybersecurity strategies or military cybercapacity.

In addition to explaining the potential drivers of PCIs, this dissertation also investigates whether a state is able to achieve its primary objective—to deter adversaries from executing cyberattacks against the state by signaling its increased power to hurt. This research demonstrates that this effort can only be successful when an adversary is susceptible to the costs created by these PCIs. Otherwise, PCIs cannot stop determined attackers. Despite this, states tend to over-invest their resources into PCIs instead of distributing them between PCIs and covert cyberactivity to maximize their overall cybercapacity. In particular, weak cyber states over-invest to appear strong and strong cyber states over-invest so that they are not viewed as weak cyber states pretending to be strong.

This dissertation offers a simplified analysis of a complex problem and has two obvious limitations that I plan to address with future research. First, my explanations generally focus on strategic factors of international politics, and do not do justice to domestic politics and, in

particular, the role public opinion plays in a government's decision to develop cybercapability and how the public perceives this capability. Second, it only explains how the state initiates two different types of PCIs, while signaling a public cybercapacity is a complex process that involves a variety of institutions used at once. While this research looks at the initiation of this process, it should also evaluate subsequent steps that involve the adoption of new documents, revisions of old documents, the creation of new agencies, and the extension of existing missions to incorporate new tasks, among others. I expand on these two limitations in the subsequent sections and explain how I plan explore these two main omissions in my future work.

5.2 Limitations and Next Steps

A Missing Puzzle: Domestic Politics & Public Opinion

The governments of the United States and Russia both report that the other country's increase in cyberoffensive capability pose a serious threat to their own national security.[1] To address this threat and to deter each other from using cyberoperations against each other, both countries have been publicly signaling the development of their cyberoffensive capabilities and clarifying the doctrines behind their use. This behavior is not an exception but rather part of a global trend—countries have been spending significant resources to publicly signal their cybercapabilities. Since the conditions under which such deterrent tactics could conceivably "work" are fairly limited (Kostyuk 2019*a*), are these measures intended to deter adversaries or to serve as "security theaters" aimed at gaining political support? If governments use these measures to gain political support, does this strategy work?

To answer these questions, future research can investigate how a country's public

[1] https://taskandpurpose.com/gao-national-security-threats-2019

perceives their and adversarial government's efforts to publicly signal an increase in their cyberoffensive capability. Given that the United State and Russia have been actively developing cybercapacity to deter each other, future research can investigate the American public's evaluation of the increase in cyberoffensive capabilities by the U.S. and Russian governments as well as their preference for how the U.S. government should respond to public increases in such capability by the Russian government. For example, have Americans begun to feel more secure since the U.S. government threatened to retaliate against cyberattacks with all its means in its *Department of Defense Cyberspace Policy Report* (2011)? Do they feel more threatened having learned that the Kremlin created information troops within its army and how, if at all, do they prefer that the U.S. government responds to this action by the Russian government? Similarly, does the Russian public feel safe from external cyberthreats knowing that the Russian government might adopt the "sovereign Runet," allowing Moscow to monitor all Internet traffic in Russia?[2] Or does this law make Russians more frightened of the Kremlin's increasing ability to monitor their online behavior? How do the Russians feel about the *U.S. National Cyber Strategy* (2018) that allows the U.S. government to confront its adversary in adversarial networks and what is their preference for how the Kremlin should respond to this strategy?

To answer these questions, I hypothesize that public signaling of a government's cybercapabilities may play three distinct roles. First, an increase in state cybercapability may cause the public to become complacent because of their over confidence in their government's ability to protect them from cyberthreats, resulting in a lower level of "civil cyberdefense" (e.g., fewer efforts to protect personal and corporate information online) and thereby making them more vulnerable to cyberthreats. Second, such an increase may make citizens worry more about their government's ability to monitor their online actions, making them more willing to engage in safe online behavior. Third, the public might not perceive potential

[2] https://www.rbc.ru/technology_and_media/08/02/2019/5c5c51069a7947bef4503927

threats of cyberoperations from adversarial nations as existential threats, which is how governments often tend to frame them (Fernandino 2018). As a result, citizens might be dissatisfied in their government's over-investment in cybercapability, costing leaders their political office (Gelpi, Reifler and Feaver 2007; Gronke, Koch and Wilson 2003).

To test this theory, I plan to use two sets of survey experiments. The first set will explore the specific mechanisms explaining public perception of their own state's increased cybercapability by looking at the reactions of Americans and Russians. The second set will test the mechanisms that explain public perception of increased cybercapability by the adversarial government, this time examining the Russian public's reaction to increased U.S. cybercapability intended to deter Russian attacks, and vice versa.

The results of these experiments will make a number of contributions to the existing international-relations literature. It will offer the first analysis of public perceptions of these deterrent efforts by their governments and adversarial governments. Existing studies on cybercoercion tend to focus on strategic interactions between major powers (Borghard and Lonergan 2017; Brantly 2016; Gartzke 2013; Libicki 2009; Lindsay and Gartzke 2015; Council et al. 2009; Nye Jr 2017; Valeriano and Maness 2018) and ignore the role that public opinion plays in shaping these interactions.

By focusing on a bottom-up perspective, this research will fill an existing gap in political science and public policy literature by evaluating both an emotional mechanism underlying public perceptions of state offensive cybercapabilities and public evaluation of policy responses to an increase in cybercapabilities by adversarial nations. A few experimental works focus either on emotional mechanisms underlying citizens' cyberthreat perceptions (Canetti, Gross and Waismel-Manor 2016; Jarvis, Macdonald and Whiting 2017; Kostyuk and Wayne 2020) or on public evaluation of policy responses to cyberattacks (Kreps and Das 2017).

Lastly, this research will take a unique approach and study public perception in both

defending and challenging countries. Most existing work take a one-sided approach and examine either public perception of the American foreign policy in relation to Russia (Koopman et al. 1998; Tetlock 2017) or public perception of Russian foreign policy in relation to the United States (Koopman et al. 1998; Zimmerman 2009). By evaluating all four perspectives, this study demonstrates actual, not anticipated or desired, effects of increased cybercapability.

This future research has important policy implications because it will help leaders seeking to formulate public policies meant to protect the psychological health and well-being of their citizenry understand the nuanced cognitive and emotional responses of civilian populations to investments in cybercapability.

Future Work: Measuring State Cybercapacity

The questions that motivated this dissertation are *"What is cybercapacity"* and *"How can we measure it"*? Measuring cybercapacity is a complicated task. Here is just the two reasons of why it is the case.

