The Mice that Roar:
What Small Countries Can Teach Great Powers About National Cyber-Defense

By

Melissa Kate Griffith

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Political Science

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Vinod K. Aggarwal, Chair
Professor Ron Hassner
Professor Steven Weber

Summer 2020

The Mice that Roar:
What Small Countries Can Teach Great Powers About National Cyber-Defense

Abstract

The Mice that Roar:
What Small Countries Can Teach Great Powers About National Cyber-Defense

By

Melissa Kate Griffith

Doctor of Philosophy in Political Science

University of California, Berkeley

Professor Vinod K. Aggarwal, Chair

What factors affect the organization and efficacy of national cyber-defense efforts? In *The Mice that Roar*[1]*: What Small Countries Can Teach Great Powers About National Cyber-Defense,* I argue that an important piece of the answer lies within the history and institutions of an often-overlooked yet significant sub-group of countries. Given that effective defense in cyberspace requires extensive civilian-military and public-private cooperation and coordination (a societal defense posture), American policymakers and academics alike frequently characterized national defense efforts in cyberspace as a significant departure from pre-existing kinetic national defense efforts in the domains of air, land, and sea. Notably, however, how states' experience this disjuncture varies. In the case of the Mice that Roar, their pre-existing national defense approaches more closely resemble the desired solution set to national defense in cyberspace (Whole of Society) than the pre-existing approaches found in far larger powers like the United States (U.S.) or the United Kingdom (U.K.). Importantly, these architectures exist, in large part, precisely because these states are *not* historically strong and resource-rich. Crucially, the historical defense problem these states faced due to deep vulnerability born from their relative size and geopolitical position has key conceptual and operational similarities with the problem of critical interconnectedness (their dependence on and the interconnectivity of cyberspace) now facing all advanced industrial states in the cyber era. In other words, by solving for significant vulnerability, these states also solved, in part, for critical interconnectedness.

By focusing specifically on how a subset of relatively small yet successful states, the Mice that Roar, have pursued national cyber-defense, the dissertation's argument and findings challenge two prevailing assumptions in security studies and cyber conflict scholarship: (1) that larger states with more resources will be better positioned to provide national defense for their populations and (2) that national cyber-defense, as a central task of states, represents a significant departure from the core requirements of national defense in the domains of air, land, and sea (i.e. that it represents a new type of defense problem for states to address).

In addition, my work promises to augment the study of cyber conflict in political science and contribute to policy discussions in two important ways. First, through a focus on often understudied

[1] This title was fondly inspired by the 1955 novel, "The Mouse that Roared", and the 1959 film by the same name.

countries in international security studies and cyber conflict studies, this dissertation takes an important step in the ongoing process of delineating systemic dynamics from situational dynamics in cyberspace: i.e. dynamics all states face due to the threat space versus dynamics that are significantly mediated through national contexts and circumstances. Second, this project illustrates that in our efforts to understand cybersecurity in the context of national security and pursue policy solutions, previously overlooked insights for the organization and efficacy of national cyber-defense efforts lay outside the more heavily studied histories of states such as the U.S.

This dissertation is dedicated to my family, without whom this project would never have been imaginable let alone possible.

And to the makers of fountain pens and inks, which I relied on to fill the stacks of notebooks within which this dissertation first took shape.

Table of Contents

List of Abbreviations

5G:	Fifth generation of telecommunications networks
AI:	Artificial Intelligence
AFDA:	Association of Finnish Defense and Aerospace Industries
APT:	Advanced Persistent Threat
CCDOE:	Cooperative Cyber Defense Centre of Excellence (NATO)
CERT:	Computer Emergency Response Team
CERT-EE:	Estonia's Computer Emergency Response Team
CERT-FI:	Finland's Computer Emergency Response Team (FICORA)
CERT-IL:	Israel National Cyber Event Readiness Team
CIA:	Central Intelligence Agency (U.S.)
CIIP:	Critical Information Infrastructure Protection (Estonia)
CISA:	Cybersecurity and Infrastructure Security Agency (U.S.)
CMF:	Cyber Mission Force (CMF) teams (USCYBERCOM)
CNIC:	Comprehensive National Cybersecurity Initiative (U.S.)
CNMF-HQ:	Cyber National Mission Force Headquarters (USCYBERCOM)
CSIRT:	Computer Security Incident Response Team
CSA:	Cyber Security Agency (Singapore)
CySP:	Cyber Scholarship Program (U.S.)
DARPA:	Defense Advanced Research Projects Agency (U.S.)
DDI:	Directorate of Digital Innovation (U.S.)
DDoS attacks:	Distributed Denial of Service attacks
DHS:	Department of Homeland Security (U.S.)
DoD:	Department of Defense (U.S.)
ERA:	Engineering Research Associates (U.S.)
EU:	European Union
FBI:	Federal Bureau of Investigation (U.S.)
FICORA:	Finnish Communications Regulatory Authority
FISC:	Finnish Information Security Cluster
Galileo:	Europe's Global Navigation Satellite System (acronym GNSS)
GAO:	General Accountability Office (U.S.)
GDP:	Gross Domestic Product
GLCs:	Government-Linked Companies (Singapore)
GLONAS:	Russia's Global Navigation Satellite System
GNSS:	Global Navigation Satellite System
GPS:	the U.S.'s Global Positioning System
IAF:	Israeli Air Force (IDF)
ICT:	Information and Communications Technology
I-CORE:	Israeli Centres of Research Excellence
IDA:	Info-communications Development Authority (Singapore)
IDF:	Israeli Defense Forces (Tzahal)
ILITA:	Israeli Law, Information, and Technology Authority (Ramot)
INCB:	Israel National Cyber Bureau
INCD:	Israel National Cyber Directorate
IoT:	Internet of Things
ISKE:	IT Baseline Security System (Estonia)

ISMP:	Infocomm Security Masterplan (Singapore)
IT:	Information Technology
ITU:	International Telecommunications Union (United Nations)
MAD:	Mutually Assured Destruction
MHA:	Ministry of Home Affairs (Singapore)
MoD:	Ministry of Defense (Estonia, Finland, Israel, Singapore)
NATO:	North Atlantic Treaty Organization
NCAP:	National Cybercrime Action Plan (Singapore)
NCSA:	National Cyber Security Authority (Israel)
NCSC:	National Cyber Security Centre (Singapore)
NCSC-FI:	National Cyber Security Centre (Finland)
NDS:	National Defence Strategy (Estonia)
NESA:	National Emergency Supply Agency (Finland)
NICE:	National Initiative for Cybersecurity Education (U.S.)
NIS:	EU Network and Information Systems Security Directive
NIST:	National Institute of Standards and Technology (U.S.)
NPPD:	National Protection and Programs Directorate (U.S.)
NSA:	National Security Agency (U.S.)
NSC:	National Security Concept (Estonia)
OCS:	Office of the Chief Scientist (Israel)
OhCR:	Ohio Cyber Reserve (U.S.)
OSCE:	Organization for Security and Co-operation in Europe
PAP"	People's Action Party (Singapore)
PE:	Persistent Engagement (U.S)
PPP:	Public Private Partnerships
R&D:	Research and Development
RE'EM:	Information Security Authority (Israel)
RIA:	Estonian Information System Authority
SAF:	Singapore Armed Forces
Shen Bet:	Israel Security Agency (acronym Shabak)
SITSA:	Technology Security Authority (Singapore)
U.K.:	United Kingdom of Great Britain and Northern Ireland
U.S.:	United States of America
USCYBERCOM:	United States Cyber Command
VC:	Venture Capital

Acknowledgements

This work would not have been possible without the support of mentors, colleagues, family, and friends. I am deeply indebted to the many individuals who made the time to discuss, debate, support, and enliven this project in seminar rooms, offices, conferences, workshops, cafés, and restaurants around the world as I jumped between numerous countries and cities in order to complete this project. There are far too many individuals and organizations that have shaped this dissertation and my tenure at Berkeley to make naming them all here remotely feasible, but I am thankful to each and every one of you all the same.

I am immeasurably grateful to my family: to my mother and my father, Sara and Stan Griffith, and to my brothers, Adam and Brian Griffith, for their love and support. Without you this dissertation would never have been imaginable let alone possible. Thank you.

I am indebted to the mentorship, support, and intellectual and professional opportunities I received from my committee: Professors Vinod K. Aggarwal, Ron Hassner, and Steven Weber. In completing this dissertation, I was very fortunate to have a committee with such varied and complimentary expertise and interests. First, no dissertation would be possible without the support of a chair. Particular thanks, therefore, go to Professor Vinod K. Aggarwal for serving as my dissertation chair and for bringing international political economy and industrial policy expertise into the cybersecurity conversation. Second, I am thankful for the role that Professor Ron Hassner has played in shaping this dissertation. His expertise in international and national security as well as his own experience working in a then nascent field of study as a graduate student (the intersection of religion and security) were invaluable. Third, this project, both in terms of its inception and the final product, greatly benefited from the cybersecurity expertise and passion of Professor Steven Weber, the Faculty Director for the Center for Long-Term Cybersecurity (CLTC). Notably, it was in his graduate seminar on international relations theory that I first became interested in the political and security ramifications of emerging technologies. Finally, and unluckily, the last year of my PhD brought with it its own unique set of circumstances. Finishing a dissertation is challenging during the best of times. Completing a dissertation in the midst of a global pandemic, however, is even more so. I deeply appreciate my committee's dedication during what was a uniquely disruptive and arduous time for us all.

In addition to the support of my committee, I have benefited enormously from the communities of scholarship I have found at the University of California, Berkeley: the Berkeley Roundtable on the International Economy (BRIE); the international relations scholars and students of the MIRTH colloquium; the UC Berkeley Social Science Matrix, the Berkeley Asia Pacific Economic Cooperation Study Center (BASC), the Berkeley Center for Law & Technology (BCLT), and the researchers and staff at the Center for Long-Term Cybersecurity (CLTC). I am particularly grateful to the amazing faculty I have had the opportunity to work with during my tenure at Berkeley in addition to my committee; and especially to Ruth Collier, Laura Stoker, John Zysman, and my first-year advisor and the person who expertly shepherded me through the prospectus process, Michaela Mattes. I would be remiss if I did not also acknowledge the hard work and dedication of the administration and staff whose expertise kept the Political Science department running smoothly; special thanks to Stephanie Alcid, Erin Blanton, Efrat Cidon, Charlotte Merriwether, and Susan Nunes. Finally, I am very grateful to my fellow graduate students from whom I have received support, feedback, encouragement, and advice: Rachel Bernhard, Caroline Brandt, Melissa Carlson,

Brad Kent, Adam Lichtenheld, Andrew Reddie, Fiona Shen-Bayh, Matthew Stenberg, Rochelle Terman, Sherry Zaks, and many more. Special thanks to Nina Kelsey, Deirdre Martin, Alice Ciciora, Ben Bartlett, Jason Klocek, Rachel Strohm, and Tanu Kumar whose friendship, kindness, humor, and conversation formed the bedrock of my Berkeley experience.

I have also greatly benefited from the communities of scholarship I have found beyond Berkeley: the Cyber Conflict Studies Association (CCSA) where I found a home amongst a vibrant community of cybersecurity experts within academia, industry, and policy; Bridging the Gap's New Era Workshop, which expanded my horizons and reinvigorated my desire to pursue a research agenda that seeks to advance political science and international relations scholarship while also addressing pressing policy and national security challenges; the Research Institute on the Finnish Economy (ETLA), which hosted me over the course of the 10+ months that I spent in Helsinki, Finland; the *Université Libre de Bruxelles* (ULB) and George Washington University's Institute for International Science & Technology Policy (IISTP) where I was a visiting researcher and scholar respectively; the Woodrow Wilson International Center for Scholars where I served as a Public Policy Fellow with the Science and Technology Innovation Program (STIP); and Stanford University's Center for International Security and Cooperation (CISAC) where I was a pre-doctoral cybersecurity fellow in the final months of my doctorate.

I also wish to acknowledge the mentorship, friendship, and inspiration I received from the cyber conflict and cybersecurity community. While there are far too many people to name here, I am deeply honored to have had the opportunity to work alongside such talented scholars and practitioners. Special thanks go to Ben Buchanan, Chris Demchak, Richard Harknett, Jason Healey, Trey Herr, Christopher Hockings, Jackie Kerr, Meg King, Herb Lin, Torey McMurdo, Adam Segal, James Shires, Max Smeets, Michael Warner, Steven Weber, JD Work, and Amy Zegart. Thank you for all the workshops, conferences, working dinners, chats over coffee, and brainstorming sessions. I am deeply grateful that this community embraced and fostered my desire to study the national security implications of cyberspace - a nascent but now rapidly developing sub-field of study – at a time when few political scientists were doing so and even fewer graduate students had the opportunity. This project would not have been possible without your support.

Furthermore, the interview and archival data collection efforts as well as the subsequent writing and revision process would never have been financially possible without generous support from the University of California, Berkeley; the *Université Libre de Bruxelles (ULB)*; the Center for Long-Term Cybersecurity (CLTC); the Research Institute on the Finnish Economy (ETLA); the Woodrow Wilson International Center for Scholars; and the Center for International Security and Cooperation (CISAC).

Finally, this dissertation relied on the hospitality and expertise of numerous individuals sitting within academia, government, armed forces, international organizations, and industry in countries spanning four continents. I owe a particular debt to each and every individual I interviewed. Thank you for your time and for sharing your experiences, expertise, and insights with me. Without you this dissertation would quite simply not exist.

PART I

The National Cyber-Defense Problem

Chapter 1
Introduction

"…no issue has emerged so rapidly in importance as cybersecurity.
And yet there is no issue so poorly understood…"
– P. W. Singer[2]

1. Two Motivating Puzzles

Our conventional understanding of national security leads us to reasonably expect that the largest, most powerful military actors will also be the best positioned to provide national defense. Yet, as the medium of global conflict expands to encompass digital weapons alongside conventional ones, a surprising set of actors emerge among the leaders in national defense in an era of cyber conflict.[3] States such as Estonia, Finland, Israel, and Singapore rank among the most secure and comprehensive in their capability to provide national cyber-defense for their populations. How have these relatively small countries, with comparatively limited resources, become significant providers of national cyber-defense ranking alongside far larger regional and global powers like the United States (U.S.)? Why and how have these Mice Roared?

This development is particularly puzzling for political scientists and security scholars alike as it represents a departure from traditionally dominant national defense players. The field's prevailing logic assumes that larger states with more resources will be better positioned to provide national defense for their populations.[4] Small states, in contrast, lack the resources to out-compete larger powers through domestic capacity alone and must rely on larger states' power to protect their populations. This view of defense capability is consistent with the literature on small states outside of the cybersecurity space. Given their unique vulnerability and their inability to apply power to or resist the application of power by larger states, one common option is to augment that power through alliances or relationships with larger powers. They bandwagon or balance.[5] But they lack the resources to provide security for their populations without leveraging the resources of other states in their defense.

Significantly, state size is an important variable within international relations theory because dominant state power models frequently describe power using material measures such as geographic,

2 Peter W. Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know*, Kindle Edition, (*Oxford University Press,* 2014).

3 This observation specifically reflects states' cyber-defense capabilities. I am not arguing, nor would it make sense to do so, that kinetic defense capabilities in air, land, and sea have become irrelevant in the era of cyber conflict or that having strong cyber-defense capabilities in some general sense outweigh kinetic weaknesses. This dissertation instead focuses specially on one domain of conflict, which is only growing in importance. Notably, cyber-defense is both (i) a necessary component of armed conflict given states reliance on cyberspace both for the daily functioning of society and states' militaries and governments and (ii) a domain of conflict where competition/conflict also occurs below the threshold of war within a state's territory or homebase (i.e. the gray-zone). The dynamics of cyber conflict are discussed in greater detail later in Chapter One and in Chapter Two, including the limitations of traditional, kinetic military means for achieving cyber-defense outcomes.

4 "If preponderance is key to capability, then security will be a function of the local balance of power; preponderant states will be secure, but smaller ones vulnerable". Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*, Kindle Edition (Princeton University Press, 2010). loc. 185.

5 Stephen M. Walt, *The Origins of Alliances*, Kindle Edition (Cornell University Press, 2013) provides the foundational exploration of these dynamics. Peter Viggo Jakobsen, "Small States, Big Influence: The Overlooked Nordic Influence on the Civilian ESDP*," *JCMS: Journal of Common Market Studies* 47, no. 1 (January 1, 2009): 81–102, highlights how Nordic states were able to magnify their influence through the European Security and Defence Policy (ESDP) despite opposition from other regional powers such as France. Also, worth mentioning is the small literature on neutrality, which puts forth a third option outside of bandwagoning and balancing. Begin with Pertti Joenniem, "Neutrality beyond the Cold War," *Review of International Studies* 19, no. 3 (1993): 289–304 for a discussion of neutrality outside of the World Wars and Cold War periods.

population, economic, or military size as proxies for power and state security capabilities. In this regard, the U.S., with its corresponding military and economic might, is universally coded as a current large power (and historically, a hegemon). In contrast, Estonia - about twice the size of New Jersey, 157th globally in terms of population size,[6] and sitting directly next to a far larger Russia - is relatively quite small. As a consequence, this theoretical orthodoxy would predict that Estonia would find itself far more poorly positioned to defend its population than the far larger U.S. given its far more limited resources. It would not predict that Estonia would be similarly positioned if not better positioned.