When it comes to military capacity, secrecy is important for preserving cybercapabilities. States cannot launch parades to show off their cybercapacity and satellite images are not useful in estimating this capacity. While cyberattacks many give a good estimate, they tend to devalue this capability after the first use. The basic parameters for most traditional weapons remain relatively static, but strategically relevant features of certain cyber weapons might look quite different tomorrow (Libicki 2009).

Furthermore, given the ubiquitous presence of the Internet, cybercapacity is more than military capacity intertwined with every single aspect of our life—healthcare, education, transportation, banking, etc. Public education about the dangers of cyberthreats and how to safely surf the web plays a crucial role in raising the country's cyberdefense. Thirty percent of data breaches occur because of "wet-ware"—situations when individual users fail to engage

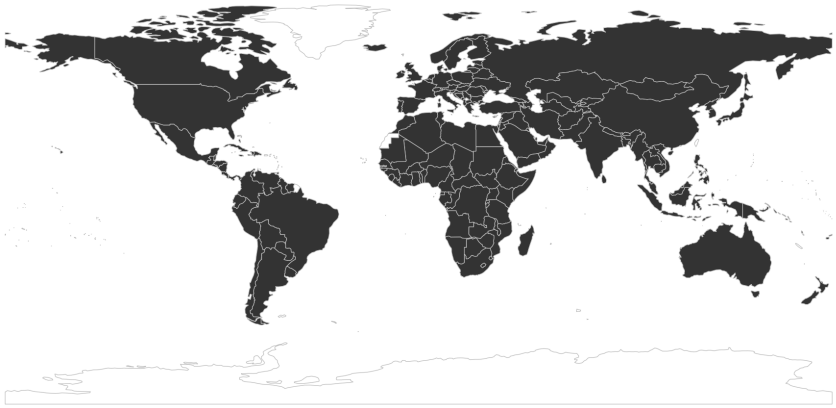
in basic cyberhygiene to protect their computers (e.g., password and software update) (Levin 2015). To some this importance of practicing cyberhygiene might seem minuscule, but studies after studies keep pointing to the importance of citizens safely browsing the Internet as the first line of defense against cyberattacks (Cain, Edwards and Still 2018; Levin 2015; Maennel, Mäses and Maennel 2018; Oravec 2017; Vishwanath et al. 2020). Adjustments in individual behavior however do not have the same effect for improving the state military defenses.

Because of these differences, estimating cybercapacity is a complicated process that will involve using a variety of indicators that lie inside and outside the government. I start with understanding how governments create their cybercapacity. While the amount of budget and personnel that they hire is not always public, I instead record information on various agencies that governments choose to create as the proxy for this capacity. Specifically, I collected the first of its kind, comprehensive data set on state cybersecurity organizations. The State Cybersecurity Organizations (SCO) data set contains information on 203 nations that developed more than 2,700 agencies within their governments to deal with different aspects of cybersecurity between 1987 until 2018. This data set distinguishes between civilian, intelligence, and military agencies and the type of change the government makes.[3] Figure 5.1 highlighted the countries that developed at least one civilian, military, or intelligence agency to deal with cybersecurity within their governments. Figure 5.1a shows that almost all nations in the world have a civilian agency that deal with opportunities and challenges presented by the Internet for economy, healthcare, transportation, education, etc. Figure 5.1b and 5.1c demonstrates that less countries devoted their attention to publicly developing their military or intelligence capability. Future research could explain why it is the case.

By mapping out the landscape of public cybercapabilities in the form of various governmental agencies, the SCO data set allows future generation of scholars not only to

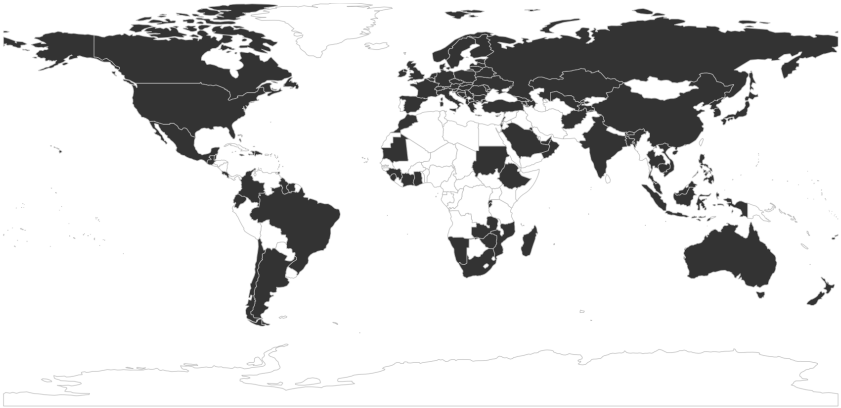
[3] Chapter 3 provides a more detailed explanation of this data.

Figure 5.1: *Diffusion of State Cybersecurity Organizations (1987-2018)*



(a) National Civilian Cybersecurity Organizations

(b) National Military Cybersecurity Organizations



(c) National Intelligence Cybersecurity Organizations

Source: State Cybersecurity Organizations (SCO) data. Countries highlighted on the map created at least of one state organization of a specified type between 1987 and 2018.

explain *why* it is the case but to investigate *how* countries develop their public capabilities, how these capabilities translate into actual operational capacity, and what implications it has for the dynamics of military effectiveness and innovation, cyberwarfare, deterrence, and escalation. The impact of ICTs and the Internet on our lives will continue to grow with the number of Internet-connected devices (known as the Internet-of-things), artificial intelligence, and quantum computing, we no longer can ignore it this undeveloped area of scientific inquire. Only a cumulative approach will allow us to fully understand how nations build their cybercapabilities—a complex, continuously evolving and expanding area of political science and public policy research that has significantly impacted how nations interact in the age of information technologies.

Works Cited

A/66/152, UNGA. 2011. A/66/152: Developments in the field of information and telecommunications in the context of international security. Technical report United Nations General Assembly.

A/66/359, UNGA. 2011. A/66/359: Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. Technical report United Nations General Assembly.

A/69/112/Add.1, UNGA. 2014. A/69/112/Add.1: Developments in the field of information and telecommunications in the context of international security. Technical report United Nations General Assembly.

A/72/315, UNGA. 2017. A/72/315: Developments in the field of information and telecommunications in the context of international security. Technical report United Nations General Assembly.

Al-Khatib, Talal. 2016. "30 Years of Cyber Attacks: An Ominous Evolution." *Seeker* .

Alperovitch, Dmitri. 2016. "Bears in the midst: Intrusion into the Democratic National Committee." *CrowdStrike Blog* 15.

Annual Cyber Security Assessment 2017 Estonian Information System Authority. 2017.