Yet, this logic, and the nascent cyber conflict field's dominate focus on large states,[7] remains fundamentally at odds with observable outcomes in cyber-defense. Several relatively small states have historically outpaced and/or continue to rival larger states in their cybersecurity readiness. While metrics are limited and not uniform in their methodology or scope, relatively small states have repeatedly been identified among the leaders.[8] In 2012, the Brussels-based think tank Security and Defense Agenda released an index of state's cybersecurity preparedness levels. Three nations topped that list: Finland, Israel, and Sweden. Estonia ranked alongside the U.S. a tier down.[9] In 2013, the Cyber Readiness Index (CRI) 1.0 revealed a similar mix of small and large countries earning higher scores, including Australia, Finland, Japan, the Netherlands, Norway, the U.K., and the U.S.[10] In 2017, Finland was acknowledged as the most cyber secure country in the EU (with a focus on vulnerability to cybercrime), beating Estonia for the top spot.[11] Germany, the Netherlands, and the U.K. rounded out the remainder of the top five. In the United Nations' (UN) International Telecommunication Union (ITU) 2017 Global Cybersecurity Index (GCI), a host of relatively small countries topped the rankings alongside the far larger U.S. This top tier of countries – termed "leaders" – included the likes of Australia, Estonia, Finland, France, the Netherlands, New Zealand, Norway, Singapore, Sweden, Switzerland, the U.S., the U.K.[12] Singapore[13] topped the index, earning the top spot beating out far larger countries such as the U.S. (second) and France (ninth).[14] Estonia snagged the fifth spot while Australia came in at number seven. In 2018, the U.K. and the U.S. topped this UN index with Estonia (fifth), Singapore (sixth), and Norway (tenth) rounding out the top ten.[15] Notably, these results are not unique to the above metrics. This mix of small and large countries has been acknowledged in academic work[16] and in elite interviewees[17] as countries like Sweden, Australia, Israel, Estonia, Finland, Denmark, Norway, the U.K., and Singapore came up alongside the U.S. time and time again when interviewees were asked to identify leaders in this space (national defense in cyberspace).

6 "Europe :: Estonia — The World Factbook - Central Intelligence Agency," accessed July 15, 2020, https://www.cia.gov/library/publications/the-world-factbook/geos/en.html.
7 Melissa K. Griffith and Adam Segal, "International Security and the Strategic Dynamics of Cyber Conflict," Columbia University SIPA and the Cyber Conflict Studies Association (CCSA), 2018.
8 Refer to the Appendix for a detailed description of the following indices.
9 Security and Defense Agenda, "Cyber-Security: The Vexed Question of Global Rules," 2012.
10 Melissa Hathaway, "Cyber Readiness Index 1.0," Report Presentation at the Belfer Center. Hathaway Global Strategies, 2013.
1111 "Which EU Country Is Most Vulnerable To Cybercrime?," Website Builder Expert, 2017, https://www.websitebuilderexpert.com/eu-cybercrime-risk/ and Ashton Young, "INFOGRAPHIC – The EU's Most Vulnerable Countries to Cybercrime," *Security Brief*, September 6, 2017.
12 International Telecommunication Union (ITU), "Global Cybersecurity Index," 2017.
13 Lester Hio, "S'pore Takes Top Spot in UN Cyber Security Index," *Straits Times*, July 7, 2017.
14 ITU, "Global Cybersecurity Index." 2017.
15 International Telecommunication Union (ITU), "Global Cybersecurity Index," 2018.
16 In their 2019 article on "The Determinants of Cyber Readiness", Makridis and Smeets note that countries like "the United States, Estonia and Singapore, are viewed as being ahead of the curve." Christos Andreas Makridis and Max Smeets, "Determinants of Cyber Readiness," *Journal of Cyber Policy* 4, no. 1 (January 2, 2019): p72, https://doi.org/10.1080/23738871.2019.1604781.
17 Author's interviews conducted for this dissertation.

In sum, while there is no single metric for measuring cyber-defense capabilities, early efforts have been uniform in one important aspect. Some relatively small states have historically found themselves as leaders in cybersecurity and defense capacity alongside far larger states. Given the field's long-standing theory that larger states are better positioned to provide national defense for their populations, why do we observe this particular constellation of leading states in this domain?[18]

Perhaps these relatively small states are merely an exception for reasons unique to each and are not emblematic of a broader theoretically important trend. In other words, is it just that Israel is distinctive in its ability to historically punch above its weight in national defense given the unique threat environment it finds itself in and its subsequent domestic investments in national defense technology and organizations? Or is it that Israel finds itself as a leader in national cyber-defense not simply for nongeneralizable reasons but instead, in part, for a similar reason to that found in other small states seen as ahead of the curve? 'Country specific' explanations are not without precedent in cybersecurity research – i.e. Israel is a weapons wizard with a strong tech sector[19] and Estonia moved quickly because they were one of the first countries to face cyberattacks.[20] However, it is not just Israel and Estonia who roar in cyberspace. While one or two of these states' presence as leaders could be explained away by unique circumstances, the presence of a handful spanning the globe requires us to consider explanations that are not so ad hoc or idiosyncratic.

Why and how have these so-called mice roared in the cyber era? If the U.S., one of the largest and most well-resourced states in global politics, has not found itself better positioned to provide national cyber-defense for its population than these smaller states, what other factors are shaping national cyber-defense capability beyond size and resources?

I argue that an important piece of the answer to these questions requires researchers to place states' historical geopolitical position and pre-existing defense architectures at the center of our analysis alongside the core strategic and operational dynamics facing all states. Put another way, to more fully understand national defense outcomes it is essential that we begin to delineate systemic dynamics from situational dynamics in cyberspace: i.e. dynamics all states face due to the threat space versus dynamics that are significantly mediated through national contexts and circumstances.

This approach represents a fundamental shift in how much of the field – both cybersecurity scholars and policymakers – has understood the organization and efficacy of national cyber-defense efforts. Yet, significantly, when we consider situational variables as well as systemic variables in the analysis of cyber-defense outcomes, a second puzzle emerges.

American policymakers and academics alike frequently characterized national defense efforts in cyberspace as a significant departure from the core requirements of national defense in the domains of air, land, and sea (i.e. that it represents a new type of defense problem for states to address). Henry Kissinger succinctly summed up this belief in a wide disjuncture between existing kinetic

[18] Note: Chris Demchak argues that cyberspace should be understood less as a domain, given the connotations domain holds for conflict, and as a "substrate". For a more detailed analysis of this debate, see Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (University of Georgia Press, 2011).
[19] Katz Yaakov and Amir Bohbot, *The Weapon Wizards: How Israel Became a High-Tech Military Superpower*, First Amer (St. Martin's Press, 2017).
[20] "How Estonia Became a Global Heavyweight in Cyber Security," E-Estonia, accessed June 27, 2020, https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

national security dynamics and cybersecurity dynamics when he argued that "[c]yberspace challenges all historical experience."[21] There are a myriad of concerns informing this view: e.g. debates that focus on the potential limitations of deterrence by punishment models[22] or a nascent, though not unchallenged, consensus that cyberspace is intrinsically an offense dominant domain.[23]

Yet, as Jason Healey argued in the first comprehensive history of cyber conflict, *The Fierce Domain*, one of the most important differences between national defense in cyberspace and prior national defense dynamics sits not at the level of strategy (e.g. deterrence) but at the level of operations (how strategies are executed or pursued in practice): "[p]erhaps the biggest difference between cyber conflicts and their traditional equivalents is the one most often overlooked: when defending against cyber conflicts, it is non-state actors, not governments, which typically are decisive in cyber defense".[24] Why? In cyber-defense, the resources states need to deploy in order to prevent an attack, defend against an ongoing attack. or recover from a previous attack are largely housed outside the military and even the government itself. Effective national cyber-defense requires significant civilian-military (frequently referred to as Whole of Government) and public-private cooperation and coordination (previously referred to Public Private Partnerships (PPP) in the U.S. and U.K. but now also frequently referred to as a Whole of Society approach). For countries like the U.S., this represented a new type of defense problem, one that required new actors within government and across society to now emerge as security players for the defense of the nation. For the U.S. this shift was simultaneously one of biggest differences between kinetic and cyber-defense and, as a consequence, initially one of the most difficult to address. As one former U.S. policy official remarked, "we weren't in the business of whole of society defense."[25]

However, while policymakers, industry, and academia in the U.S. saw this as a largely new feature of national defense in general, how states experience this disjuncture, in fact, varies. In Finland, for example, national cyber-defense efforts were articulated less as a pivot away from an existing national defense-posture but as an explicit extension of their kinetic defense posture. This was laid out most succinctly in one interview when a Finnish government official remarked that it took them a long time to figure out what Americans meant by public private partnerships (PPP) and why we were so concerned about finding a way to deploy them for national defense purposes. Why? Because "what you call PPP, we just call Finland."[26] Notably, this view was echoed across interviews and government documents: at the operational level, private roles and responsibilities were and are core to the implementation of national defense strategies more broadly. For Finland, despite other more readily studied states' preoccupation with categorizing cyber-defense as a sharp disjuncture from historical experience, the operational realities of national cyber-defense were not perceived to be as sharp a break from their historical experience.

21 Henry Kissinger, *World Order: Reflections on the Character of Nations and the Course of History*, Kindle Edition (Penguin, 2014).
22 For examples of work on deterrence refer to Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?," *Strategic Studies Quarterly* 4, no. 3 (September 22, 2010): 102–36; Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly*, no. 75 (2014) ; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (January 2, 2015): 4–37; Martin Libicki, "Would Deterrence in Cyberspace Work Even with Attribution?," *Georgetown Journal of International Affairs*, 2016; and Joseph S. Nye Jr, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 2016/2017: 44–71.
23 For examples of work on offense versus defense refer to Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (2013): 40–63 and Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (April 3, 2015): 316–48.
24 Jason Healey, *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, Kindle Edition (Cyber Conflict Studies Association (CCSA), 2013).
25 Lunch meeting with former US government official, 2019.
26 Author's Interview with Finnish Government Official tasked with cybersecurity, 2018.

While at face value these two motivating puzzles may appear to be causally distinct – why do mice roar in the cyber era and why is cyber-defense seen as a less revolutionary defense problem by some countries – there is a single factor significant to both outcomes. As states seek to address the strategic and operational realties of national defense in cyberspace, historical experience matters. And for these mice that roar, the defense problem they faced as a relatively small state in facing a precarious security environment shares an important operational reality with the national cyber-defense problem they now face.

I argue that national cyber-defense is best understood as a kind of "societal defense problem": a national security threat where (1) the vulnerabilities are society-wide, embedded within the daily functioning of civil society, government, the military, and the economy and (2) the resources states need to deploy in order to prevent an attack, defend against an ongoing attack, or recover from a previous attack are largely housed outside the military and even the government itself, i.e. within industry and the civilian population. Therefore, in order to address the core pressing national security concern facing states seeking to provide defense for their populations in the cyber era (what I refer to as 'critical interconnectedness': their dependence on and the interconnectivity of cyberspace), states must structure national cyber-defense in a manner that does not rely on military or intelligence agencies as the sole or even primary defense actors while simultaneously integrating both public and private actors into a cohesive, real-time national defense posture.

Significantly, when understood as a societal defense problem, cyber-defense does not represent a universal departure from the core requirements of national defense in the domains of air, land, and sea. Notably, these Mice that Roar, have historically faced another kind of societal defense problem – one born not from the strategic and operational dynamics of a particular domain of conflict but rather from their geopolitical position. Given their size and geographically precarious position, these Mice that Roar have historically deployed unique models for national defense seeking to address high levels of vulnerability across the homebase (or homeland) by pointedly emphasizing both public-private and civilian-military roles and responsibilities, coordination and cooperation. As a result, and in contrast to larger states like the U.S., these states have been able to more coherently incorporate cyber-defense into their historical approaches to national defense.[27] In other words, these mice have roared in cyber-defense because they have been able to leverage an existing societal defense architecture, an operational bedrock that leverages resources across society for the defense of the state, to address this new kind of societal defense problem.

As a consequence, my research challenges two prevailing assumptions in security studies and cyber conflict scholarship: (1) that larger states with more resources will be better positioned to provide national defense for their populations and (2) that national cyber-defense, as a central task of states, represents a significant departure from the core requirements of national defense in the domains of air, land, and sea (i.e. that it represents a fundamentally new kind of defense problem for states to address).

If this dissertation, therefore, where to be framed as a direct reply to Kissinger, I would contend that cyberspace challenges some historical experience more than others. The nature and severity of that

[27] In January 2019, I published an article in the *Journal of Cyber Policy* examining how Finland has leveraged its historical comprehensive security approach into cyberspace. Notably, In comprehensive security (*kokonaisturvallisuus*), which includes cybersecurity, the responsibility for and the safeguarding of the vital functions of society are jointly held by private and public actors, industry and government, defense forces and citizens. Melissa K. Griffith, "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 407–29.

challenge, in fact, influences the organization and efficacy of a given state's national defense models in the cyber era.

If this dissertation were to be framed as a direct response to the conventional understanding of national security that leads us to reasonably expect that the largest, most powerful military actors will also be the best positioned to provide national defense for their populations, I would argue that the very defense postures these relatively small states developed to mitigate the consequences of the geo-strategic environment in which they were imbedded are now mirrored in the postures far larger states hope to adopt in the cyber era. Given the strategic and operational dynamics underpinning national cyber-defense, there are advantages to having been small and precariously placed.

The remainder of this introductory chapter proceeds in five parts. First, I provide an overview of the central argument animating this dissertation – as states seek to solve for critical interconnectedness in the cyber era, their historical defense posture matters. This overview is then further augmented in Chapter Two, which presents the theoretical foundations that support this argument. Second, I provide a summary of the evidence gathered across five distinct country cases, which supports this argument. In order to maximize transparency in the research design underpinning the argument presented in this dissertation, Chapter Three describes, in depth, the case selection and data collection methods utilized in this research project. Part II of this dissertation, which includes Chapters Four through Six, delves into these cases in depth, walking the reader through the evolution of their particular cyber-defense posture and the degree to which the operational foundations of their kinetic-defense postures - an architecture that leveraged resources across society in defense of the state – overlapped with the operational realities of their cyber-defense posture. Third, I discuss the significance of this research for scholarship. I place my work into conversation with the emerging cyber conflict sub-field and demonstrate the important contributions this research makes to this literature through its focus on (i) small states, (ii) the defensive aspects of cyber conflict, (iii) the operational rather the predominate focus on strategic questions, and (iv) delineating systemic versus situational dynamics in cyber conflict. Fourth, given that cyber conflict is simultaneously an academic area of study and a pressing policy challenge, I provide an overview of the policy relevance of this work as states seek to bolster national cyber-defense capability. The policy implications stemming from this research is also the focus of Chapter Seven, in Part III of this dissertation and is discussed in more detail there. Fifth, and finally, I offer a roadmap for the remainder of this dissertation and walk the reader through the content and purpose of subsequent chapters.

2. The Argument

At its core, this research project hinges around two interrelated inquiries: (1) which factors underpin national cyber-defense capabilities and (2) which factors shape how successfully states adjust to the realities of national defense in the cyber era?

An important part of the answer lies in a frequently acknowledged in policy and political science circles but rarely systematically or rigorously examined variable: a state's defense posture – the defense strategies states adopt and the means through which they operationalize those strategies in practice. Resources need to be marshalled and organized to meet a strategic purpose (and often also a domestic purpose) given the national security needs of a state. This is not to say that states do not learn over time or that resources do not matter, either in terms of quality or quantity. Rather, there are a range of theoretical determinants of defense capacity. A state's defense posture is one critical and understudied determinant, and, importantly, it is this factor that is significant to answering both

motivating puzzles: why do mice roar in the cyber era and why is cyber-defense seen as a less revolutionary defense problem by some countries.

My argument, which is supported by two and a half years of within country, cross-national case study research across five countries[28] (Estonia, Finland, Israel, and Singapore in comparison to the much larger U.S.), can be broken down into three constituent parts.

First, despite the dominant focus on size as a measure for a state's defense capacity within international relations and security studies scholarship, resources (both in terms of preponderance and quality) are only one determinate of state defense capacity. In fact, we cannot accurately assess relative cyber-defense capability without taking seriously how states organize their resources in an effort to address the need they face (the threat environment they find themselves embedded within). States' cyber-defense postures – defense strategies and the defense architectures that support or operationalize those strategies in practice – shape why states develop certain resources and how they chose to deploy the resources they have at their disposal. As a consequence, defense postures are a critical component of defense capability and defense outcomes alongside the need or threat they face and the resources they can bring to bear.