A/RES/52/199, UNGA. 1997. A/RES/52/199: Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes. Technical report United Nations General Assembly.

A/RES/53/70, UNGA. 1998. A/RES/53/70: Developments in the field of information and telecommunications in the context of international security. Technical report United Nations General Assembly.

A/RES/63/41, UNGA. 2010. A/RES/65/41: Developments in the field of information and telecommunications in the context of international security. Technical report United Nations General Assembly.

Assessing Russian activities and intentions in recent US elections. 2017. *Unclassified Version* .

Avant, Deborah. 2000. "From mercenary to citizen armies: Explaining change in the practice of war." *International Organization* 54(1):41–72.

Axelrod, Robert. 1997. "The dissemination of culture: A model with local convergence and global polarization." *Journal of conflict resolution* 41(2):203–226.

Axelrod, Robert and Rumen Iliev. 2014. "Timing of cyber conflict." *Proceedings of the National Academy of Sciences* 111(4):1298–1303.

Bailey, Michael A, Anton Strezhnev and Erik Voeten. 2017. "Estimating dynamic state preferences from United Nations voting data." *Journal of Conflict Resolution* 61(2):430–456.

Baliga, Sandeep, SOM Kellogg, Ethan Bueno de Mesquita and Alexander Wolitzky. 2018. Deterrence with imperfect attribution. Technical report mimeo, 2018. URL http://home. uchicago. edu/˜ bdm/PDF/deterrence. pdf.

Ball, M Margaret. 1951. "Bloc voting in the General Assembly." *International Organization* 5(1):3–31.

Baum, Matthew A. 2004. "How public opinion constrains the use of force: The case of Operation Restore Hope." *Presidential Studies Quarterly* 34(2):187–226.

Beck, Nathaniel, Jonathan N Katz and Richard Tucker. 1998. "Taking time seriously: Time-series-cross-section analysis with a binary dependent variable." *American Journal of Political Science* 42(4):1260–1288.

Beck, Nathaniel and Simon Jackman. 1998. "Beyond linearity by default: Generalized additive models." *American Journal of Political Science* 42:596–627.

Bennett, Colin J. 1991. "What is policy convergence and what causes it?" *British journal of political science* 21(2):215–233.

Benson, Brett V, Adam Meirowitz and Kristopher W Ramsay. 2014. "Inducing deterrence through moral hazard in alliance contracts." *Journal of Conflict Resolution* 58(2):307–335.

Benson, Brett V and Joshua D Clinton. 2016. "Assessing the variation of formal military alliances." *Journal of Conflict Resolution* 60:866–898.

Berinsky, Adam J. 2009. *In time of war: Understanding American public opinion from World War II to Iraq*. University of Chicago Press.

Berry, Frances Stokes and William D Berry. 1990. "State lottery adoptions as policy innovations: An event history analysis." *American political science review* 84(2):395–415.

Beuth, Patrick, Kai Biermann, Martin Klingst and Holger Stark. 2017. "Merkel and the Fancy Bear." *ZEIT Online* .

Bitzinger, Richard A. 1994. "The globalization of the arms industry: The next proliferation challenge." *International Security* 19(2):170–198.

Borghard, Erica D and Shawn W Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26(3):452–481.

Boulding, Kenneth E. 1962. "Conflict and defense: A general theory.".

Box-Steffensmeier, Janet M, Dan Reiter and Christopher Zorn. 2003. "Nonproportional hazards and event history analysis in international relations." *Journal of Conflict Resolution* 47(1):33–53.

Brantly, Aaron Franklin. 2016. *The Decision to Attack: Military and Intelligence Cyber Decision-making*. University of Georgia Press.

Brattberg, Erik and Tim Maurer. 2018*a*. "How Sweden is preparing for Russia to hack its election." *BBC News* .

Brattberg, Erik and Tim Maurer. 2018*b*. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Vol. 23 Carnegie Endowment for International Peace.

Brecher, Michael, Jonathan Wilkenfeld, Kyle Beardsley, Patrick James and David Quinn. 2016. "International crisis behavior data codebook, version 11." *URL: http://sites. duke. edu/icbdata/data-collections* .

Brecher, Michael, Jonathan Wilkenfeld et al. 1997. *A study of crisis*. University of Michigan Press.

Bremer, Stuart A. 1992. "Dangerous dyads: Conditions affecting the likelihood of interstate war, 1816-1965." *Journal of Conflict Resolution* 36(2):309–341.

Brooks, Risa. 2007. *Creating military power: The sources of military effectiveness*. Stanford University Press.

Brooks, Sarah M. 2005. "Interdependent and domestic foundations of policy change: The diffusion of pension privatization around the world." *International Studies Quarterly* 49(2):273–294.

Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.

Bueno de Mesquita, Ethan. 2007. "Politics and the suboptimal provision of counterterror." *International Organization* 61(01):9–36.

Cain, Ashley A, Morgan E Edwards and Jeremiah D Still. 2018. "An exploratory study of cyber hygiene behaviors and knowledge." *Journal of information security and applications* 42:36–45.

Cambodia ICT Master Plan. 2014. The Ministry of Communications.

Canetti, Daphna, Michael L Gross and Israel Waismel-Manor. 2016. "Immune from Cyberfire?" *Binary Bullets: The Ethics of Cyberwarfare* p. 157.

Cederberg, Gabriel. 2018. "Catching Swedish Phish: How Sweden is Protecting its 2018 Elections." *Defending Digital Democracy Project, Belfer Center for Science and International Security* .

Cerrotti, Rachel. 2017. "Sweden was among the best countries for immigrants. That's changing." *PRI* .

Clark, David D and Susan Landau. 2011. "Untangling attribution." *Harv. Nat'l Sec. J.* 2:323.

Coats, Daniel. 2018. "DNI Coats Statement.".

Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. 2011. Ministry of Defence of the Russian Federation, Moscow.

Cook, James. 2017. "The world's 10 biggest cybercrime hotspots in 2016, ranked." *Business Insider* pp. 1–2.

Cordell, Rebecca, K Chad Clay, Christopher J Fariss, Reed M Wood and Thorin M Wright. 2020. "Changing standards or political whim? Evaluating changes in the content of US State Department Human Rights Reports following presidential transitions." *Journal of Human Rights* 19(1):3–18.

Council, National Research et al. 2009. *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. National Academies Press.

Craig, Anthony. 2018. "The proliferation of cyber capabilities: an external threat model." *Draft* .

Craig, Anthony and Brandon Valeriano. 2016*a*. Conceptualising cyber arms races. In *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE pp. 141–158.

Craig, Anthony and Brandon Valeriano. 2016*b*. "Reacting to Cyber Threats: Protection and Security in the Digital Age." *Global Security and Intelligence Studies* 1(2):4.

Craig, Anthony and Brandon Valeriano. 2016*c*. "Securing Cyberspace: The Drivers of National Cyber Security Policy." *Presented at the International Studies Association Conference* .

Cunningham, Fiona. 2018. "Maximizing Leverage: Explaining China's Cyber Force Posture.".

Cyber Security Strategy for Defense. 2014. The Government of Belgium.

Cybersecurity Strategy for Energy. 2019. The Ministry of Climate, Energy and Building.

Cybersecurity Strategy for Health. 2019. The Ministry of Health.

Cybersecurity Strategy for Transportation. 2019. The Ministry of Transportation.

Danilovic, Vesna. 2001. "The sources of threat credibility in extended deterrence." *Journal of Conflict Resolution* 45(3):341–369.

Debs, Alexandre and Nuno P Monteiro. 2014. "Known unknowns: Power shifts, uncertainty, and war." *International Organization* 68(1):1–31.

Defence Guidelines for 2025 and Beyond. 2017. Directorate of Defence.

Deibert, Ronald. 2011. "Tracking the emerging arms race in cyberspace.".

Department of Defense Cyberspace Policy Report. 2011.

Diehl, Paul F. 1985. "Contiguity and military escalation in major power rivalries, 1816-1980." *The Journal of Politics* 47(4):1203–1211.

Digital Agenda. 2015. The Government of Albania.

Digital Agenda. 2016. The Government of Denmark.

Dragu, Tiberiu. 2011. "Is there a trade-off between security and liberty? Executive bias, privacy protections, and terrorism prevention." *American Political Science Review* 105(1):64–78.

Dragu, Tiberiu and Mattias Polborn. 2014. "The rule of law in the fight against terrorism." *American Journal of Political Science* 58(2):511–525.

Drezner, Daniel W. 2005. "Globalization, harmonization, and competition: the different pathways to policy convergence." *Journal of European Public Policy* 12(5):841–859.

Early, Bryan R. 2014. "Exploring the final frontier: An empirical analysis of global civil space proliferation." *International Studies Quarterly* 58(1):55–67.

E-Government Strategy. 2017. The Government of Albania.

Electronic Design Concept of Society. 2010. The Government of Albania.

Elkins, Zachary, Andrew T Guzman and Beth A Simmons. 2006. "Competing for capital: The diffusion of bilateral investment treaties, 1960–2000." *International organization* 60(4):811–846.

Eyestone, Robert. 1977. "Confusion, diffusion, and innovation." *American Political Science Review* 71(2):441–53.

Eyre, Dana P and Mark C Suchman. 1996. "Status, norms, and the proliferation of conventional weapons: An institutional theory approach." *The culture of national security: Norms and identity in world politics* pp. 79–113.

Faria, João Ricardo. 2006. "Terrorist innovations and anti-terrorist policies." *Terrorism and Political Violence* 18(1):47–56.

Farrell, Joseph and Robert Gibbons. 1989. "Cheap talk with two audiences." *The American Economic Review* 79(5):1214–1223.

Fearon, James. 2002. "Selection effects and deterrence." *International Interactions* 28(1):5–29.

Fearon, James D. 1995. "Rationalist explanations for war." *International organization* 49(3):379–414.

Fearon, James D. 2018. "Cooperation, conflict, and the costs of anarchy." *International Organization* 72(3):523–559.

Fearon, James Dana. 1992. *Threats to use force: costly signals and bargaining in international costs*. University of California, Berkeley.

Fernandino, Lisa. 2018. "Cybercom to Elevate to Combatant Command." *U.S. Department of Defense* .

Finnemore, Martha. 1996. "Norms, culture, and world politics: insights from sociology's institutionalism." *International organization* 50(2):325–347.

Fordham, Benjamin O and Victor Asal. 2007. "Billiard balls or snowflakes? Major power prestige and the international diffusion of institutions and practices." *International Studies Quarterly* 51(1):31–52.

France says no trace of Russian hacking Macron. 2017.

Fudenberg, Drew and Jean Tirole. 1991. "Game theory, 1991." *Cambridge, Massachusetts* 393(12):80.

Füglister, Katharina. 2012. "Where does learning take place? The role of intergovernmental cooperation in policy diffusion." *European Journal of Political Research* 51(3):316–349.

Fuhrmann, Matthew and Michael C Horowitz. 2017. "Droning on: Explaining the proliferation of unmanned aerial vehicles." *International organization* 71(2):397–418.

Galante, Laura and Shaun EE. 2018. *Defining Russian Election Interference: An analysis of select 2014 to 2018 cyber enabled incidents*. Atlantic Council.

Gartzke, Erik. 1998. "Kant we all just get along? Opportunity, willingness, and the origins of the democratic peace." *American Journal of Political Science* pp. 1–27.

Gartzke, Erik. 2013. "The myth of cyberwar: bringing war in cyberspace back down to Earth." *International Security* 38(2):41–73.

Gartzke, Erik and Alex Weisiger. 2013. "Fading friendships: Alliances, affinities and the activation of international identities." *British Journal of Political Science* 43(1):25–52.

Gartzke, Erik and Jon R Lindsay. 2015. "Weaving tangled webs: offense, defense, and deception in cyberspace." *Security Studies* 24(2):316–348.

Gartzke, Erik and Jon R Lindsay. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press.

Gelpi, Christopher, Jason Reifler and Peter Feaver. 2007. "Iraq the vote: Retrospective and prospective foreign policy judgments on candidate choice and casualty tolerance." *Political Behavior* 29(2):151–174.

George, Alexander L. 2019. Case studies and theory development: The method of structured, focused comparison. In *Alexander L. George: A pioneer in political and social sciences*. Springer pp. 191–214.

Gerden, Eugene. 2016. "Russia to spend 250 million US dollars strengthening cyber-offensive capabilities.".

Gibler, Douglas M. 2008. *International military alliances, 1648-2008*. CQ Press.

Gibler, Douglas and Toby Rider. 2004. "Prior commitments: Compatible interests versus capabilities in alliance behavior." *International Interactions* 30(4):309–329.

Gochman, Charles S and Zeev Maoz. 1984. "Militarized interstate disputes, 1816-1976: Procedures, patterns, and insights." *Journal of Conflict Resolution* 28(4):585–616.

Goertz, Gary and Paul F Diehl. 1993. "Enduring rivalries: Theoretical constructs and empirical patterns." *International studies quarterly* 37(2):147–171.