Second, some defense postures are better suited for addressing the realities of national defense in the cyber era than others. Just as military capability in the twentieth century relied on a pattern of force employment that allowed militaries to reduce their exposure in response to increasing lethality,[29] cyber-defense capability relies, in significant part, on a defense posture that allows states to leverage resources across their society in order to address a central problem they now face given the realities of this domain: what I call 'critical interconnectedness' - their dependence on and the interconnectivity of cyberspace.

Third, importantly, states do not start with a blank conceptual and institutional slate every time a new defense problem is introduced or prior defense problems evolve.[30] Notably, however, pre-existing defense postures, developed in specific geo-political and domestic environments, can provide strong or weak foundations for the emerging national cyber-defense problem states now face. For the U.S., the conceptual and operational foundations underpinning its existing kinetic defense posture served largely as a constraining force with national defense approaches that were largely maladapted to the societal defense problem they found themselves in. In contrast, for the Mice that Roar, existing kinetic defense postures served as an important operational, and sometimes strategic, bedrock from which to build.

More specifically, each of the Mice that Roar had strong historical foundations spanning six conceptual and operational categories. All six of which are essential for an effective cyber-defense posture. The U.S., despite (and due in large part to) its status as a great power, did not have these foundations at its disposal.

- Threats to national security not limited to kinetic, military operations

[28] Interviews were also conducted in Brussels, Belgium with individuals who could speak to the defense postures and cybersecurity dynamics of the Estonia, Finland, and the U.S., the role of the North Atlantic Treaty Organization (NATO) and the European Union (EU) within countries defense efforts, as well as national defense dynamics of cybersecurity more broadly.
[29] Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*.
[30] This concept is explored in depth in Chapter Two through a review of literature focusing on the stickiness of existing institutions and concepts over time.

- The homebase as a location for conflict
- Citizens as security actors
- The private sector as security actors
- The breadth and character of the economy as a national security imperative
- Strategic and operational oversight, coordination, and visibility across the defense-ecosystem

In short, for a subset of relatively small states, their pre-existing kinetic national defense approaches more closely resembled the desired solution set to national defense in cyberspace (a national defense posture supported by a societal defense architecture that leveraged public and private actors in depth) than the pre-existing approaches found in far larger powers like the U.S. These societal defense architectures exist, in large part, precisely because these states are not historically strong and resource-rich. Importantly, the defense problem of deep vulnerability born from their relative size and geopolitical position has key conceptual and operational similarities with the problem of critical interconnectedness now facing all advanced industrial states in the cyber era.

3. The Evidence

Through rigorous explanatory (aimed at theory building) and diagnostic (aimed at theory testing) case studies, I hope to convince readers that (1) the argument developed here is valuable for understanding outcomes within the five cases presented in this dissertation and (2) that the cases examined provide plausible grounds for believing this argument has wider utility for explaining the organization and efficacy of state cyber-defense postures more broadly while also (3) strengthening our understanding, theoretically and empirically, of the cyber-defense problem states currently face.

Note, I discuss my research design in significant detail in Chapter Three for those readers interested in a robust explanation of the case selection and data collection decisions that underpin the argument presented in this dissertation.

As an overview of this more detailed explanation, my argument - as states try to solve for critical interconnectedness in the cyber era, historical patterns of national defense matter - is supported by two and half years of within country, cross-national case study research on five countries (Estonia, Finland, Israel, Singapore, and the U.S.). By leveraging between and within case variation across these five states, the in-depth case research completed here illustrates the limitations of alternative explanations for addressing why these mice roar, develops and evaluates the argument presented in this dissertation, and demonstrates how the core dynamics animating this argument across states can also be observed within each of these states as they develop a cyber-defense posture over time.

Data collection consisted of three prongs: (1) archival research focused on both primary and secondary sources; (2) extensive in-depth, elite interviews with ninety-five individuals central to or experts in cybersecurity policy formation and ongoing operations in each country; and (3) observational data collected through attendance of and/or active participation in formal and informal meetings with policy-focused researchers, policy makers, and industry members focused on assessing the state of and opportunities for improvement in cyber-defense capabilities within and across states. In any study of recent events, but especially those laying within the national security space, there are significant limitations to basing analysis off publicly available documentation. Importantly, carrying out extensive within country interviews and participating in and observing formal and informal briefings and meetings significantly augmented the written primary source and secondary source records allowing for greater nuance and accuracy in tracing the decision processes

behind and the various strategic and operational choices over time. I did not merely study these five countries, I lived in them for periods ranging from one month to nine months at a time.

The initial structured comparison between Finland and the U.S. illustrates why historical defense postures matter for the organization and efficacy of cyber-defense efforts and how Finland, in developing a defense posture that sought to mitigate the potential negative outcomes stemming from significant vulnerability due to its relative size, laid useful conceptual and operational foundations for addressing critical interconnectedness whereas the U.S. experienced a sharper disjuncture between the driving factors motivating its kinetic defense posture and the systemic reality of national defense in the cyber era. Given Finland's geopolitical position neighboring Russia, its kinetic national defense posture has hinged off a focus on defense of society by maintaining society-wide resilience in the event of a crisis. In comprehensive security (*kokonaisturvallisuus*), as deliberately mirrored in the sub-category of cybersecurity, the responsibility for and the safeguarding of the vital functions of society are jointly held by private and public actors, industry and government, defense forces and citizens. For Finland, given limited resources, its societal defense architecture centered around resilience as a perceived defense imperative: the ability to absorb a big hit from a large neighbor and carry on critical economic, military, and societal functioning for as long as possible. This operational foundation allowed Finland, despite being a relatively late starter in cyber-defense in comparison to the U.S., to achieve a level of cyber-defense capability that very quickly ranked alongside far larger and historically powerful states.

The inclusion of Israel bolsters the generalizability of my argument in two ways: first, by introducing variation in terms of geographic location and the specific threat environment these relatively small states face and second, by testing this argument in a country whose specific defense strategy – an offensively based deterrence strategy – more closely resembles the U.S.'s strategic focus on deterrence than it does Finland's strategic focus on resilience.[31] The inclusion of Israel alongside Finland further highlights the importance not just of the strategy at the conceptual level but also in how strategies are operationalized (which actors are security actors and how they coordinate and cooperate toward that strategic goal). Notably, while Israel's defense posture more closely resembles the U.S. at the strategic level, the operationalization of its deterrence posture more closely resembles Finland by leveraging all citizenry and industry in-depth in order to implement that deterrence strategy. Israel's societal defense architecture, like Finland's, centers citizens as security actors (compulsory service and reserve forces) but, rather than the Finnish focus on resilience, Israel historically leveraged industry in support of innovation as a perceived defense imperative in order to address vulnerabilities born of population asymmetries (often framed in terms of population that could serve in a defense capacity relative to potential adversaries) and a lack of strategic depth (for example, a "hostile fighter could fly across all of Israel (40 nautical miles wide from the Jordan River to the Mediterranean Sea) within four minutes, while traveling at "only" subsonic speed."[32]).

Singapore provides an additional test of the argument by further expanding variation in geography and threat environment but also introducing a state whose strength has been, in large part, its ability to learn from other states and then to implement those lessons rapidly from the top-down across its society. Like Finland and Israel, Singapore's size is perceived as a source of vulnerability. As one

[31] A systemic quality of absorbing and recovering from attack, disruption or failure. In the case of Finland, they apply this term to the national level rather than just at the level of the firm, operating system, sector, etc.
[32] "Strategic Doctrine - Israel," Federation of American Scientists, 25 May 2000. Archived from the original on 1 July 2014. Retrieved 25 June 2020. https://web.archive.org/web/20140701145333/http://fas.org/nuke/guide/israel/doctrine/.

Singaporean interviewee remarked, Indonesia would simply need to have its population stand on the coast and pee in Singapore's general direction to put them underwater.[33] Yet, unlike Israel's focus on bolstering innovation or Finland's focus on strengthening resilience in response to unique vulnerabilities born of their relative size, Singapore's societal defense architecture features importing/adjusting lessons from abroad and implementing them cohesively across society at speed. For Singapore, unity and cohesion are framed as a national security imperative: "[a]s a small, multi-racial, multi-religious nation dependent on free trade to survive, and connected to the world by air, sea and the Internet" every Singaporean, individually and collectively, have been called upon "to build a strong, secure and cohesive nation".[34] In short, even in a state that is particularly good at "control c and control v",[35] as one Singaporean interviewee jested, we can observe the foundations of a pre-existing societal defense architecture first developed to operationalize their 'Poisonous Shrimp'[36] deterrence strategy now underpinning their subsequent cyber-defense efforts, operational foundations that are largely absent in the far larger U.S.

The final case, Estonia, differs from the prior four country cases in one important aspect. Gaining its independence from the USSR in 1991, Estonia came of age in the cyber era. As a consequence, it provides a unique test of my argument. Here we can observe the development of a small but precariously placed state's kinetic defense posture alongside and in direct conversation with its cyber-defense posture. Underpinning joint strategies of national resilience and deterrence (leveraging the North Atlantic Treaty Organization's (NATO) mutual defense clause), the responsibility for and the safeguarding of the vital functions of society are jointly held by private and public actors. In Estonia, we observe how the problem of vulnerability born from relative size and the problem of critical interconnectedness have key conceptual and operational similarities in real time rather than those similarities simply being perceived by policymakers retroactively as a consequence of the stickiness of defense postures even when circumstances have meaningfully changed.

4. Contributions to Scholarship

Cyberspace is altering the nature of warfare and conflict itself, and along with them, the character of security policy and the diversity of states prominently pursuing those policies. Notably, explaining these national security outcomes has only recently become a focus of political scientists and security scholars. Within this nascent but rapidly progressing field of study, my research fills two gaps in the existing literature.

First, it provides significant insight into the defensive dynamics of cyber conflict beyond the field's prevailing focus on deterrence strategies. I identify the core national defense concern underlying cyber-defense efforts – critical interconnectedness – and examine how states' existing defense postures can be maladapted to this reality while other states kinetic defense postures provide stronger conceptual and operational foundations from which to build. Within defense-oriented scholarship, the overwhelming focus of political scientists has been at the strategic level – namely deterrence – while those with a computer science background have focused on the technical level –

[33] Author's Interview, 2019.
[34] Singaporean Ministry of Defense, "Total Defence," accessed July 20, 2020, https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/total-defence.
[35] Author's Interview, 2019.
[36] According to former Singaporean Prime Minister Lee Kuan Yew, "[i]n a world where the big fish eat small fish and the small fish eat shrimps, Singapore must become a poisonous shrimp" in order to deter potential hostilities by imposing high costs on any potential aggressor even in the event of an overwhelming force. For an overview of this defense doctrine, refer to Stephen Kuper, "Taking a Closer Look at Singapore's 'Poison Shrimp' Defence Doctrine," *Defence Connect*, February 11, 2020.

e.g. questions of network defense - through technical analysis. In contrast, operational analysis is all too rare. This dissertation rests soundly within the operational segment of conflict. Importantly, it is the operational foundations that the Mice that Roar have in common while their particular defense strategies vary from an offensive-brand of deterrence to resilience. As a result, my research explicitly differentiates between technical expertise and the operational and strategic components of national cybersecurity efforts. In fact, it is in the operationalization of strategy: spreading and applying technological expertise to broad swathes of industry, civil society, and government; information sharing and coordination in response to threats and in determining responsibilities between public and private actors; pooling of resources to stay ahead of the evolving threat landscape, maintaining critical infrastructure and services, etc. – that represents one of the biggest difference between cyber conflicts and their traditional equivalents.

Second, the overwhelming focus of the literature has been on a handful of larger states.[37] This leaves the question of how smaller states have pursued their national defense in cyberspace systematically unanswered. This small-state focus takes on greater significance when the contours of national cyber-defense are considered. Specifically, in our efforts to understand cybersecurity in the context of national security, previously overlooked insights for the organization and efficacy of national cyber-defense efforts lay outside the more heavily studied and larger states. Moreover, by expanding the aperture of cases to include these states alongside their larger and more readily studied counterparts, my research takes an important step toward delineating systemic (dynamics all states face due to the realities of cyberspace) from situational (dynamics that are significantly mediated by national or sub-national contexts) dynamics of cyber conflict. Most notably, the second puzzle from the beginning of this chapter points to a dynamic – that the requirements of cyber-defense represent a stark departure from the requirements of kinetic national defense – which is heavily mediated by national contexts rather than universally and equally experienced.

As a relatively nascent field, existing scholarship on cyber conflict and national security dynamics largely falls into four broad buckets.[38] This dissertation speaks directly to and contributes most heavily to scholarship falling within bucket three (research on the defensive dynamics in the cyber era) and four (the types of states that have been the primary focus of researchers).

4.1. Systemic Dynamics

The first bucket of work focuses on the systemic dynamics of cyber conflict and/or war. Researchers falling into this category have made important contributions to questions of stability,[39]

[37] For examples of emerging country specific empirically grounded analysis refer to Xu Wu, *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications* (Lexington Books, 2007); John Tkacik, "Trojan Dragon: China's Cyber Threat," Heritage Foundation, 2008; Nigel Inkster, "China in Cyberspace," *Survival* 52, no. 4 (September 21, 2010): 55–66; Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests* 35, (January 2013): 31–44; Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (June 2011): 1–24; Clement Guitton, "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?," *European Security* 22, no. 1 (March 2013): 21–35; Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34, no. 6 (July 2013): 1054–74; Arvind Subramanian, "Preserving the Open Global Economic System: A Strategic Blueprint for China and the United States," Peterson Institute for International Economics, 2013; and Jon R Lindsay and Tai Ming Cheun, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek Reveron (Oxford University Press, 2015).

[38] For a full review of the range of cyber conflict research, see Griffith and Segal, "International Security and the Strategic Dynamics of Cyber Conflict.".

[39] Erik Gartzke and Jon R Lindsay, "Thermonuclear Cyberwar," *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 37–48 and James N. Miller Jr. and Richard Fontaine, "A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict," New America, 2017.

escalation,[40] the offense-defense balance,[41] and the security dilemma.[42] For systemic work, the differences between kinetic conflict and cyber conflict are of particular interest rather than the particularities of individual states' behavior. Scholarship in this area is also some of the oldest and began with debates over whether cyber conflict represented a revolution or an evolution in how states compete[43] and whether the term 'cyberwar' accurately captured activity in this domain.[44] This early work took on particular importance because if it is an evolution, previous theoretical models more readily describe the phenomenon. If it is a revolution, then many, if not most, of our theoretical models contain assumptions and dynamics that are inappropriate to the study of cyber conflict and cyber security.

4.2. Tools of State Competition

The second bucket of work moves away from systemic concerns and focuses instead on the utility and character of the traditional tools of state competition in the cyber era. Questions that fall into this category often have an offensive component and include theoretical and empirical examinations of coercion,[45] shaping vs signaling,[46] and power[47] in the cyber era. In the same vein, though focused

[40] Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (September 22, 2012): 46–71; James D Fielder, "Bandwidth Cascades: Escalation and Pathogen Models for Cyber Conflict Diffusion," *Small Wars Journal* 9, no. 3 (2013); and Erica Borghard and Shawn Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* Fall (2019): 122–45.

[41] There is widespread support in academic and policy circles for viewing cyberspace as offense dominant. However, a vocal minority Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (July 2013): 365–404 and Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013) are pushing back against the claim that offense has the upper hand. For examples of the former, refer to Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007); Joseph S. Nye Jr, "Cyber Power," Essay from the Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 401–428; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (October 28, 2013): 7–40; and Keir Lieber, "The Offense-Defense Balance and Cyber Warfare," in *Cyber Analogies*, ed. Emily O. Goldman and John Arquilla (Naval Postgraduate School, 2013). For examples of the latter, refer to Lindsay, "Stuxnet and the Limits of Cyber Warfare" and Rid, *Cyber War Will Not Take Place*.

[42] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Kindle Edition (Oxford University Press, 2017).

[43] Refer to John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993): 141–65; Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Reprint Edition (HarperCollins e-books, 2011) ; Nazli Choucri, *Cyberpolitics in International Relations* (MIT Press, 2012); Timothy Junio, *A Theory of Information Warfare* (University of Pennsylvania dissertation, 2013); Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft."; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology and Politics* 10, no. 1 (January 2013): 86–103; Rid, *Cyber War Will Not Take Place*.; Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (2014): 181–192; Lucas Kello, *The Virtual Weapon and International Order*, Kindle Edition (Yale University Press, 2017); Jon Randall Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 493–514; and George Perkovich and Ariel E. Levite, eds., *Understanding Cyber Conflict: Fourteen Analogies* (Georgetown University Press, 2017).

[44] For examples of work on cyberwar more broadly, refer to Jeffrey Carr, *Inside Cyber Warfare: Mapping The Cyber Underworld*, Second Editon (O'Reilly Media, 2010); Rid, *Cyber War Will Not Take Place*; and Singer and Friedman, *Cybersecurity: What Everyone Needs to Know*.

[45] Benjamin M. Jensen, Brandon Valeriano, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, 2018); Travis Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony," *Journal of Strategic Studies* 40, no. 7 (November 10, 2017): 898–926; and Quentin E. Hodgson et al., "Fighting Shadows in the Dark Understanding and Countering Coercion in Cyberspace," RAND, 2019.