Gohdes, Anita R. 2014. "Pulling the Plug: Network Disruptions and Violence in Civil Conflict?".

Gohdes, Anita R. 2020. "Repression technology: Internet accessibility and state violence." *American Journal of Political Science* .

Goldman, Emily O. 2007. "International competition and military effectiveness: Naval air power, 1919–1945." *Creating Military Power: The Sources of Military Effectiveness* pp. 158–85.

Graham, Benjamin AT and Jacob R Tucker. 2019. "The international political economy data resource." *The Review of International Organizations* 14(1):149–161.

Grambsch, Patricia M and Terry M Therneau. 1994. "Proportional hazards tests and diagnostics based on weighted residuals." *Biometrika* 81(3):515–526.

Grant, Keith A. 2013. "Outsourcing security: Alliance portfolio size, capability, and reliability." *International Studies Quarterly* 57(2):418–429.

Greig, J Michael and Andrew J Enterline. 2017. "National Material Capabilities (NMC) Data Documentation, Version 5.0." *Correlates of War. Disponível em:< http://cow. dss. ucdavis. edu/data-sets/national-material-capabilities/nmc-codebook-v5-1>. Acesso em* 27.

Grissom, Adam. 2008. To Digitize an Army: The US Army Force XXI Initiative and the Digital Divide Controversy, 1993–2003 PhD thesis Doctoral Dissertation, KingâĂŹs College, London.

Gronke, Paul, Jeffrey Koch and J Matthew Wilson. 2003. "Follow the leader? Presidential approval, presidential support, and representatives' electoral fortunes." *The Journal of Politics* 65(3):785–808.

Gurr, Ted R, Monty G Marshall and Keith Jaggers. 2010. "Polity IV Project: Political Regime Characteristics and Transitions, 1800-2009." *Center for International Development and Conflict Management at the University of Maryland College Park* .

Haltiwanger, John. 2019. "Trump keeps criticizing NATO allies over spending. HereâĂŹs how NATO's budget actually works." *Business Insider* .

Hankewitz, Sten. 2018. "Mattis: Estonia, Denmark, the Netherlands will provide cyber contributions to help NATO." *Estonian World* .

Harrell Jr, Frank E, Kerry L Lee and Daniel B Mark. 1996. "Multivariable prognostic models: issues in developing models, evaluating assumptions and adequacy, and measuring and reducing errors." *Statistics in medicine* 15(4):361–387.

Hays, Scott P. 1996. "Patterns of reinvention: The nature of evolution during policy diffusion." *Policy Studies Journal* 24(4):551–566.

Hensel, Paul R. 1994. "One thing leads to another: Recurrent militarized disputes in Latin America, 1816-1986." *Journal of Peace Research* 31(3):281–297.

Hensel, Paul R et al. 2000. "Territory: Theory and evidence on geography and conflict." *What do we know about war* pp. 57–84.

Herpig, Sven. 2017. "Cyber Operations: Defending Political IT-Infrastructures.".

Hewitt, J Joseph. 2003. "Dyadic processes and international crises." *Journal of Conflict Resolution* 47(5):669–692.

Holsti, Ole R. 2004. *Public opinion and American foreign policy*. University of Michigan Press.

Horowitz, Michael C. 2010. *The diffusion of military power: Causes and consequences for international politics*. Princeton University Press.

Hoyt, Timothy D. 2007. "Social structure, ethnicity, and military effectiveness: Iraq, 1980–2004." *Creating Military Power. The Sorces of Military Effectiveness* pp. 55–79.

Huntley, Wayne. 2018. "Strategic Implications of Cyber Exploit Perishability and Obsolescence." *International Studies Association Meeting* .

Huth, Paul and Bruce Russett. 1988. "Deterrence failure and crisis escalation." *International Studies Quarterly* 32(1):29–45.

Huth, Paul K. 2009. *Standing your ground: Territorial disputes and international conflict*. University of Michigan Press.

Information and Communication Technologies Policy. 2003. The Ministry of Communications.

InternationalTelecommunicationsUnion. 2018. "Guide to Developing a National Cybersecurity Strategy." *International Telecommunication Union* .

Jackson, Matthew O and Massimo Morelli. 2009. "Strategic militarization, deterrence and wars." *Quarterly Journal of Political Science* 4(4):279–313.

Jarvis, Lee, Stuart Macdonald and Andrew Whiting. 2017. "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat." *European Journal of International Security* 2(1):64–87.

Jervis, Robert. 1976. *Perception and Misperception in International Politics*. Princeton, Princeton University Press.

Jo, Dong-Joon and Erik Gartzke. 2007. "Determinants of nuclear weapons proliferation." *Journal of Conflict Resolution* 51(1):167–194.

Johnson, Jeh. 2017. "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." *US Department of Homeland Security, January* 6.

Johnson, Simon and Catherine Evans. 2018. "Anti-immigration Sweden Democrats poll record high ahead of September election." *Reuters* .

Johnston, Alastair Iain. 1998. *Cultural realism: Strategic culture and grand strategy in Chinese history*. Vol. 178 Princeton University Press.

Joint Publication 3 13 Information Operations. 2014.

Katzenstein, Mary Fainsod. 1996. *The culture of national security: Norms and identity in world politics*. Columbia University Press.

Keele, Luke. 2010. "Proportionally difficult: testing for nonproportional hazards in Cox models." *Political Analysis* 18(2):189–205.

Kier, Elizabeth. 1995. "Culture and military doctrine: France between the wars." *International Security* 19(4):65–93.

Kier, Elizabeth. 1997. *Imagining war: French and British military doctrine between the wars*. Princeton University Press.

Klein, James P, Gary Goertz and Paul F Diehl. 2006. "The new rivalry dataset: Procedures and patterns." *Journal of Peace Research* 43(3):331–348.

Koopman, Cheryl, Eric Shiraev, Rose McDermott, Robert Jervis and Jack Snyder. 1998. "Beliefs about international security and change in 1992 among Russian and American national security elites." *Peace and Conflict* 4(1):35–57.

Kostyuk, Nadiya. 2019*a*. "Deterrence in the Cyber Realm: Public versus private cyber capability.".

Kostyuk, Nadiya. 2019*b*. "Online Appendix A: Interviews on Institutional Change as a Deterrent.".

Kostyuk, Nadiya. 2020*a*. Diffusion of Cybersecurity Policies.

Kostyuk, Nadiya. 2020*b*. "A Network Analysis of Diplomatic Exchanges on the Topic of Cybersecurity.".

Kostyuk, Nadiya and Carly Wayne. 2020. "Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats." *Journal of Global Security Studies* 0(0):1–25.