[46] Refer particularly to Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Kindle Edition (Harvard University Press, 2020).

[47] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security.* (National Defense University Press, 2009); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (National Defense University Press and Potomac Books, 2010); Alexander Klimburg, "Mobilizing Cyber Power," *Survival* 53, no. 1 (2011): 41–60; David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed," *Journal of Strategic Studies* 35, no. 5 (October 2012): 689–711; Ebert and Maurer, "Contested Cyberspace and Rising Powers."; John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 286–293; Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (July 3, 2017): 452–81; Kello, *The Virtual Weapon and International Order*; Tim. Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2017); and Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony."

on a different unit of analysis, scholars who examine the ways in which cyber operations can be integrated into the battlefield[48] or how offensive cyber capabilities have developed and proliferated[49] would also fit into this category of research. Notably, cyber operations are not merely the purview of states, they can be and have been leveraged by non-state actors to achieve tactical and strategic goals. This trend has led to a subset of research focusing on non-state actors, such as proxy actors and militias.[50]

4.3. Defensive Dynamics

The third bucket of work, and where this dissertation is primarily located, addresses the defensive aspects of cyber conflict. Scholarship here has largely focused its attention on the feasibility of one particular national defense strategy – deterrence – and the limitations of such a strategy for cyber-defense.[51] Research focusing on increasing cybersecurity and decreasing the threats states face emanating from cyberspace through the use of norms[52] and international cooperation including military alliances[53] also falls into this bucket and broadens defense-centered conversations beyond

[48] Max Smeets, "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment," *Defence Studies* 18, no. 4 (October 2, 2018): 395–410.

[49] Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, no. 1–2 (February 23, 2018): 6–32.

[50] Refer to Scott Applegate, "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare," *IEEE Security and Privacy* 9, no. 5 (September 2011): 16–22; Adam Segal, "The Rise of Asia's Cyber Militias," The Atlantic, 2012; Nicolò Bussolati, "The Rise of Non-State Actors in Cyberwarfare," in *Cyber War: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein (Oxford Scholarship Online, 2015); and Maurer, *Cyber Mercenaries: The State, Hackers, and Power*.

[51] Refer to Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security.*, ed. Franklin Kramer, Stuart H. Starr, and Larry K. Wentz, First Edition (Potomac Books, 2009), 309–342; Martin C. Libicki, "Cyberdeterrence and Cyberwar," 2010; Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?," *U.S. Senate Washington, DC Committee on Armed Services* 4, no. 3 (2010); Joseph S Nye, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly*, 5(4): 18–38, 2011; Jeffrey Cooper, "A New Framework for Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek. S. Reveron (Georgetown University Press, 2012), 105–120; Brandon Valeriano and Ryan C Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11," *Journal of Peace Research* 51, no. 3 (May 1, 2014): 347–60; Gartzke and Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace."; Richard Harknett, "Information Warfare and Deterrence," *Parameters*, 1996, 93–107.; Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*.; Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War."; Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (July 1, 2012): 229–44.; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth," *International Security* 38, no. 2 (2013): 41–73.; Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?," *Journal of Strategic Security* 7, no. 1 (2014): 54–67.; Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution," *Fletcher Security Review* 1, no. 2 (2014): 54–73.; Jon R Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (September 1, 2015): 53–67.; Jason Healey, "Beyond Attribution: Seeking National Responsibility in Cyberspace," 2016.; and Amir Lupovici, "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward," *International Studies Perspectives* 17, no. 3 (August 1, 2014).

[52] For examples, refer to Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future: Security and Prosperity in the Information Age*, ed. Kristin M. Lord and Travis Sharp (The Center for a New American Security (CNAS), 2011).; Eneken Tikk, "Ten Rules for Cyber Security," *Survival* 53, no. 3 (June 2011): 119–32; Panayotis Yannakogeorgos, "Cyberspace, the New Frontier – and the Same Old Multilateralism," in *Global Norms, American Sponsorship and the Emerging Patterns of World Politics*, ed. S. Reich (Palgrav, 2011).; Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (April 2012): 148–70; Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 322–31; Harry Farrell, "Promoting Norms for Cyberspace," Council on Foreign Relations (CFR), 2015.; Toni Erskine and Madeline Carr, "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace," in *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO Cooperative Cyber Defence Centre of Excellence, 2016).; Anna-Maria Osula and Henry Rõigas, eds., *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO Cooperative Cyber Defence Centre of Excellence, 2016).; and Henry Farrell and Charles L Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 7–17.

[53] For work focusing on a subset of cooperation —"Cyber Arms Control Institutions and Regimes"— refer to Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 2010): 384–410; Kenneth Geers, "Cyber Weapons Convention," *Computer Law and Security Review* 26, no. 5 (September 1, 2010): 547–51; Herbert Lin, "Arms Control in Cyberspace: Challenges and Opportunities," *World Politics Review* March (2012).; Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).; Valeriano and Maness, "The Dynamics of Cyber Conflict between

the utility of deterrence and national means alone. Research focusing on the operational requirements and importance of homebase defense, which are the focus of this project, also falls here.

4.3.1. Deter, Deny, and Contest

It is worth delving into the deterrence literature in more detail because it speaks directly to the question of why states need to develop cyber-defense capabilities for homebase defense purposes in the first place. Namely, can cyber-threats simply be deterred either through offensive cyber or cross-domain (e.g. air, land, and sea) means? States have at their disposal a series of national-defense postures ranging from prevention to effective warfighting/conflict to recovery after cessation of hostilities. Some might ask, therefore, why any state would need to increase the security and resilience of its critical functions in the face of potential cyberattacks if, instead, they could simply deter potential adversaries from treating their homebase as a conflict space in the first place.

This question, been one of the most heavily investigated questions within the cyber conflict literature and has similarly been a significant focus of industry and policy practitioners alike.[54] Notably, there is widespread consensus within scholarship, industry, and policy that cyber conflict raises a series of specific challenges for classical models of deterrence.[55]

Classical deterrence strategies rely on two central mechanisms in order to effectively prevent conflict from occurring in the future: (1) a credible threat of the imposition of costs in retaliation (deterrence by punishment), and/or (2) the ability to deny strategic benefit (deterrence by denial) if an attack does occur. Notably, however, both of these mechanisms (though, the first mechanism in particular) face significant challenges in cyber conflict for four reasons.

First, the first mechanism hinges off the ability of a state to attribute attacks in order for a state to then be in a position to subsequently impose costs. Yet, attribution presents a unique challenge in cyberspace. Complications examined within the cyber-deterrence literature include "the time it may take to technically or politically attribute an attack to a specific actor; difficulties raised by false flags, plausible deniability, and proxy actors; and reliance in some instances on private actors for forensic attribution."[56] While some cyberattacks are harder to attribute than others and some of these aspects can potentially be mitigated,[57] attribution remains a particular technical and policy challenge facing states seeking to prevent cyberattacks through a deterrence by punishment model.

Rival Antagonists, 2001–11." Other notable works in the broader cooperation and international institutions literature include Robert Axelrod, " Beyond the Tragedy of the Commons: A Discussion of Governing the Commons: The Evolution of Institutions for Collective Action ," *Perspectives on Politics* 8, no. 2 (June 2010): 580–82; Melissa E. Hathaway, "Toward a Closer Digital Alliance," *SAIS Review of International Affairs* 30, no. 2 (2010).; Eneken Tikk, "Global Cybersecurity–Thinking About the Niche for NATO," *SAIS Review of International Affairs* 30, no. 2 (2010).; Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Issue Brief for The Atlantic Council, 2011.; Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly* 6, no. 3 (September 22, 2012): 20–46.; James W. Forsyth, "What Great Powers Make of It: International Order and the Logic of Cooperation in Cyberspace," *Strategic Studies Quarterly* 7, no. 1 (2013).; David Clark, Thomas Berson, and Herbert S. Lin, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (National Academies Press, 2014).; Laura. DeNardis, *The Global War for Internet Governance* (Yale University Press, 2014).; Lindsay, "Restrained by Design: The Political Economy of Cybersecurity."; and Joshua Rovner and Tyler Moore, "Does the Internet Need a Hegemon?," *Journal of Global Security Studies* 2, no. 3 (July 1, 2017): 184–203.

54 Griffith and Segal, "International Security and the Strategic Dynamics of Cyber Conflict."

55 For examples refer to Libicki, "Cyberdeterrence and Cyberwar."; Iasiello, "Is Cyber Deterrence an Illusory Course of Action?"; and Rid and Buchanan, "Attributing Cyber Attacks."

56 Griffith and Segal, p6.

57 Gartzke and Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace."

Second, the first mechanism relies on the ability of the attacked state to impose costs on the attacker. Yet, reliance on cyberspace is asymmetric: not all states share the same dependence on cyberspace for the critical functioning of society, its military, and government. In reality, some states and non-state actors have smaller relative attack surfaces than others, which constrains both the potential scope and scale of deterrence by punishment through retaliation in-kind. This stands in stark contrast to the deterrence model known as Mutually Assured Destruction (MAD). In contrast to nuclear weapons, seen by some as the penultimate deterrence model because all states are vulnerable to them, in cyberspace potential adversaries may not be equally vulnerable to cyberattacks and therefore may not be susceptible to the level of cost imposition necessary to deter them. However, it is worth noting that punishment does not need to be in kind. Moreover, some forms of cyberattacks may rise to the threshold of armed conflict and merit a kinetic response.

Third, the first mechanism centers around states' ability to tailor retaliation to specific types of attacks. Retaliation as a tool for preventing certain types of conflict from occurring is not a catch-all response to any type of malicious activity by any hostile actor. Instead, retaliation, particularly given concerns over conflict escalation and proportionality (of particular concern for many states),[58] requires that states are able to categorize an incident and tailor a specific response. Yet, in the realm of cyber conflict

> the purpose and scale of an attack is often ambiguous. An observable outcome could be a failed effort at a more major network breach, a warning shot, espionage, or an operational preparation of the environment (OPE) for future activity. On the other side of the coin, the effects from any given attack can be unpredictable and can far exceed the root cause.[59]

As a result, even if the attribution problem could be adequately overcome and reliance on cyberspace was not asymmetric, states seeking to secure their homebase solely through a deterrence by punishment strategy would still face a significant challenge in how to effectively tailor their retaliation.

Fourth, both the first and the second mechanism for deterrence rely on the ability of a state to signal capabilities to other states.[60] In terms of deterrence by punishment, states need to be capable of signaling cost-imposing capabilities to potential adversaries. Yet, "cyber capabilities are less visible than their kinetic counterparts and have limited life spans (i.e., once attacked, the target is made aware of a vulnerability and has an opportunity and incentive to address it)."[61] Moreover, for the second mechanism to be effective (deterrence by denial) states not only need to increase the security and resilience of the homebase in the face of potential malicious cyberactivity (the focus of this dissertation), but also to be able to signal those robust defensive capabilities to potential adversaries in a manner that does not undermine the security and resilience of those same systems.

Taken together, these four challenges undercut the ability of states to credibly threaten the imposition of costs in retaliation (deterrence by punishment) and to signal their capability of denying the benefits gained from cyberattacks (deterrence by denial). This recognition has led to a lively

[58] For example, the U.S. does not threaten to retaliate with nuclear weapons in any instance of malicious behavior but only in specific instances that rise to certain thresholds. Similarly, carpet bombing is not considered appropriate retaliation for shooting down a drone. Proportionality is not only a priority for states concerned with the ethics of a particular action (Just War Theory) but also a concern for those seeking to prevent escalation, unintended or otherwise.
[59] Griffith and Segal, "International Security and the Strategic Dynamics of Cyber Conflict.", p7.
[60] Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*.
[61] Griffith and Segal, "International Security and the Strategic Dynamics of Cyber Conflict." p6.

debate over whether these limitations can be overcome and, if so, to what degree.[62] This includes work focused on cross-domain deterrence[63] and efforts to expand the conceptual framework of deterrence to include dissuasion through entanglement and norms[64] rather than the classical focus on punishment and denial. Yet, there is little agreement in the defense-focused literature on whether or not these challenges can be meaningfully overcome, especially in areas where cyberattacks are not occurring in the context of warfare alongside kinetic operations[65] or do not meet or surpass thresholds for war in their own right and therefore result in armed conflict.[66]

This persisting concern over the limitations of deterrence as a strategy for cyber conflict prevention is mirrored in policy circles. For example, in 2018, U.S. Cyber Command (USCYBERCOM) publicly announced a strategic vision for the newly unified combatant command. This strategic vision introduced the concept of persistent engagement (PE). PE stemmed from the recognition that while deterrence could be seen as largely effective in the upper levels of conflict (above the threshold of significant, armed interstate-conflict and at the level of nuclear deterrence), the U.S. continued to be subject to increasing malicious cyber activity at home below those thresholds. PE focused not on deterrence but on "continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver."[67] This shift in strategy is consistent with Harknett and Fischerkeller's argument that, given its limitations, deterrence is not a credible strategy for cyberspace, and that the U.S. should turn instead to a strategy of cyber persistence. This overlap should come as no surprise, given their connections with USCYBERCOM during the development process for this strategy. Notably, that same year, the U.S. established the Cybersecurity and Infrastructure Security Agency (CISA) under the auspices of the Department of Homeland Security (DHS) in an effort to increase the security and resilience of the homebase given the civilian and government dependence on cyberspace for critical functions. In short, the defense posture of the U.S., a superpower with significant traditional military capabilities including nuclear weapons, shifted its efforts to specifically bolster its capabilities to contest and deny malicious cyberactivity rather than simply rely on its ability to deter malicious activity.

Moreover, even prior to the emergence of this 5th domain of conflict,[68] deterrence was never the sole thread of the U.S. defense posture. In the event that prevention fails (other than in the case of MAD, where mutual destruction is assured), the U.S. has always relied on defense capabilities focused on securing favorable outcomes in the event of hostilities or conflict. Therefore, even without all of the prior discussion regarding the limitations of deterrence-based models, a tomahawk missile would not bring an electricity grid back online or protect a military's center of gravity (the network of networks linking troops, weapons, and weapons platforms to each other and up the chain of command) in the field.

62 For examples refer to Gartzke and Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace."; Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation," 2018; and Nye Jr, "Deterrence and Dissuasion in Cyberspace.".
63 Gartzke and Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace."
64 Nye Jr, "Deterrence and Dissuasion in Cyberspace."
65 Cyber operations can and have occurred alongside kinetic operations in the context of ongoing military operations and/or conflict.
66 A significant portion of cyber conflict exists below the threshold of war in what scholars and practitioners refer to as the gray-zone.
67 Jacquelyn G. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy - Lawfare," *Lawfare*, May 10, 2019.
68 The first four domains of conflict being air, land, sea, and space. For many states, space is not a domain of conflict (they lack space capabilities and/or programs), which would make cyberspace the 4th domain of conflict for them.

In short, as Martin Libicki argued in his 2009 RAND report, cyber conflict has its own strategic, operational, and tactical dynamics that set it apart from kinetic conflict in air, land, and sea. Most notably, "the ambiguities of cyber deterrence contrast starkly with the clarities of nuclear deterrence" as well as our models of conventional deterrence more broadly.[69] While this dissertation does not seek to directly address questions of strategy more broadly or deterrence in particular, the importance of homebase defense, and the operational challenges it entails given the reality of critical interconnectedness in the cyber era, compliment and gain greater importance given the concerns raised in this ongoing area of research.

4.3.2. Public Private Partnerships

Another particular strand of work within this third bucket, which mirrors a concern widely acknowledged within policy circles globally, is the emerging cybersecurity research centered on the unique importance of public private partnerships (PPP) for cybersecurity purposes.[70] This literature hinges off the observation that evolution in technology has led to increasing privatization of national defense.[71] Much of this work has focused, however, on specific cases of PPP, frequently the U.S. and U.K., and as a consequence privileges specific patterns for "how policy-makers and the private sector are conceptualizing their respective roles in national cyber security"[72] while overlooking significant variation between and within states over time. As a consequence, this dissertation builds off these existing PPP foundations while also addressing both of those gaps. Despite a proliferation of other relevant actors, state organization and capacity – domestic regulations, civilian-military divisions of power, private-public partnerships, etc. - remain a core component of providing national cyber-defense for their populations.

4.3.2. Explaining Variation in Defense Outcomes

Within the realm of national defense dynamics more broadly, little systematic attention has been paid to why we observe variation in the organization and efficacy of cyber-defense capabilities: in other words, operationalizing strategies. The one notable exception is a 2019 article by Christos Andreas Makridis and Max Smeets, which sought to identify which factors best predict cyber readiness rankings assigned by the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) over time.[73] They found that states with a high dependence on cyberspace and a more threatening security environment were more likely to receive higher GCI rankings.[74] However, consistent with the puzzle presented at the start of this chapter, resources (primarily GDP) were not a good predicator of GCI rankings.

[69] Libicki, "Cyberdeterrence and Cyberwar." p. xvi.