Kostyuk, Nadiya and Erik A. Gartzke. 2019. "Fighting in Cyberspace: Complementarity versus substitutability in cyber operations." *Presented at the International Studies Association Conference* .

Kostyuk, Nadiya and Yuri M. Zhukov. 2019. "Invisible Digital Front: Can cyber attacks shape battlefield events?" *Journal of Conflict Resolution* 63:317–347.

Kragh, Martin and Sebastian Åsberg. 2017. "Russia's strategy for influence through public diplomacy and active measures: the Swedish case." *Journal of Strategic Studies* 40(6):773–816.

Kreps, Sarah and Debak Das. 2017. "Warring from the virtual to the real: Assessing the public's threshold for war over cyber security." *Research & Politics* 4(2):2053168017715930.

Kunz, Barbara. 2015. "Sweden's NATO workaround: Swedish security and defense policy against the backdrop of Russian revisionism." *Enote. Focus Strateguque* .

Kydd, Andrew. 2000. "Arms races and arms control: Modeling the hawk perspective." *American Journal of Political Science* pp. 228–244.

Lai, Brian and Dan Reiter. 2000. "Democracy, political similarity, and international alliances, 1816-1992." *Journal of Conflict Resolution* 44(2):203–227.

Laudrain, Arthur P.B. 2019. "France's New Offensive Cyber Doctrine." *Lawfare* .

Leeds, Brett Ashley. 2003. "Do alliances deter aggression? The influence of military alliances on the initiation of militarized interstate disputes." *American Journal of Political Science* 47(3):427–439.

Leeds, Brett Ashley. 2005. "Alliance Treaty Obligations and Provisions Dataset." *Rice University (http://www. ruf. rice. edu/˜ leeds)* .

Leeds, Brett Ashley, Andrew G Long and Sara McLaughlin Mitchell. 2000. "Reevaluating alliance reliability: Specific threats, specific promises." *Journal of Conflict Resolution* 44(5):686–699.

Leeds, Brett, Jeffrey Ritter, Sara Mitchell and Andrew Long. 2002. "Alliance treaty obligations and provisions, 1815-1944." *International Interactions* 28(3):237–260.

Legro, Jeffrey W. 1996. "Culture and preferences in the international cooperation two-step." *American Political Science Review* 90(1):118–137.

Lemke, Douglas and William Reed. 2001. "War and rivalry among great powers." *American Journal of Political Science* pp. 457–469.

Levin, Adam. 2015. "Wetware: The Major Data Security Threat You've Never Heard Of." *Forbes Magazine* .

Lewis, James. 2018. *Economic Impact of Cybercrime, No Slowing Down*. McAfee.

Libicki, Martin C. 2007. *Conquest in cyberspace: national security and information warfare*. Cambridge University Press.

Libicki, Martin C. 2009. *Cyberdeterrence and cyberwar*. Rand Corporation.

Lijphart, Arend. 1963. "The analysis of bloc voting in the General Assembly: A critique and a proposal." *American Political Science Review* 57(4):902–917.

Lindsay, Jon R. 2013. "Stuxnet and the limits of cyber warfare." *Security Studies* 22(3):365–404.

Lindsay, Jon R and Erik Gartzke. 2015. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." *Typescript, University of California, San Diego* .

Lutscher, Philipp M, Nils B Weidmann, Margaret E Roberts, Mattijs Jonker, Alistair King and Alberto Dainotti. 2020. "At home and abroad: The use of denial-of-service attacks during elections in nondemocratic regimes." *Journal of Conflict Resolution* 64(2-3):373–401.

Maennel, Kaie, Sten Mäses and Olaf Maennel. 2018. Cyber Hygiene: The Big Picture. In *Nordic Conference on Secure IT Systems*. Springer pp. 291–305.

Maoz, Zeev. 2005. "Dyadic Militarized Interstate Disputes Dataset Version 2.0." *UC Davis)* .

Marinov, Nikolay, William G Nomikos and Josh Robbins. 2015. "Does electoral proximity affect security policy?" *The Journal of Politics* 77(3):762–773.

Matsubara, Mihoko. 2018. "How JapanâĂŹs Pacifist Constitution Shapes Its Approach to Cyberspace." *Council on Foreign Relations* .

Maurer, Tim. 2018. *Cyber Mercenaries: The state, hackers, and power*. Cambridge University Press.

McWhorter, Dan. 2013. "Mandiant Exposes APT1-One of ChinaâĂŹs Cyber Espionage Units & Releases 3,000 Indicators." *Mandiant, February* 18.

Meirowitz, Adam and Anne E Sartori. 2008. "Strategic uncertainty as a cause of war." *Quarterly Journal of Political Science* 3(4):327–352.

Meyer, John W and W Richard Scott. 1992. *Organizational environments: Ritual and rationality*. Sage Publications, Inc.

Moon, Bruce E. 1985. "Consensus or compliance? Foreign-policy change and external dependence." *International Organization* 39(2):297–329.

Morrow, James D. 1989*a*. "Capabilities, uncertainty, and resolve: A limited information model of crisis bargaining." *American Journal of Political Science* pp. 941–972.

Morrow, James D. 1989*b*. "A twist of truth: A reexamination of the effects of arms races on the occurrence of war." *Journal of Conflict Resolution* 33(3):500–529.

Morrow, James D. 1991. "Alliances and asymmetry: An alternative to the capability aggregation model of alliances." *American journal of political science* pp. 904–933.

Morrow, James D. 1994. "Alliances, credibility, and peacetime costs." *Journal of Conflict Resolution* 38(2):270–297.

Mueller, RS. 2019. "Report on the investigation into Russian interference in the 2016 presidential election." *US Department of Justice* .

Muggan, Robert, Gustavo Diniz and Misha Glenny. 2014. "Brazil doubles down on cyber security." *Open Democracy* .

National Cybersecurity Policy. 2017.

National Cybersecurity Strategy. 2016. Republic of Bulgaria.

National Cybersecurity Strategy III. 2018. The Government of Luxembourg.

National Defence Development Plan 2017-2026. 2017.

Newman, Lily Hay. 2019. "What Israel's strike on Hamas hackers means for cyberwar.".

Nimmo, Ben. 2017. "The KremlinâĂŹs Amplifiers in Germany." *Digital Forensic Research Lab* .

Nye Jr, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41(3):44–71.

Obama, Barack. 2013. "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity.".

O'Dwyer, Gerard. 2018. "Sweden steps up cyber defence measures.".

Olson, Mancur and Richard Zeckhauser. 1966. "An economic theory of alliances." *The review of economics and statistics* pp. 266–279.