[70] For examples of analysis on private actors in cyber-defense and conflict see Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179–87.; Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *Brown Journal of World Affairs* 18, no. 1 (2011): 57–69.; Chris Golden, "Creating New Private-Public Partnerships in Cybersecurity," *National Cybersecurity Institute Journal* 2, no. 3 (2015).; Tatiana Tropina and Callanan Cormac, *Self- and Co-Regulation in Cybercrime, Cybersecurity and National Securit* (SpringerBriefs in Cybersecurity, 2015).; and Griffith, "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity."

[71] Refer to Myriam Dunn Cavelty and Elgin M. Brunner, "Introduction: Information, Power, and Security—an Outline of Debates and Implications," in *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, ed. Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel (Aldershot: Ashgate, 2007). p8-9 and Joseph E. Stiglitz and Scott J. Wallsten, "Public-Private Technology Partnerships," *American Behavioral Scientist* 43, no. 1 (September 27, 1999): 52–73 p57.

[72] Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies," *International Affairs* 92, no. 1 (2016): 43–62.

[73] Makridis and Smeets, "Determinants of Cyber Readiness."

[74] These two factors fall under the category need in my theoretical framework, which is presented in detail in Chapter Two.

In contrast to Makridis and Smeets work, this dissertation focuses not just on identifying quantifiable factors that predict variation in cyber readiness rankings, but on why resources appear to be a poor predictor of national cyber-defense outcomes. In order to accomplish the latter, I establish a theoretical framework in Chapter Two for national cyber-defense capability and its theoretical determinants. This framework hinges not just on the more frequently discussed drivers in national security and defense scholarship more broadly – the threat environments states are embedded within and/or a relative preponderance of resources – but on the defense purpose and organization of resources within states. It is the latter factor, importantly, that provides significant insight into why a sub-group of relatively small states have been able to become significant providers of national defense for their populations despite their limited resources. Therefore, while Makridis and Smeets work further reinforces the puzzle that motivated this project, it does not identify the answer or establish its broader significance.

4.4. Historical and Country Analysis

The fourth and final bucket of work focuses heavily on historical analysis of specific countries. Whether within academic or think tank venues, country specific cybersecurity analysis has focused primarily on larger or historical great power states such as the U.S., U.K., China, and Russia[75] with a scattering of exceptions.[76] This dominant focus of the cybersecurity field of study on a subset of large states or great powers leaves the question of how most states have understood and approached national cyber-defense and cybersecurity systematically unanswered. Moreover, while this country specific work has provided important insights into cyber conflict and the trials these particular states faced in adjusting to the realities of conflict in the cyber era, it has also brought with it a critical conceptual shortcoming: the risk that many of the dynamics found in this sub-set of states, though assumed to be largely systemic (dynamics all states face), are in fact better understood as situational (mediated through national or regional contexts). Even more concerningly, these assumed systemic dynamics later find themes baked into subsequent theoretical models of national security in the cyber era to the potential detriment of both our academic understanding and our sub-national, national, and international policies.

By focusing instead on a subset of often overlooked countries and placing them in direct comparison to a more frequently studied state that has informed much of our theoretical, empirical, and policy development, my research takes an important step toward (a) a more global and comprehensive understanding of the cybersecurity problem and (b) exposes factors that drive variation in cyber-defense approaches and subsequently (c) provides a more robust foundation from

[75] Much of the academic scholarship is underpinned by empirics drawn from far larger states and emerging country specific work predominantly focuses on these same states. For examples of emerging country specific empirically grounded analysis refer to Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age* (Routledge, 2007).; Wu, *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications*.; Tkacik, "Trojan Dragon: China's Cyber Threat."; Inkster, "China in Cyberspace."; Nikolas K. Gvosdev, "The Bear Goes Digital: Russia and Its Cyber Capabilities," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek Reveron (Georgetown University Press, 2012).; Adam Segal, "The Code Not Taken: China, the United States, and the Future of Cyber Espionage," *Bulletin of the Atomic Scientists* 69, no. 5 (September 27, 2013): 38–45; Blank, "Russian Information Warfare as Domestic Counterinsurgency."; Guitton, "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?"; Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence."; Subramanian, "Preserving the Open Global Economic System: A Strategic Blueprint for China and the United States."; Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (January 27, 2015): 7–47; and Lindsay and Cheun, "From Exploitation to Innovation: Acquisition, Absorption, and Application."

[76] There are a few notable exceptions within academic scholarship, such as Burton's analysis of New Zealand, which examines New Zealand approach to cybersecurity through the traditional lens of three small-state defense models: alliances, institutional cooperation, and norms, and Ebert and Maurer's research on rising powers' efforts to contest cyberspace. See Joe Burton, "Small States and Cyber Security: The Case of New Zealand," *Political Science* 65, no. 2 (2013): 216–38 and Ebert and Maurer, "Contested Cyberspace and Rising Powers."

which to examine fundamental national security dynamics in global politics such as stability, escalation, and power.

5. Policy Significance and Implications

Cyber conflict is simultaneously an important and vibrant area of academic research and a pressing policy challenge. One such challenge rests at the center of my work: how can a state - where much of critical services, infrastructure, and technical competency is privately held - provide national defense for their population in an era of critical interconnectivity? In broad brushstrokes, this dissertation provides important empirical and theoretical leverage in two ways as states seek to answer this question.

First, by identifying the main drivers behind cyber-defense capability, this research provides the policy community with a necessary foundation for the defensive aspects of cyber conflict and competition. Identifying the factors that shape states relative ability to effectively organize their resources allows for more nuanced and accurate recommendations regarding the types of investments that may provide greater utility for a wide variety of states attempting to bolster their relative cyber-defense capabilities now and in the future. Opportunities for learning exist across all three dimensions of cybersecurity at the national level - technical, operational, and strategic – offering insight into developing and maintaining technological expertise and tools, integrating a societal defense approach into strategic goals and imperatives, and the tangible operationalization of these strategies.

Second, by examining how a subset of relatively small countries (Estonia, Finland, Israel, and Singapore) have become significant providers of national cyber-defense for their populations, my work presents the evolution of four cyber-defense models that robustly integrate both public and private actors into a cohesive, real-time national defense posture. "Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective",[77] yet the particularities of those ecosystems will remain largely national in character. They bring with them their own strengths and shortcomings. These models, therefore, provide important analytical leverage for policy-makers within government and industry seeking to bolster their own national cyber-defense postures given the peculiarities of their own domestic ecosystems and the special character of the threat environment they found themselves embedded within.

Notably, for policy audiences, the three countries that are leveraging a historical society defense architecture into the development of their cyber-defense posture – Finland, Israel, and Singapore – have three very different purposes for developing that architecture in the first place. If each of these countries had a particular 'superpower' when it comes to leveraging all of society in defense of the states they would be Resilience, Innovation, and Implementation in turn.

[77] Tom Miler, "U.N. Survey Finds Cybersecurity Gaps Everywhere except Singapore," *Reuters*, July 5, 2017.

Overview of Three Historical Models for Societal Defense

	Societal Defense Problem	Defense Strategy	Focus of Societal Defense Architecture
Finland	Small population (relative) Big neighbor along entire eastern border with which there is a historical rivalry Concerned over territorial integrity and independence	Comprehensive Security (maintaining critical functions) Buying time in order to increase the costs of conflict for adversaries through a war of attrition and increase the odds of a more favorable outcome	Conscription (bolster numbers) Resilience (the ability to absorb a big hit)
Israel	Small population (relative) Severe lack of strategic depth Four neighbors along its borders and several states within the region more broadly with which there are historical rivalries Concerned over territorial integrity, independence, and (in some policy circles) survival of the population	Offensive Deterrence Preemption and rapid escalation of conflict into enemy territory to decrease the duration of conflict and increase the odds of a more favorable outcome	Conscription (bolster numbers) Innovation (quality over quantity)
Singapore	Small population (relative) Severe lack of strategic depth Two neighbors with which there are historical tensions Concerned over territorial integrity and independence	Deterrence (Poisonous Shrimp/Porcupine) The ability to inflict high costs on adversaries during hostilities	Conscription (bolster numbers) Implementation (rapid cohesive response from the top-down)

In conclusion, given the pressing security policy challenges facing states in cyberspace, a more nuanced and far reaching discussion of the policy implications stemming from this research can be found in Chapter Seven in Part III of this dissertation. There, policy implications as well as important future research opportunities building off the foundations laid over the course of the dissertation are discussed at length and in detail.

6. Roadmap for the Dissertation

PART I of this dissertation wraps up with the following two chapters. Chapter Two provides the theoretical foundations central to the argument of this dissertation: as states try to solve for critical interconnectedness in the cyber era, some historical patterns of national defense are better suited to the operational realities of cyber-defense than others. In this chapter, I first establish a theoretical framework for thinking about national defense capability and its theoretical determinants and assess the utility of those determinants for explaining why a grouping of relatively small states have been able to rival far larger states' cyber-defense capabilities before addressing why historical approaches

can shape a state's development of cyber-defense capabilities, for better or for worse. This chapter concludes with a broader discussion of societal defense problems, placing cyber-defense into direct conversation with this parent category of national security imperatives and drawing out core similarities and differences between cyber-defense and prior societal defense iterations. Chapter Three discusses the research design that underpins this project in detail. It addresses why Estonia, Finland, Israel, Singapore, and the U.S. were selected as cases and how data was collected and will be presented in the remainder of the dissertation. This section answers questions like 'to what extent is this argument generalizable beyond the five countries examined within these pages' systematically and in detail.

PART II introduces detailed empirical analysis across these five distinct countries in order to develop, illustrate, and test the utility and generalizability of my theoretical framework for cyber-defense capability and my argument for how, in the cyber era, mice roar. Chapters Four through Six examine how these five states sought to address critical interconnectedness in their cyber-defense postures and the degree to which they could and did leverage historical patterns of national defense in that effort. In addition to between case variation, this analysis illustrates important within case variation that is consistent with and provides greater nuance to the argument presented in Chapter Three. No single state has perfect overlap between their kinetic societal defense posture born from being small and precariously placed and the requirements of a societal cyber-defense posture given critical interconnectedness. And that disjuncture, though far smaller than that faced by the U.S., further illustrates the difficulties of pivoting and the degree to which existing institutions shape subsequent policy choices and implementations for better or for worse.

PART III moves away from the empirical realities of five countries' cyber-defense posture evolution and into a broader discussion of the contributions and opportunities stemming from this research. Chapter Seven finishes out the dissertation with a brief summary of the argument and empirical results and offers concluding thoughts and next steps. I lay out lingering questions for scholarship and policy that this project raises and identify critical areas for future research. This chapter will likely be of particular interest to policymakers or policy interested readers as it identifies persisting unknowns regarding national cyber-defense and conflict, details lessons learned for both the Mice that Roar as well as other countries building out their own cyber-defense capabilities moving forward, and speaks to the unique set of challenges the U.S. continues to face that shape its ability to adopt a societal defense posture to address national security concerns in the cyber era.

CHAPTER 2
Theoretical Foundations and the Argument:
When Solving for Critical Interconnectedness in the Cyber era, History Matters

We are always prepared to fight the last war.
– a well-worn proverb

1. Introduction

Given that the observable cyber-defense outcomes discussed in detail in the introductory chapter run counter to the conventional wisdom that larger, more militarily powerful states will be better positioned to provide national defense for their populations, what other factors could potentially explain why states such as the U.S. would punch below their weight and/or why a subset of smaller states appear to be punching above their weight in the cyber domain?

At its core, this research project hinges around two interrelated inquiries: (1) which factors underpin national cyber-defense capabilities and (2) which factors shape how successfully states adjust to the realities of national defense in the cyber era?

While there are no tailor-made theoretical explanations for why certain states have a higher state of readiness in cyberspace, there are several threads within international relations and security studies scholarship that can be drawn on to propose a series of potential factors and develop a theoretical framework. Identifying which factors affect the organization and efficacy of national cyber-defense capabilities is significantly aided by an understanding of the theoretical determinants of national defense capabilities in general.

In particular, Stephen Biddle's seminal work,[78] which focused on military capability, provides key insights into the examination of cyber-defense capability: namely, that while resources are one driver of military capability, those resources are mediated and structured through force employment (a military's doctrine and tactics) and that those patterns of force employment shape the utility of those resources in practice. While my research does not focus on the question of military capability, a similar logic holds for the evaluation of state's relative cyber-defense capability. We cannot accurately assess cyber-defense capability without taking seriously the defense strategies and the defense architectures that support those strategies in practice.

Notably, it is through an examination of the evolution of states' defense postures to include cybersecurity – strategies and the operationalization of those strategies – that reveals critical but previously overlooked variation between states cyber-defense capabilities. States are not starting from a blank conceptual or institutional slate. Nor are they able to instantaneously create mature security concepts and architectures from scratch. Defense postures are painstakingly built out over time. Critically, the conceptual and operational legacies states inherit from land, air, and sea can be maladapted for the realities of dependence on and the interconnectivity of cyberspace (taken together: critical interconnectedness).

[78] Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*.

This chapter proceeds in three parts before offering concluding thoughts. First, I establish a theoretical framework for thinking about national defense capability and its theoretical determinants. Second, I use this framework to assess cyber-defense capabilities. This section highlights which factors poorly explain why mice roar in the cyber era (potential competing explanations) and which provide greater analytic leverage (my argument). This second section also walks through the theoretical foundations underpinning why historical approaches can shape a state's development of cyber-defense capabilities, for better or for worse. Third, I flesh out societal defense problems as a parent category within which cyber-defense is merely one iteration. This section highlights the core features that societal defense problems share (kinetic or digital), outlines the ways in which cyber-defense presents a unique challenge in comparison to its historical predecessors, and explores six conceptual and operational features fundamental to societal defense in an era of cyber conflict.

2. Theoretical Background: National Defense Capabilities

National defense capabilities are primarily a function of two factors: (1) need and (2) capacity. In its simplest form, need is determined by the threats (or perceptions of those threats) that a given state faces while capacity is comprised of the resources (not limited to material factors) that a state can bring to bear in order to mitigate those threats. Significantly, although the preponderance of resources has been a prevailing focus of international relations and security studies scholarship, it remains only one aspect of state defense capacity. Equally important is the quality of those resources as well as the organization and deployment of those resources within a given defense architecture for a particular strategic purpose.

This sub-section is broken down into two parts: (1) a definition of national defense capability followed by (2) an examination of two central theoretical determinants, need and capacity.

2.1. Defining National Defense Capabilities

'National defense capability', sometimes assessed as readiness, refers to a country's ability or degree of preparedness to act in the event of a conflict or an attack. While this concept is frequently deployed in the context of military readiness[79] or combat readiness, "referring to the state of the armed forces and their related units to perform during military operations or other activities" in support of a national strategy,[80] ;national defense capability should instead be understood more broadly to include a country's military, economic, social, and political conditions that underpin a state's ability act in the event of conflict or crisis.

In order for states to effectively act in times of crisis, defense capability must be established and maintained in times of peace. A state cannot suddenly create these capabilities – including doctrine and tactics as well as the organizational structures, processes, and technology that underpins them – from whole cloth in times of need. They need to be invested in and developed over time. Moreover, when defense capability is being leveraged to prevent conflict or an attack from occurring in the first place, peacetime capabilities serve as credible signals[81] of state capability in the event of crisis. For

[79] For a more detailed discussion of military readiness, including its operational and structural dimensions, refer to Richard Betts, *Military Readiness: Concepts, Choices, and Consequences* (Brookings Institution Press, 1995).
[80] Makridis and Smeets, "Determinants of Cyber Readiness." p2.
[81] Ben Buchanan identified two core approaches to the more competitive aspects of statecraft – shaping and signaling. Shaping seeks to alter the conditions under which states are competing to their advantage (to change the state of play) while signaling seeks to influence adversary state behavior by credibility demonstrating capability (to change the information an adversary has available to it when make decisions). Buchanan notes that while much of international relations and security studies research has focused on signaling, far less has focused on shaping. Of particular importance to this research project, both of these approaches can occur below

example, the ability to act in a time of crisis underpins deterrence strategies in both theory and practice.[82]

Yet, security comes at a cost. It is merely one of many important policy objectives competing over limited resources.[83] Resources spent on security cannot also then be spent again on other policy objectives such as education, healthcare, etc. Independent of resource expenditure, prioritizing security may also require deliberate tradeoffs between other core goals within a society such as economic growth, business competitiveness, efficiency, and privacy. As a consequence, national defense capabilities are the result of a series of choices and tradeoffs made by policy makers, military commanders, industry players, and the general public. These choices and tradeoffs correspond, in aggregate, to a national defense posture: national defense strategies and the operationalization of those strategies.

Crucially, national defense capability should not be conflated with the concept of state power. Whereas the former centers on defensive capabilities, power encompasses both defensive and offensive capabilities as states seek to influence and resist the influence of other states at home and abroad. Importantly, the focus of this research, and the focus of early efforts to measure national cyber-defense capabilities across states, is on the defensive aspects of national security. These aspects focus on 'defense of the homebase'[84] rather than a discussion of the theoretical determinants of cyber power more broadly.[85] However, just as power is a relative term (defined in relationship to other states' power), defense capability is as well.

In addition, while some states conceptualize offensive operations as a core component of national defense (e.g. Israel's defense posture, which centers offensive deterrence and preemption), this dissertation is not primarily concerned with the integration of cyber capabilities into military operations and tactics (i.e. the development, proliferation, and deployment of cyber weapons) or as a tool of statecraft more broadly. Rather, it focuses on how states address cyber-enabled malicious activity directed at their homebase or in the context of conflict centered on defending that same homebase. Discussions of offensive cyber capabilities more broadly speak to aspects of state competition and national security concerns beyond defense of the homebase, such as questions of compellence as well as the ability to shape others' policy decisions and the international environment in your favor.[86] These aspects of offensive cyber operations, therefore, lay outside the scope of this project.

the threshold of armed conflict while also reducing the likelihood of potential of conflict as well as a state's likelihood of winning if conflict were to break out. Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. p3.

82 For example, what Joseph Nye coined as "deterrence by denial" as well as "deterrence by punishment" are both the product of peacetime capabilities that serve as a credible signal for capabilities in the instance of conflict or attack. Nye Jr, "Deterrence and Dissuasion in Cyberspace."

83 David A. Baldwin, "The Concept of Security," *Review of International Studies* 23, no. 1 (1997): 5–26.

84 'Defense of national territory" is an analogue to this term within the context of armed conflict use by Stephen Biddle in his book *Military Power*. However, within the context of cyber conflict, it is important to recognize that defense of the homebase or national territory includes more than just the physical boundaries of the state but also the people, institutions, activity, etc. that occurs within that territory and underpins the daily functioning of the state and its society.

85 For research instead focusing on cyber power and influence, refer to Kuehl, "From Cyberspace to Cyberpower: Defining the Problem."; Kramer, Starr, and Wentz, *Cyberpower and National Security*.; John B. Sheldon, "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.*, ed. Derek Reveron (Georgetown University Press, 2012).; and Adam Segal, *Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (Public Affairs, 2016).

86 Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*.

2.2. Theoretical Determinants of National Defense Capabilities

What factors determine variation in states national defense capabilities? National defense capabilities have traditionally been understood as a function of two factors: (1) need and (2) capacity. In its simplest form, need is determined by the threats (or perceptions of those threats) that a given state faces while capacity is comprised of the resources (not limited to material factors) that a state can bring to bear in order to mitigate those threats.

2.2.1. Need

In addition to the role national defense capabilities play in state power more broadly, need as a determinant of national defense capabilities is driven by the character of threats states face. Importantly, states react not to some objective measure of threat but their perceptions of those threats. As a consequence, it is threat perception that "is the decisive intervening variable between action and reaction in international crisis" and likewise decisive in why states pursue specific types of defense capabilities.[87]

Perceived need, in its most basic form, is a risk calculation and can be broken down into two set of variables: (1) vulnerabilities and (2) the likelihood and cost of those vulnerabilities being exploited by a potential adversary in the future. Vulnerability includes considerations such as the limitations of geography (e.g. lack of strategic depth), the absence of core resources (e.g. natural resources, population size, GDP, etc.), critical dependence on a set of resources (e.g. transportation, ICT technology, etc.), and/or dominant technological facts of the battlefield or domain of conflict (e.g. increasing lethality). In contrast, the likelihood of these vulnerabilities being exploited hinges on a state's broader geopolitical environment (e.g. potential rivals or peer competitors). For example, many states lack short-range counter-rocket, artillery, and mortar (C-RAM) weapons systems. Yet for many of those same states, their neighbors, if perceived as adversaries at all, are unlikely to deploy short-range rockets, artillery, or mortars against them in the future. In contrast, Israel developed and deployed the Iron Dome defense systems in order to address this vulnerability by intercepting rocket attacks from Hezbollah in southern Lebanon and Hamas in Gaza.[88]

Need is only one factor shaping the character and effectiveness of states' national defense capabilities. The question then becomes, how do states seek to mitigate the perceived threats they face? To answer this question, we must consider the capacity of states to meet that need.

2.2.2. Capacity

Significantly, although preponderance and, to a lesser extent, quality of resources have been a prevailing focus of international relations and security studies scholarship,[89] resources remain only one aspect of states' defense capacity. Equally important is the state's defense posture – the organization and deployment of those resources within a given defense architecture in order to put states' national defense strategy into practice.

Resource based determinants of national defense capacity have two broad flavors: (1) those that center around the preponderance of resources and (2) those that center around the quality of those resources.

87 Raymond Cohen, "Threat Perception in International Crisis," *Political Science Quarterly* 93, no. 1 (1978): 93.
88 Ellen Ioanes, "The US Military Is Buying Israel's Battle-Proven Iron Dome That Destroys Rockets. Here's How It Works," *Business Insider*, August 15, 2019.
89 For a more detailed discussion of the components of state power, refer to Joseph S. Nye Jr, *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone*, Kindle Edition (Oxford University Press, 2003).

In terms of preponderance, many believe that states with larger populations, larger or more industrialized economies, and/or larger militaries or greater military expenditures should be better positioned to provide security for their populations. This association of defense capability with measurements of relative size also underpins traditional treatments of power in international relations more broadly.[90] While some of these arguments rely on numerical superiority alone as the primary determinant of power in general and defense capabilities in particular, others introduce more nuance to the assessment of material factors such as the benefits of 'force density' rather than purely 'force size'[91] and theories of a defender's relative advantage.[92] Yet, as Biddle points out, "[w]hile specialists debate the proper counting rules, both the public debate and the scholarly literature thus rely heavily on simpler measures of gross preponderance per se: the greater A's numerical superiority over B, the greater its relative capability."[93]

In terms of resource quality, arguments focus not just on numerical strength but additional factors that shape the relative utility of each unit. Literature that falls into this approach of assessing defense capability include efforts to move away from measures such as troop numbers and toward quality-adjusted "combat power"[94] as well as assessment of technological superiority though an evaluation of the relative technology holdings of various states.[95] Significantly, while in some instances this aspect of state defense capabilities may be used to overcomes shortcomings in preponderance, what one Israeli military official referred to as overcoming quantity with quality,[96] it can also bolster the existing relative numerical strength of a state. Notably, in most models of capability that include some measure of quality, capability is driven by some combination of resource quality and preponderance.[97]

Materially deterministic treatments of national defense capability continue to dominant the literature and theoretical frameworks in general. International relations theory has mostly overlooked alternative drivers of national defense capability since "[m]any, [consistent with the rational choice literature],[98] assume that states will use materiel "optimally", hence the materiel itself is the only important variable" in their theoretical models and data collection.[99] Importantly, resource-based determinants capture only part of the overall national defense capability of states and overlook other important theoretical and empirical determinants.[100]

90 Stephen Biddle points out that this dominant approach to capability underlies large swaths of international relations and security studies scholarship, ranging from hegemonic transition theory to the balance of power and from long range threat assessments to the relative gains that stem from international cooperation. See Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*. loc. 441.
91 Refer specifically to Basil Liddell Hart, "The Ratio of Troops to Space" *Military Review* 40 (April 1960).
92 Refer to John J. Mearsheimer, "Assessing the Conventional Balance: The 3:1 Rule and Its Critics," *International Security* 13, no. 4 (1989): 54–89 as an example.
93 Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*. loc. 467.
94 As an example, refer to Basil Henry and Liddell Hart, *The Defence of Britain* (Praeger, 1980). and Mearsheimer, "Assessing the Conventional Balance: The 3:1 Rule and Its Critics."
95 Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*. loc. 488.
96 Author's Interview, 2019.
97 Take Lanchester theory as an example. Lanchester theory sought to predict the outcomes of aerial dogfights in the first World War using a combination of preponderance and technology. Refer to F.W. Lanchester, *Aircraft in Warfare: The Dawn of the Fourth Arm*, Kindle Edition, 2011.
98 A central tenant of rational choice theory is that states select their actions because they are seen as value-maximizing means for achieving their objectives.
99 Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*. loc. 537.
100 Other issues that have been introduced as shaping a state's defense capabilities include morale, leadership, motivation, and domestic political concerns. However, while these factors have appeared in policy assessments/analysis and within historical studies, these variables have been treated fairly unsystematically rather than incorporated into a broader theoretical framework for defense capability outcomes.

A particularly noteworthy exception to this trend is the work of Biddle on the determinants of military power.[101] He focused his analysis on "force employment, or the doctrine and tactics by which armies use their materiel in the field", and demonstrated how a particular pattern of force employment was pivotal to assessing military capability in the twentieth century.[102] Significantly, Biddle's work moved theoretical frameworks of military capability away from the prevalent approach of counting and assessing military assets and toward the inclusion of (a) asset deployment and structure and (b) the ability of that deployment and structure to reduce a state's vulnerability to the realities of twentieth century weapons and sensors. Although his research speaks specifically to the determinants of military power, it sheds important light on the determinants of national defense capabilities more broadly by systematically addressing the importance of purpose, process, and structure in our models of capability.

2.3. Conclusion

The myriad of factors that shape a state's relative defense capability rely predominantly on two sets of drivers: the need and the capacity of a state to mitigate that need. Orthodox approaches for assessing state capacity have focused heavily on the preponderance or type of resources that states have at their disposal. This orthodoxy underpins the first puzzle presented in the introduction to this dissertation – why are relatively small states, with comparatively limited resources, outperforming or keeping pace with the far larger U.S. in early cyber-defense capability assessments? Yet, an important portion of the answer lies in the recognition of the second puzzle – why does the delta between existing defense postures and the requirements of a cyber-defense posture vary across states? Importantly, resources are only one component of state capacity. The defense strategies states adopt and the processes and structures they put into place in pursuit of those strategies are often overlooked but equally as important for assessing defense capability and variation in states' ability to address the security threats they face.

3. Explaining Variation in Cyber-Defense Capabilities

In the prior section of this chapter (section 2), I established a theoretical framework for thinking about national defense capability and its theoretical determinants. Now, in this section, I place the observable outcome - small states as leaders in cyber-defense capability - into direct conversation with that theoretical framework to present my argument and to highlight which factors poorly explain why mice roar in the cyber era and which provide greater analytic leverage.

3.1. Assessing Potential Determinants of National Cyber-Defense Capabilities

The remainder of this sub-section assesses potential explanations for why these relatively small countries, with comparatively limited resources, became significant providers of national cyber-defense for their populations ranking alongside far larger regional and global powers like the U.S. This assessment includes and concludes with my argument, placing it in direct conversation with the theoretical framework presented above.

3.1.1. Need

Need can be broken down into three components: the technical realities of the defense problem states face in the cyber era, the degree to which states are vulnerable to those realities, and their perceptions of their vulnerability. Despite the nature of the defense problem states face, variation in

[101] Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*.
[102] Biddle. loc. 165.

need does not adequately explain why the U.S. appears to be underperforming and a sub-group of relatively small countries overperforming.

Critically, if militaries needed to solve for increasing lethality in the twentieth century,[103] states now need to solve for critical interconnectedness in the twenty-first. The defense problem of increasing critical interconnectedness now facing states is the product of two overlapping but distinct dynamics: their dependence on and the interconnectivity of cyberspace. The former dynamic stems from the activity occurring on or through cyberspace while the latter is a feature of the terrain itself. Notably, unlike the domains of air, land, and sea, cyberspace is simultaneously a manmade terrain and a domain through which human activity traverses. This domain of conflict and state competition is built, maintained, and advanced by humans, many if not most of which are currently sitting within industry rather than government.

In terms of dependence, there is a national security imperative in cyberspace given how cyberspace underpins the daily functioning of advanced industrial economies. Today, cyberspace – "a network of networks and devices (and the users behind them) through which information is stored, shared, and communicated online"[104] – is central to how economies compete; individuals, and communities communicate; and states provide security for their populations. It underpins our electricity grids, healthcare systems, communication networks, banking and financial services, commerce, as well as the ways our militaries fight and our governments gather intelligence. As a consequence of this dependency, U.S. Deputy Secretary of Defense, William Lynn argued that "[in] the 21st century, bits and bytes can be as threatening as bullets and bombs."[105]

The far-reaching impact of cyberattacks and insecurity due to this dependency is not merely theoretical. Awareness of this 5th domain of conflict has only increased in the past few years. Cyber operations have become an ever increasing and sophisticated part of state competition and conflict as "[h]ackers wiretap, spy, alter, sabotage, disrupt, attack, manipulate, interfere, expose, steal, and destabilize" for strategic and tactical gain.[106] In 2016 alone, often spoken of as a critical turning point for cyber conflict, we publicly witnessed incidents in numerous critical sectors globally: communication (Deutsche Telecom and Yahoo), democratic institutions (the U.S.' Democratic National Committee and the Philippines' Commission on Elections), energy (the power grid in Ukraine), financial services (the Central Bank of Bangladesh and Tesco Bank), healthcare (the Australian Red Cross and National Health Service Hospitals in the UK), IT services (domain name provider Dyn), and security (the FBI and Homeland Security in the U.S.).[107] States and non-state actors have utilized cyber operations for a wide range of purposes including espionage (e.g. U.S. intelligence gathering to ascertain the goals, concerns, and negotiating positions of UN Security Council members regarding potential sanctions on Iran in 2010),[108] to disrupt essential services (e.g. Russian hackers shutting down the Ukrainian power grid in 2016),[109] to inflict physical damage (e.g. Stuxnet, a destructive computer worm designed to undermine the Iranian nuclear program by

[103] Biddle.
[104] Singer and Friedman, *Cybersecurity: What Everyone Needs to Know*. loc. 325.
[105] Cheryl Pellerin, "DOD Releases First Strategy for Operating in Cyberspace," *American Forces Press Service*, July 14, 2011.
[106] Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. loc. 159.
[107] EPSC Strategic Notes, "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level," *European Political Strategy Centre*, no. 24 (2017). p2.
[108] Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. loc. 202-255.
[109] Walters Riley, "Russian Hackers Shut Down Ukraine's Power Grid," *Newsweek*, January 14, 2016.

secretly setting Iran's nuclear centrifuges to dangerously high speeds in 2010),[110] or to destabilize countries (e.g. Russian interference in the 2016 and 2020 U.S. elections).[111]

Although we have not witnessed a cyber Pearl Harbor, cyber 9/11, or civilization-ending cyberwar that animating some of the early imaginings, advanced industrial economies remain heavily dependent on cyberspace and that dependence makes cyberspace a now tried and tested tool through which malicious actor can degrade, disrupt, destroy, or defray the critical day-to-day functioning of society and the state. These trends in cyber operations are only increasing, making the need for robust cyber-defense capabilities an indelible part of international and domestic politics.

In terms of interconnectivity, cyberspace as a terrain is a web of connections, a network of networks and devices. This interconnectivity provides malicious actors with previously unheard-of opportunities for access and raises concerns about back doors, cascading effects, single points of failure, and contagion across and within sectors but also within and between countries.

In the midst of armed conflict between Russia and Ukraine, it was interconnectivity that made it possible in 2017 for the Russian hacker group known as Sandworm to leverage the hijacked update servers of Linkos Group - a small, family-run Ukrainian software business - to establish a hidden back door into thousands of PCs. Sandworm used this back door to release a piece of destructive malware that was designed to spread automatically, rapidly, and indiscriminately.[112] It did so throughout Ukraine and out into the infrastructure of the modern world. As Andy Greenberg, the author of *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*[113] and a senior writer for WIRED explained:

> Within hours of its first appearance, the worm raced beyond Ukraine and out to countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania. It crippled multinational companies including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser. In each case, it inflicted nine-figure costs. It even spread back to Russia, striking the state oil company Rosneft.[114]

NotPetya, leveraging the interconnectivity of cyberspace, was responsible for more than $10 billion in total global damages and a wave of screens around the world rapidly turning black.[115] It inflicted significant costs at speed.

Critical interconnectedness – states dependence on and the interconnectivity of cyberspace – is only likely to get worse. Take for example, the development and deployment of 5G, the "fifth generation" of mobile network technology. As I have previously argued, 5G will enable activity throughout society including but not limited to finance (e.g. mobile services), urban development and planning (e.g. smart cities), and transportation (e.g. driverless cars).[116] As Meredith Atwell Baker summarized, "5G is the platform for tomorrow's economy."[117] Its importance does not stop with

110 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014.
111 Matt Laslo, "Russia Is Going to Up Its Game for the 2020 Elections," *Wired*, July 31, 2019.
112 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018.
113 Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Kindle Edition (Doubleday, 2019).
114 Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History."
115 Greenberg.
116 Melissa K Griffith, "5G and Security: There Is More to Worry About than Huawei," *Wilson Center Policy Brief*, 2019. p5.
117 Ahiza Garcia, "Who's Winning the 5G Race?," *CNN*, April 2, 2019.

economic and social activity; even military operations will be reliant on the security and resilience of the networks and devices in place.[118] As potentially one of the most important networks of the 21st century, 5G is the very definition of high levels of dependency on a deeply interconnected ecosystem.

In sum, critical interconnectedness has two broad implications for states' national security. First vulnerability is more pervasive and dispersed across the state and second, there are a wider range of actors that are targets, first responders, collateral damage, innovators, and points of failure. As a consequence, the capacity to respond to cyber operations is dispersed across the entire society – the government, the private sector, and the citizenry.