Oravec, Jo Ann. 2017. Emerging "cyber hygiene" practices for the Internet of Things (IoT): professional issues in consulting clients and educating users on IoT privacy and security. In *2017 IEEE International Professional Communication Conference (ProComm)*. IEEE pp. 1–5.

Osho, Oluwafemi and Agada D Onoja. 2015. "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis." *International Journal of Cyber Criminology* 9(1).

Palmer, Glenn. 1990. "Corralling the free rider: deterrence and the western alliance." *International Studies Quarterly* 34(2):147–164.

Pennings, Johannes M and Farid Harianto. 1992. "The diffusion of technological innovation in the commercial banking industry." *Strategic management journal* 13(1):29–46.

Pevehouse, Jon CW, Timothy Nordstrom, Roseanne W McManus and Anne Spencer Jamison. 2019. "Tracking organizations in the world: The Correlates of War IGO Version 3.0 datasets." *Journal of Peace Research* p. 0022343319881175.

Plümper, Thomas and Eric Neumayer. 2015. "Free-riding in alliances: Testing an old theory with a new method." *Conflict Management and Peace Science* 32(3):247–268.

Posen, Barry. 1984. *The sources of military doctrine: France, Britain, and Germany between the world wars*. Cornell University Press.

Powell, Robert. 1993. "Guns, butter, and anarchy." *American Political Science Review* 87(1):115–132.

Powell, Robert. 2006. "War as a commitment problem." *International organization* 60(1):169–203.

Powell, Walter W and Paul J DiMaggio. 1991. *The new institutionalism in organizational analysis*. University of Chicago Press.

Presidential Policy Directive/PPD-21. 2013.

Press, Daryl Grayson. 2005. *Calculating credibility: How leaders assess military threats*. Cornell University Press.

Public Elements of the Doctrine on Military Cyber Offensive. 2019.

Putin's Assymetric Assault on Democracy in Russia and Europe. 2018.

Ramirez, Francisco O and John Boli. 1987. "Global patterns of educational institutionalization." *Institutional structure: Constituting state, society, and the individual* .

Reiter, Dan. 2003. "Exploring the bargaining model of war." *Perspectives on Politics* 1(1):27–43.

Reiter, Dan and Allan C Stam. 2002. *Democracies at war*. Princeton University Press.

Relations with Sweden. 2018.

Rettman, Andrew and Lisbeth Kirk. 2018. "Sweden raises alarm on election meddling." *EU Observer* .

Reuters. 2017. "Russia sets up information warfare units - defence minister." *Reuters* .

Rid, Thomas. 2013. *Cyber war will not take place*. Oxford University Press.

Rid, Thomas and Ben Buchanan. 2015. "Attributing cyber attacks." *Journal of Strategic Studies* 38(1-2):4–37.

Riley, Michael and Jordan Robertson. 2017. "Russian cyber hacks on US electoral system far wider than previously known." *Bloomberg* 13.

Roberts, Margaret E. 2018. *Censored: distraction and diversion inside China's Great Firewall*. Princeton University Press.

Robertson, Maxine, Jacky Swan and Sue Newell. 1996. "The role of networks in the diffusion of technological innovation." *Journal of management studies* 33(3):333–359.

Rød, Espen Geelmuyden and Nils B Weidmann. 2015. "Empowering activists or autocrats? The Internet in authoritarian regimes." *Journal of Peace Research* 52(3):338–351.

Roden, Lee. 2017. "Sweden's government wants newspapers to pay less tax in an effort to combat fake news." *The Local* .

Roeder, Ollie. 2018. "Why We're Sharing 3 Million Russian Troll Tweets.".

Rogers, Everett M. 1995. *The Diffusion of Innovations*. 3rd edition ed. New York: Free Press.

Rosen, Stephen Peter. 1996. *Societies and military power: India and its armies*. Cornell University Press.

Ruppert, David, Matt P Wand and Raymond J Carroll. 2003. *Semiparametric regression*. Number 12 New York: Cambridge University Press.

Russett, Bruce M. 1966. "Discovering voting groups in the United Nations." *American Political Science Review* 60(2):327–339.

Russia Concerned by Efforts to Draw Finland, Sweden Into NATO - Defense Minister. 2018.

Ryabikova, Victoria. 2019. "How Russia protects critical infrastructure from cyber attacks." *Russia Beyond* .

Sabillon, Regner, Victor Cavaller and Jeimy Cano. 2016. "National cyber security strategies: global trends in cyberspace." *International Journal of Computer Science and Software Engineering* 5(5):67.

Sagan, Scott D. 1997. "Why do states build nuclear weapons? Three models in search of a bomb." *International security* 21(3):54–86.

Sandler, Todd. 1993. "The economic theory of alliances: a survey." *Journal of conflict resolution* 37(3):446–483.

Sapronas, Robertas. 1999. "BALTBAT and development of Baltic Defence Forces." *Baltic Defence Review* 2(2):55–70.

Schelling, Thomas C. 2008. *Arms and influence: With a new preface and afterword*.

Schneider, Jacquelyn. 2019. Cyber and Cross Domain Deterrence: Deterring Within and From Cyberspace. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Jon R. Lindsay and Erik Gartzke. Oxford University Press chapter 5.

Schulze, Matthias and Sven Herpig. 2018. "Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them." *Council on Foreign Relations* .

Schweller, Randall L. 1994. "Bandwagoning for profit: Bringing the revisionist state back in." *International Security* 19(1):72–107.

Schwirtz, Michael. 2017. "German Election Mystery: Why No Russian Meddling?" *New York Times* .

Sechser, Todd S and Elizabeth N Saunders. 2010. "The army you have: the determinants of military mechanization, 1979–2001." *International Studies Quarterly* 54(2):481–511.

Selznick, Philip. 1949. *TVA and the grass roots: A study in the sociology of formal organization*. Vol. 3 Univ of California Press.

Senese, Paul D. 2005. "Territory, contiguity, and international conflict: Assessing a new joint explanation." *American Journal of Political Science* 49(4):769–779.

Shadden, Mark and Christopher Zorn. 2011. Data transformations for social science research: Theory and best practices. In *In annual meeting of Society for Political Methodology, Princeton, NJ, June*. pp. 28–30.

Signorino, Curtis S and Jeffrey M Ritter. 1999. "Tau-b or not tau-b: Measuring the similarity of foreign policy positions." *International Studies Quarterly* 43(1):115–144.

Simmons, Beth A, Paulette Lloyd and Brandon M Stewart. 2018. "The global diffusion of law: Transnational crime and the case of human trafficking." *International organization* 72(2):249–281.