Given the nature of the defense problem states face, could variation in need (the level or perception of the cyber threat states face) account for the specific assortment of leaders emerging in cyber-defense capability assessments?

For need to be sufficient in explaining why the U.S. appears to be punching below its resource weight and/or why the Mice that Roar appear to be punching above theirs, we would expect to see an inverse relationship between resources and need. In short, the U.S. did not invest its resources in cyber-defense because it did not face a security threat in this domain. This need-based theory would predict that the U.S. with its significant resource advantage should either be less dependent on cyberspace or not perceive the vulnerabilities that dependence entails. Neither of these explanations, however, are consistent with the facts.

Empirical trends are not consistent with a theory of low relative need leading the U.S. not to invest resources and therefore, subsequently, appear to underperform given its size. Importantly, Makridis and Smeets in their 2019 article found that while variation in need correlates with variation between those states with low readiness scores and those states that appear to be ahead of the curve with high readiness scores, those states that are ahead of the curve are more likely to face "a more threatening security environment" and be "highly dependent on cyberspace".[119] Advanced industrial economies are heavily dependent on cyberspace, as previously discussed, and the leaders in cyber readiness face a security environment in which potential rivals have incentives to exploit that dependency.

However, even if need is fairly consistent across these leading states, their recognition of the threat may vary. If this were the case, we would expect to observe low perceptions of threat within the U.S. However, the importance of cyberspace and the risks associated with its widespread use has not gone unnoticed. and spans presidential administrations. As early as 2003, President George W. Bush argued that, "[s]ecuring cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society--the federal government, state and local government, the private sector and the American people".[120] In May of 2009, President Barack Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."[121] Notably, his efforts directly built on President George W. Bush's

[118] Griffith, "5G and Security: There Is More to Worry About than Huawei."
[119] Makridis and Smeets, "Determinants of Cyber Readiness." p2.
[120] Robert Lemos, "Bush Unveils Final Cybersecurity Plan," *CNET*, November 13, 2003.
[121] "Text: Obama's Remarks on Cyber-Security," *New York Times*, May 29, 2009.

2008 Comprehensive National Cybersecurity Initiative (CNCI).[122] In 2011, U.S. Deputy Secretary of Defense, William Lynn, pointed to the inevitability of cyber conflict, arguing that the "centrality of information technology to our military operations and our society virtually guarantees that future adversaries will target our dependence on it".[123] He went on to say that, "Our assessment is that cyber attacks will be a significant component of any future conflict, whether it involves major nations, rogue states or terrorist groups".[124] Obama's Director of National Intelligence, James Clapper, echoed this sentiment when he ranked cyberattacks at the top of his list of threats faced by the U.S. during a 2015 Congressional testimony to the Senate Armed Services Committee.[125] In a 2019 testimony to Congress on "Threats to the Homeland", President Donald Trump's Department of Homeland Security (DHS) Secretary Kirstjen Nielsen argued that although the DHS was created post-9/11 to address terrorism, "I believe an attack of that magnitude is now more likely to reach us online."[126] In short, across administrations, we observe a recognition of the severity of the threat the U.S. faces in an era of cyber conflict rather than the low perceptions of threat that an argument hinging off 'low perception of need' would require.

Therefore, while dependence on cyberspace and the broader security environment of states provides analytical leverage for why some states have relatively poor capability and others relatively strong capability, these factors do not vary meaningfully within those states demonstrating relatively strong capability. Moreover, while the U.S.'s perceived underperformance could be driven by a lack of recognition of the threat by the largest military power, the U.S. has consistently elevated this concern as one of the most pressing security issues facing the country.

In conclusion, if variation in need were the central reason for why the U.S. appears to be underperforming and relativity small states appear to be overperforming, we would expect to see these smaller states experiencing and recognizing far higher need than the U.S. This, however, is not the case. Given the persisting defense problem of critical interconnectedness facing all states, this leaves us to turn our attention to factors related to capacity.

3.1.2. Capacity

Given the defense problem states face and the limitation of need as a potential explanation for why mice roar in the cyber era, this section turns its attention to two core components of state capacity: potential variation in the resources they have at their disposal and their cyber-defense postures. Although resources-based explanations have dominated the canonical literature, they do not provide sufficient analytical leverage for explaining the puzzle that motivates this dissertation. Instead, it is how states structure and deploy their resources that provides theoretical leverage that is consistent with observed outcomes.

The puzzle motivating this research itself stands in stark contrast to resource-based theories. The U.S. ranked 2nd globally with an estimated GDP of $19.49 trillion in 2017. In sharp contrast, Estonia's estimated GDP was $41.65 billion, bringing it in at 157th globally. Coming in higher than Estonia but still far below the U.S., Finland's estimated GDP was $244.9 billion, Israel's $317.1

122 "The Comprehensive National Cybersecurity Initiative," The Obama White House Archives, 2008, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.
123 Pellerin, "DOD Releases First Strategy for Operating in Cyberspace."
124 Pellerin.
125 Guy Taylor, "James Clapper, Intel Chief: Cyber Ranks Highest on Worldwide Threats to U.S.," *The Washington Times*, February 26, 2015.
126 Breanne Deppisch, "DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump.," *Politico*, December 18, 2019.

billion, and Singapore's $528.1 billion.[127] These observations are consistent with work of Makridis and Smeets, who found that resources (primarily GDP) was not a good predicator of Global Cybersecurity Index (GCI) rankings.[128] In terms of military resources (excluding cyber resources), the U.S. topped the Global Firepower Index[129] in 2019, ranking 1st out of 137 countries. Israel came in at 17th, Singapore 59th, Finland 63rd, and Estonia 112th. This trend continues with assessments of population, another variable often used in preponderance calculations as a measure for the upper limits of troop and work-force size. As of 2018, the U.S. had the 3rd largest population globally while Israel fell at 98th, Singapore 112th, Finland 117th, and Estonia 157th.[130]

Even if we expand our evaluation of resources to include those specific to the cybersecurity sector, resources continue to vary widely. The North American market, primarily driven by the U.S., comprises over half of global spending on cybersecurity[131] and more broadly, the Big Five tech giants (Alphabet, Amazon, Apple, Facebook, and Microsoft) are all American companies.[132] These are two stark realities that have not been overlooked by other states.[133] Even when we look at look more narrowly to cybersecurity assessments of resource quality, the U.S. once again tops the charts. In Cybersecurity Venture's rating of the 500 most innovative cybersecurity firms in 2018,[134] 350 out of 500 firms were American. Israel came in at second place with only 42 firms. Estonia didn't have a single firm that made the list while Finland and Singapore had two firms each.

In short, amongst the states that are ahead of the cyber-defense capability curve, resources vary significantly and the U.S. maintains a strong and largely universal resource advantage. If resources were the main drivers of cyber-defense capability, the U.S. should significantly outperform these relatively small states. Yet, it has not yet done so. Why?

Resources need to be organized and deployed in response to the realities of the specific defense problems states face. This requires us to differentiates between (a) technical or industry resources and expertise and (b) the operational and strategic components of national cyber-defense efforts. The latter two, which taken together comprise a state's defense posture, are core mechanisms through which states can leverage existing technological capacity and competency into society writ large in a manner that protects both civilian and government use of cyberspace. In sum, there is an important distinction between the presence of potential resources and the effective deployment of those resources throughout industry, government, and the broader civilian population for national defense purposes.

States' cyber-defense postures are simultaneously intuitively important and yet largely overlooked in the emerging cyber conflict literature. While there is widespread policy and academic recognition of

127 GDP (purchasing power parity) figures are from the CIA World Factbook and represent 2017 estimates.
128 Makridis and Smeets, "Determinants of Cyber Readiness."
129 The Global Firepower index assessments focus on states war-making potential through conventional means in air, land, and sea. You can find these ranking and more detailed information on how they are calculated at "Global Firepower - 2020 World Military Strength Rankings," accessed July 18, 2020, https://www.globalfirepower.com/.
130 Population figures are from the CIA World Factbook and represents 2018 estimates.
131 "Cybersecurity Market Report," Cybersecurity Ventures, 2016, https://cybersecurityventures.com/cybersecurity-market-report-test/.
132 For a more detailed analysis of the American ecosystem and corresponding industrial policies see Vinod K. Aggarwal and Andrew W. Reddie, "Comparative Industrial Policy and Cybersecurity: The US Case," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 445–66.
133 Griffith, "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity."
134 The 500 most innovative cybersecurity firms in 2018 was compiled by Cybersecurity Ventures and can be located at "500 Most Innovative Cybersecurity Firms in 2018," Cybersecurity Ventures, 2018, https://cybersecurityventures.com/.

the importance of leveraging all of society for the defense of the state in the cyber era, little attention has been paid to explaining how this effort fits into a broader theoretical framework of cyber-defense capability or why we see widespread variation in the organization and effectiveness of states' attempts to implement such a posture in practice.

What factors then explain why states vary in their ability to adopt a societal defense posture? The evolution and maturity of defense postures could merely be a question of time. First movers could have higher relative cyber-defense capability because they have had more time to adjust to the changing threat landscape (the disjuncture) and to evolve defense postures that address that reality. Recall, defense postures do not appear out thin air. They have startup costs and require sustained investment and political support.

However, if timing were sufficient to explain variation in the ability of states to develop a defense posture, we would expect the composition of this group of leaders to be primarily early movers. These states would be among the first to recognize this new threat and to begin the process of building out a subsequent defense-posture to address that threat. Yet, while Israel and the U.S. could be categorized as early movers, the same could not be said of Finland who first topped a ranking in 2012 and 2013, the same years they launched their working group followed by their first cybersecurity strategy, or Singapore who rose to the top of a ranking in 2017 beating out the U.S. for the top spot[135] only a few years after the ink on their first cybersecurity strategy had dried.[136]

Ultimately, it is history that takes on a unique importance for the organization and effectiveness of states cyber-defense capability. Rather than frame cyber-defense as a novel type of defense problem facing states, I argue that cyber-defense is best understood as a kind of "societal defense problem". States facing a societal defense problem have adopted a variety of societal defense postures: structure national defense in a manner that does not rely on military or intelligence agencies as the sole or even primary defense actors while simultaneously integrating both public and private actors into a cohesive, real-time national defense posture.

Significantly, this framing provides analytical leverage for the second puzzle introduced at the beginning of this dissertation: why is cyber-defense seen as a less revolutionary defense problem by some countries. When understood as a societal defense problem, cyber-defense does not entirely represent a complete departure from the core requirements of national defense in the domains of air, land, and sea. Relatively small states in imperiled geo-strategic environments, for example, have historically pursued variations of a societal defense posture: leveraging all of society for the defense of the state in response to perceived widespread vulnerability across the homebase stemming from an external threat. In the case of the Mice that Roar, those pre-existing kinetic national defense approaches – in some instances their strategic concepts as well, but across cases their approach to operationalizing those concepts - have provided a conceptual and operational foundation upon which to build out national cyber-defense capability that addresses the national security reality of critical interconnectedness in the cyber era.

135 Tom Brant, "Singapore Tops U.S. for Best Cybersecurity," *Entrepreneur*, July 6, 2017.
136 Finland first began to develop their cyber-defense posture in the late 2000s and early 2010s as compared to Israel, which began in the late 90s and early 2000s. The U.S., like Israel, began its policy development in late 90s and early 2000s. Singapore, began to develop their cyber-defense posture in the mid-2010s.

Recall, one of the fundamental realities of the defense problem states face in cyberspace is critical interconnectedness. As a consequence, as President Bush noted, cyber-defense represents an "extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society--the federal government, state and local government, the private sector and the American people".[137] Yet, for a subset of relatively small states, conventional (or kinetic) national defense also represented an extraordinarily difficult strategic challenge that required a coordinated and focused effort from their entire society - the government, the private sector, and the citizenry. In adopting defense postures to solve for their geostrategic vulnerability, these states coincidently developed defense postures that overlap with the solution sets states are now pursuing in the cyber era. In other words, by solving for significant vulnerability, these states also solved, in part, for critical interconnectedness.

Existing patterns of policy influence subsequent patterns of policy. Within political science more broadly, both the historical institutionalism and path dependence literatures highlight the role that history plays in shaping current and future policy decisions, e.g. existing institutions can be sticky and constrain subsequent efforts.[138] In a more limited sense, the impact of historical legacies has also begun to be addressed within cybersecurity scholarship more broadly as emerging research points to the ways in which existing domestic policy patterns have influenced emerging cyber-policy patterns. Take for example, the 2018 special issue in the Journal of Cyber Politics organized by Vinod K. Aggarwal and Andrew Reddie analyzing motivations for industrial cyber-policy.[139] Through a collection of case-studies on China,[140] the EU,[141] Finland,[142] France,[143] Japan,[144] Taiwan,[145] the U.K.,[146] and the U.S.,[147] the combined articles illustrate how countries utilized various types of industrial policy in order to address specific cybersecurity market failures such as skills shortages/education and research and development (R&D). In particular, my article on Finland in this special issue explicitly argues that Finland extensively leveraged its historical logic for and approach to marketcraft in its efforts to address cybersecurity market failures. In other words, Finland largely used institutional inertia to its advantage when possible and then departed from

137 Lemos, "Bush Unveils Final Cybersecurity Plan."
138 For examples of work on how historical institutions and policies have influenced the development of and approach to subsequent issues refer to Steven D. Krasner, "Approaches to the State: Alternative Conceptions and Historical Dynamics," *Comparative Politics*, no. 16 (1984): 223–246.; Peter A. Hall, "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain," *Comparative Politics* 25, no. 3 (April 1993): 275; Paul Pierson, "When Effect Becomes Cause: Policy Feedback and Political Change," *World Politics* 45, no. 4 (July 1993): 595–628; Peter A. Hall and Rosemary C. R. Taylor, "Political Science and the Three New Institutionalisms," *Political Studies* 44, no. 5 (December 1, 1996): 936–57; Kathleen Thelen, "Historical Institutionalism in Comparative Politics," *Annual Review of Political Science* 2, no. 1 (June 1999): 369–404; Paul Pierson, "Increasing Returns, Path Dependence, and the Study of Politics," *American Political Science Review* 94, no. 2 (June 2000): 251–67; Paul Pierson, "The Limits of Design: Explaining Institutional Origins and Change," *Governance* 13, no. 4 (October 1, 2000): 475–99; and Guy B. Peters, *Institutional Theory in Political Science* (London: Continuum, 2001).
139 Vinod K. Aggarwal and Andrew W. Reddie, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 291–305.
140 Tai Ming Cheung, "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 306–26.
141 Paul Timmers, "The European Union's Cybersecurity Industrial Policy," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 363–84.
142 Griffith, "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity."
143 Danilo D'Elia, "Industrial Policy: The Holy Grail of French Cybersecurity Strategy?," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 385–406.
144 Benjamin Bartlett, "Government as Facilitator: How Japan Is Building Its Cybersecurity Market," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 327–43.
145 Hsini Huang and Tien-Shen Li, "A Centralised Cybersecurity Strategy for Taiwan," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 344–62.
146 Madeline Carr and Leonie Maria Tanczer, "UK Cybersecurity Industrial Policy: An Analysis of Drivers, Market Failures and Interventions," *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 430–44.
147 Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: The US Case."

historical legacies only when necessary and with some difficulty. Though not the explicit focus of this special issue more broadly, throughout the country-specific analyses readers can find examples of when various aspects of states' industrial cyber-policy paralleled historical patterns of industrial policy.

There are two broad, non-mutually exclusive pathways identified within the broader political science literatures through which history shapes present and future outcomes. First, states, facing a similar policy challenge prefer to adopt similar policy responses, but existing ideas, resources, and institutions constrain how quickly or effectively they can do so.[148] Second, when facing new environments or threats, states formulate their policy responses depending on the tools – ideas, resources, and institutions - available to them.[149] One important consequence of both of these mechanisms, however, is that the more emerging policy imperatives diverge from existing policies or require new instruments to operationalize those policies, the more difficult those policies will be to formulate and implement. In contrast, the more emerging policy imperatives overlap with existing policy legacies and instruments, the easier those policies will be to formulate and implement. In other words, the more emerging policy imperatives overlap with prior policy imperatives, the better.[150]

Notably, while historical legacies play a role in all five of the countries examined in this dissertation, the consequences of those institutional legacies vary. In sharp contrast with the experience of the U.S., when it comes to addressing critical interconnectedness, these smaller states' conventional defense patterns served primarily not as a constraining force that led to the use of national defense approaches that were largely maladapted to cyber-defense's realities, but instead as an important operational, and sometimes strategic, bedrock from which to build.

4. Societal Defense Problems: Placing Cyber-Defense into Historical Context

Recall, I argue that national cyber-defense is best understood not as an entirely novel defense problem now facing states but as a kind of "societal defense problem": a national security threat where (1) the vulnerabilities are society-wide, embedded within the functioning of civil society, government, and the economy and (2) the resources states need to deploy in order to prevent an attack, defend against an ongoing attack, or recover from a previous attack are largely housed outside the military and even the government itself, i.e. within industry and the civilian population. Therefore, in order to address the core pressing national security concern facing states seeking to

148 For examples of work addressing this mechanism, refer to Jeffrey W. Taliaferro, "State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State," *Security Studies* 15, no. 3 (July 2006): 464–95 and Tom Dyson, "Convergence and Divergence in Post-Cold War British, French, and German Military Reforms: Between International Structure and Executive Autonomy," *Security Studies* 17, no. 4 (2008): 725–74.