Simmons, Beth A and Zachary Elkins. 2004. "The globalization of liberalization: Policy diffusion in the international political economy." *American political science review* 98(1):171–189.

Singer, Peter W and Allan Friedman. 2014. *Cybersecurity: What Everyone Needs to Know*. Oxford University Press.

Slantchev, Branislav L. 2005. "Military coercion in interstate crises." *American Political Science Review* 99(4):533–547.

Smith, Aaron. 2018. "Attitudes about cybersecurity policy.".

Smith, Alastair. 1995. "Alliance formation and war." *International Studies Quarterly* 39(4):405–425.

Snyder, Glenn H. 1984*a*. "The security dilemma in alliance politics." *World politics* 36(4):461–495.

Snyder, Jack L. 1984*b*. "The ideology of the offensive: military decision making and the disasters of 1914/Jack Snyder.".

Soldatov, Andrei and Irina Borogan. 2017. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. Public Affairs.

Stephen, Walt. 1987. "The Origins of Alliances." *Ithaca New York* 1:87.

Stinnett, Douglas M, Jaroslav Tir, Paul F Diehl, Philip Schafer and Charles Gochman. 2002. "The correlates of war (cow) project direct contiguity data, version 3.0." *Conflict Management and Peace Science* 19(2):59–67.

Stinnett, Douglas M and Paul F Diehl. 2001. "The path (s) to rivalry: Behavioral and structural explanations of rivalry development." *The Journal of Politics* 63(3):717–740.

Stone, Diane. 2004. "Transfer agents and global networks in the 'transnationalization' of policy." *Journal of European public policy* 11(3):545–566.

Strategy for Operating in Cyberspace. 2011.

Suchman, Mark C and Dana P Eyre. 1992. Military procurement as rational myth: Notes on the social construction of weapons proliferation. In *Sociological Forum*. Vol. 7 Springer pp. 137–161.

SverigesRadio. 2017. "Swedish PM warns of foreign influence ahead of 2018 poll." *Radio Sweden* .

Sweden's Defense Policy: 2016 to 2020. 2015.

Sweeney, Kevin and Paul Fritz. 2004. "Jumping on the bandwagon: An interest-based explanation for great power alliances." *The Journal of Politics* 66(2):428–449.

Tetlock, Philip E. 2017. *Expert Political Judgment: How Good Is It? How Can We Know?-New Edition*. Princeton University Press.

The DOD Cyber Strategy. 2015. The U.S. Department of Defense.

Therneau, Terry, Cynthia Crowson and Elizabeth Atkinson. 2020. "Multi-state models and competing risks." *CRAN-R (https://cran. r-project. org/web/packages/survival/vignettes/compete. pdf)* .

Therneau, Terry M and Patricia M Grambsch. 2000. The Cox model. In *Modeling survival data: extending the Cox model*. New York: Springer-Verlag.

Therneau, Terry M, Patricia M Grambsch and Thomas R Fleming. 1990. "Martingale-based residuals for survival models." *Biometrika* 77(1):147–160.

Tor, Uri. 2017. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40(1-2):92–117.

U.S. Cyber Strategy. 2015.

U.S.DepartmentOfDefense. 2016. "Consolidated DoD FY17 Budget Fact Sheet." https://dod.defense.gov/Portals/1/features/2016/0216_budget/docs/2-4-16_Consolidated_DoD_FY17_Budget_Fact_Sheet.pdf. Accessed: 2019-07-13.

USDepartmentOfJustice. 2014. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.".

USDepartmentOfJustice. 2016. "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector.".

USDepartmentOfJustice. 2018*a*. "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election.".

USDepartmentOfJustice. 2018*b*. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.".

USDepartmentOfJustice. 2018*c*. "United States of America v. Internet Research Agency LLC et al.".

US DoD Active Defense. 2019. https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=37. Accessed: 2019-07-13.

U.S. National Cyber Strategy. 2018.

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

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

Van Buuren, Stef. 2018. *Flexible imputation of missing data*. CRC press.

Vanderburg, Eric. 2017. "Ransomware developers learn from the mistakes of WannaCry, NotPetya." *Carbonite* .

Vasquez, John A. 1995. "Why do neighbors fight? Proximity, interaction, or territoriality." *Journal of Peace Research* 32(3):277–293.

Vasquez, John A. 2001. "Mapping the probability of war and analyzing the possibility of peace: The role of territorial disputes." *Conflict Management and Peace Science* 18(2):145–173.

Vasquez, John A. 2009. *The war puzzle revisited*. Vol. 110 Cambridge University Press.

Vavra, Shannon. 2017. "The world's top cyber powers." *Axios* .

Vishwanath, Arun, Loo Seng Neo, Pamela Goh, Seyoung Lee, Majeed Khader, Gabriel Ong and Jeffery Chin. 2020. "Cyber hygiene: The concept, its measure, and its initial tests." *Decision Support Systems* 128:113160.

Voeten, Erik. 2005. "The political origins of the UN Security Council's ability to legitimize the use of force." *International Organization* 59(3):527–557.

Voeten, Erik, Anton Strezhnev and Michael Bailey. 2017. "United Nations General Assembly Voting Data.".
URL: *http://hdl.handle.net/1902.1/12379*

Volden, Craig. 2006. "States as policy laboratories: Emulating success in the children's health insurance program." *American Journal of Political Science* 50(2):294–312.

Walt, Stephen M. 1997. "Why alliances endure or collapse." *Survival* 39(1):156–179.

Ward, Hugh and Xun Cao. 2012. "Domestic and international influences on green taxation." *Comparative Political Studies* 45(9):1075–1103.

Weede, Erich. 1983. "Extended deterrence by superpower alliance." *Journal of Conflict Resolution* 27(2):231–253.

Weidmann, Nils B. 2016. "A closer look at reporting bias in conflict event data." *American Journal of Political Science* 60(1):206–218.

Weidmann, Nils B and Espen Geelmuyden Rød. 2019. *The Internet and political protest in autocracies*. Oxford Studies in Digital Poli.

Yuen, Amy. 2009. "Target concessions in the shadow of intervention." *Journal of Conflict Resolution* 53(5):745–773.

Zagare, Frank C and D Marc Kilgour. 2003. "Alignment patterns, crisis bargaining, and extended deterrence: A game-theoretic analysis." *International Studies Quarterly* 47(4):587–615.

Zimmerman, William. 2009. *The Russian people and foreign policy: Russian elite and mass perspectives, 1993-2000*. Princeton University Press.

Zisk, Kimberly Marten. 1993. *Engaging the enemy: Organization theory and Soviet military innovation, 1955-1991*. Princeton University Press.