149 For examples of work addressing this second mechanism, refer to Margaret Weir and Theda Skocpol, "State Structures and the Possibilities for 'Keynesian' Responses to the Great Depression in Sweden, Britain, and the United States," in *Bringing the State Back In*, ed. Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge University Press, 1985): 120-125.; G. John Ikenberry, "The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s," *International Organization* 40, no. 1 (1986): 105–37; and Peter J. Katzenstein, "Same War - Different Views: Germany, Japan, and Counterterrorism," *International Organization* 57, no. 4 (2003): 731–760.

150 Paul Pierson builds off economics path dependences scholarship focused on the dynamics of industry and form lock-in by identifying how certain political realities make it harder to disrupt historical policy legacies: institutional density of politics (which make institution formation and cessation more difficult); power asymmetries (which allows actors to employ their authority in ways that enhance their own power); complexity/opacity (which makes learning difficult and increases transaction costs); short time horizons (shifting paths is typically costly in the short term making it unavailable as politicians prefer short-term payoffs); and prevalent status-quo bias in political institutions. For more information, see Pierson, "Increasing Returns, Path Dependence, and the Study of Politics."

provide defense for their populations in the cyber era (what I refer to as 'critical interconnectedness': their dependence on and the interconnectivity of cyberspace), states must structure national cyber-defense in a manner that does not rely on military or intelligence agencies as the sole or even primary defense actors while simultaneously integrating both public and private actors into a cohesive, real-time national defense posture.

Placing national cyber-defense within this broader category of defense problems appropriately frames cyber-defense and cybersecurity less as a predominantly path-breaking topic and, more appropriately, within the bounds of historical experiences of national security. This is not to say that cyber-defense is identical to prior kinetic societal defense problems that states have faced. There are important differences between historical experiences and this emergent domain of conflict. However, it does share core features with various kinetic iterations of societal defense problems that are worthy of note and examination.

4.1. Historical Forms of Societal Defense Problems

Historical forms of societal defense problems have been rooted in vulnerability born from a state's geostrategic environment: an existential threat to the homebase. In an effort to mitigate that threat states have sought to bolster their resources by cohesively leveraging citizens, industry, and government as security actors in support of their particular deterrence and/or defense-based national security strategy. Importantly, while these states' defense postures share the core features of societal defense architectures, the specific systems in place vary across national contexts, as do the particular defense strategies these architectures underpin.[151]

For relatively small and precariously placed states with either a far larger or a series of regional rivals, this existential threat stems, in part, from concerns over size: a significant, relative disadvantage that needs to be overcome. For example, the societal defense problem facing Israel is simultaneously the need to overcome (i) a resource disparity (often framed today in terms of a lack of manpower but historically also conceptualized as a lack of weapons, weapons platforms, and military equipment) between itself and a series of neighboring states that pose a kinetic military threat and (ii) a lack of strategic depth (the maximum distance from the border to the sea being just 135 kilometers and the minimum distance a mere 14 kilometers).[152] As a result, Israel's defense strategy prioritizes deterrence and in the event of a conflict, quickly escalating and shifting the locust of conflict within the rival state(s)' territory to bring about the cessation of hostilities as quickly as possible. As a second example, the societal defense problem facing Finland is that of a larger neighboring state (i.e. Russia), which poses both a kinetic military threat and economic challenge. Notably, in contrast to Israel, the physical territory of Finland is seen as a less severe challenge, with more strategic depth giving Finland greater domestic maneuverability and the opportunity to frame its defense strategy around absorbing a significant hit from a larger neighbor and to carry-on fighting over time – buying time while waging a war of attrition. Yet, both Finland and Israel, have south to overcome the particular limitations of their size by leveraging resources across their society in-depth for national defense purposes. Notably, not all relatively small states face societal defense problems or build out

[151] While I do provide historical context both in terms of the societal defense problem facing Estonia, Finland, Israel, and Singapore, this dissertation does not seek to provide readers with a detailed examination of why states adopted particular iterations of kinetic societal defense architectures.

[152] "THE LAND: Geography and Climate," Israel Ministry of Foreign Affairs, accessed July 18, 2020, https://mfa.gov.il/mfa/aboutisrael/land/pages/the land- geography and climate.aspx.

societal defense architectures. For example, while Singapore has such a historical legacy, Costa Rica, which has had no standing army since 1948, does not.[153]

Moreover, smaller states facing existential threats are not the only states to face societal defense problems. Larger states have as well. Yet, in contrast to the Mice that Roar, their societal defense problems have traditionally been discrete (bounded to a period of ongoing conflict with a peer rival(s)) rather than sustained (a posture maintained in periods of peace to prevent or prepare of periods of crisis). Take, for example, the U.S. and the U.K. in World War II. Both states, actively leveraged their citizenry, industry, and government as defense actors by integrating both public and private actors into a cohesive, real-time national defense posture in a time of crisis. Yet, for the U.S., unlike the U.K. the homebase was not a contested space with active conflict other than the initial salvos of war: Pearl Harbor. Notably, however, these societal defense architectures were not maintained in-depth after the cessation of hostilities once the perceptions of the existential threat underpinning those architectures had dissipated. As discussed in more detail in Chapter Seven, this creates unique policy challenges for states like the U.S. given the costs – both in terms of objective resources but also the domestic political grappling for how those resources should be allocated – of sustaining a societal defense architecture in cyberspace when a corresponding operational reality is not present in the domains of air, land, and sea.

4.2. The Societal Defense Problem Facing States in Cyberspace

In contrast to its kinetic predecessors, in this 5th domain of conflict, the societal defense problem facing states is not principally rooted in a situational variable – a state's geostrategic position – but in the systemic vulnerability facing advanced industrial economies given their dependence on and the interconnectivity of cyberspace – critical interconnectivity. As a consequence, while states like the U.S. have not recently faced a kinetic societal defense problem in the domains of air, land, and sea, they do in cyberspace. This is not to say that cyber conflict is unrooted from the geopolitical environment states are rooted within. Rather, that the societal defense problem is a function of the structural realities of the threat space itself, and those structural realities take on greater weight given the range of potential adversaries states face. As one Estonian academic pointed out, malicious cyber activity comes from the usual suspects.[154] Germany is not now suddenly in the business of attacking Denmark. Though, indeed, malicious cyber activity may stem from (intelligence activity, for example) or emanate from Germany (pass through or leverage German digital infrastructure) on its way to Denmark.

In addition, while kinetic defense postures are primarily targeted toward episodic conflict that falls within the range of armed crises or war, in cyberspace, another strategic space - "actual and continuous strategic competition in cyberspace that does not reach the level of armed conflict"[155] – is of equal if not greater importance. There are two structural aspects of cyber conflict of particular note here. First, unlike kinetic societal defense postures that are geared toward conflict or war that is perceived as discrete events – either on or off – cyber conflict, as a consequence of interconnectivity (one part of critical interconnectedness), features constant contact. While there are discrete events or campaigns in cyberspace, in order to facilitate strategic outcomes in this domain, malicious actors

153 Amanda Trejos, "Why Getting Rid of Costa Rica's Army 70 Years Ago Has Been Such a Success," *USA Today*, 2018.
154 Author's Interview, 2018.
155 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation," 2018: p1.

must imbed themselves within adversary networks. Ben Buchanan explores this structural reality in-depth in his 2017 book on the cybersecurity dilemma.[156] Put simply:

> [t]he development of offensive weapons requires advance intrusion into other states' networks; maximizing defense also necessitates intrusion; therefore, states penetrate foreign networks whenever they can—even while interpreting intrusions against them as threatening.[157]

Second, much of cyber conflict falls below the threshold of war. These gray-zone challenges or gray-zone conflicts fall between traditional, declared war and peace.[158] This reality challenges conventional defense postures structured around those thresholds. It also limits perceptions of cyber conflict as an existential threat, though cyber-enabled armed conflict could easily be seen as such. As Michael P. Fischerkeller and Richard J. Harknett summarize, "[t]he cyber-strategic environment comprises two strategic spaces—armed conflict and the competitive space short of armed conflict."[159] National cyber-defense postures are grappling with both of those strategic spaces.

4.3. Conceptual and Operational Overlap

As discussed in the previous section (4.2.) and in Chapter One, no state's kinetic defense and cyber-defense posture will be identical given that cyber conflict has its own strategic, operational, and tactical dynamics that set it apart from kinetic conflict on air, land, and sea. Yet, relatively small states with pre-existing societal defense architectures in place have conceptual and operational foundations within their historical defense posture that overlap with and provide foundations for developing a societal defense posture to address the reality of critical interconnectedness in cyberspace.

Although the specific qualities of that overlap vary across the Mice that Roar, given their specific threat environment and unique domestic conditions, together they point to historical foundations across six conceptual and operational categories required of any cyber-defense posture. Each of these six conceptual and operational areas, which are fundamental to cyber-defense, are briefly summarized below, though all of them have been discussed and referenced in detail throughout Chapters One and Two and will be further elaborated upon in each of the case studies found in PART III.

4.3.1. Threats to national security not limited to kinetic, military operations

As previously discussed in detail, the 5th domain of conflict differs from the domains of air, land, and sea in several ways. One such difference relates to kinetic versus virtual tools for conflict, warfighting, and competition. Cyberspace underpins physical systems (e.g. electricity grids) as well as enables certain types of activity (e.g. e-banking, telecommunications, mass data collection, etc.). Economies rely on cyberspace to generate value, militaries rely on it to fight,[160] and intelligence agencies leverage it to gather and analyze information. As such, critical functions of society, government, and militaries can be undermined without deploying the traditional kinetic military operations that have been the primary focus on national defense postures historically.

156 Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*..
157 Lucas Kello, "The Security Dilemma of Cyberspace: Ancient Logic, New Problems - Lawfare," *Lawfare*, August 28, 2017.
158 For a detailed analysis of gray zone challenges, refer to Philip Kapusta, "The Gray Zone," *Special Warfare*, 2015.
159 Michael P. Fischerkeller and Richard J. Harknett, "What Is Agreed Competition in Cyberspace?," *Lawfare*, February 19, 2019.
160 Networks (the underlying structure of cyberspace) enabled the Revolution in Military Affairs (RMA) with total systems integration across land, air, sea, and space capabilities. There is an extensive literature on the RMA spanning political science, history, and military affairs, but for a primer on the topic, refer to Norman C Davis, "An Information-Based Revolution in Military Affairs," *Strategic Review* 24, no. 1 (1996): 43–53 and Michael E. O'Hanion, "Beware the RMA'nia!" *Brookings Report*, September 9, 1998.

4.3.2. The homebase as a location for conflict

Due to increasing dependence on cyberspace, states face significant vulnerabilities within their own territories and have faced an increasing trend of malicious cyberactivity targeting their citizenry, governments, companies, militaries, and critical functions more broadly. As previously discussed in detail in section 3.1.1. of this chapter, this insecurity is not merely theoretical. In 2016 alone, often spoken of as a critical turning point for cyber conflict, there were numerous, public, and costly incidents across critical sectors globally. This reality has also been widely recognized across countries as they hone in on strategies for developing robust protections for and the resilience of critical infrastructure/services spanning traditional public-private, civilian-military divides. Yet, importantly, recognition of need does not mean that states have successfully built out robust or mature defense postures in this space.

4.3.3. Citizens as security actors

Citizens are vital security actors in cyberspace for two reasons.

First, individuals interact with cyberspace daily, in both their personal and professional lives. Through these interactions, people pose one of the greatest risks. Whether clicking a malicious link, falling victim to a spear-phishing attack, accidently divulging credentials to a third party, failing to update their system, downloading insecure or malicious software onto a device, or connecting an insecure device to a sensitive network, individuals can aid malicious actors in their endeavors. As a consequence, they represent a significant and frequently leveraged attack vector for malicious actors seeking to degrade, disrupt, destroy, or defray the critical day-to-day functioning of companies, society, and the state. However, when individuals are well informed, resourced, and trained (in a position to practice good cyber-hygiene), they can also be an asset and an essential first line of defense.

Second, given private ownership and operation of large swaths of cyberspace as well as the critical functions that utilize or depend on it, effective cyber-defense requires a network of cybersecurity experts and practitioners across government and civilian sectors. This network must operate cohesively in real-time in order to prevent, respond, and recover to cyber-attacks. An example of the necessity of such a network can be found in the Estonian case study in Chapter Six. To summarize, in 2007, Estonia faced a series of cyber-attacks over three weeks targeting government networks and critical infrastructure, including domain names and telecoms. Over the course of those three weeks, a vibrant network of cybersecurity experts and practitioners from across the country (and neighboring countries) had to rapidly coalesce in defense of the state (public and private critical infrastructure and services across the country). Given the importance of expertise, access, and resources across the ecosystem during the 2007 campaign, this network was later formalized in the form of the Estonian Defence League's Cyber Defense Unit (*Küberkaitse Üksus*), a voluntary unit comprised of cybersecurity experts and practitioners.

4.3.4. The private sector as security actors

Notably, unlike the domains of air, land, and sea, cyberspace is simultaneously a manmade terrain and a domain through which human activity traverses. This domain of conflict and state competition is built, maintained, and advanced by humans, many if not most of which are currently sitting within industry rather than government. This issue is further compounded when we consider the critical functions that have integrated cyberspace into their operations (e.g. modern militaries or healthcare sectors) or are enabled by cyberspace itself (e.g. telecommunications or global geospatial

positioning systems such as GPS). The resources states need to deploy in order to deter an attack, repel an ongoing attack, or recover from a previous attack are largely housed outside the military itself. In short, any strategy seeking to bolster the security and resiliency of domestic critical functions will, therefore, require strong public private cooperation and coordination given that in advanced industrial democracies most of those functions are largely privately owned and operated.

4.3.5. The breadth and character of the economy as a national security imperative

The economy as a whole is an important source of domestic cyber-defense capacity, both in terms of the quality and quantity of resources at a state's disposal, but also in how those resources are then deployed across the state ecosystem from civilian sectors to the military and intelligence agencies. Cybersecurity at the national level has three broad dimensions: technical, operational, and strategic. While governments hold unique expertise and authority when it comes to strategic dimensions of cyber-defense and security, it shares (often heavily relies on) the expertise and authority of the private sector for the technical and operational dimensions. This is true both across the civilian sector, but also within government networks. Consider, the military is neither the lead buyer nor the lead producer of the pantheon of cyber technologies from which national security threats emerge. Finally, the breadth and character of the economy takes on even greater significance when we consider securing supply chains and product lifecycles (discussed in more detail in Chapter Seven). In short, effective cyber-defense is as reliant on the defense postures states adopt as it is on a robust and agile domestic economy underpinning those postures.

4.3.6. Strategic and operational oversight, coordination, and visibility across the defense-ecosystem

Cyber-defense lies at a series of intersections: (a) cyberspace is notable as a highly interconnected domain where (b) single points of failure, cascades, and dependencies are highly concerning and (c) security and resilience efforts require a real-time 'whole of society' response. Though critical, an integrated and comprehensive response can be undermined by a siloed system, broken down into specific sectors without clear strategic or operational oversight and coordination across as well as visibility into the ecosystem as a whole. These silos can be between public and private sectors but also between external and internal security actors/agencies (for example, in the case of the U.S., DoD and DHS). As one senior U.S. government official mentioned, it is the cross-cutting nature of cyber-defense that represents one of the greatest security challenges for states in general and the U.S. in particular.[161]

Notably, there is a critical difference between recognizing the importance of these six factors and successfully addressing all six in practice. Importantly, while all six factors discussed above are essential to an effective national cyber-defense posture, they also overlap with conceptual and operational foundations found within precariously placed, relatively small states seeking to provide national defense for their populations. This is not to say that all kinetic societal defense postures are identical or that they provide equal foundations for addressing the reality of critical interconnectedness in the cyber era. As demonstrated in the subsequent country case-studies, even within these relatively small countries, we see them pivoting away from existing components of their defense posture while extending and evolving others. However, they do share a similar advantage over the U.S.: for them, leveraging all of society in defense of the nation is not only not particularly novel, it is core to their existing strategic concepts and the defense architecture that underpins the implementation of those strategies in practice.

[161] Meeting, Washington D.C., US. 2019.

4.4. Summary

In conclusion, while significant attention has been placed on how the strategic and operational realities of cyber-defense diverge from prior threat spaces, cyber-defense is not an entirely new type of defense problem. While it represents an extraordinarily difficult challenge that requires a coordinated and focused effort across society (the government, the private sector, and the citizenry), for a subset of relatively small states, conventional (or kinetic) national defense also represented an extraordinarily difficult challenge that required a coordinated and focused effort from across their society. Therefore, while the structural realties of cyber-defense diverge from its kinetic counterparts in several important aspects, understanding cyber-defense as a societal defense problem allows us to recognize that it is not without relevant precedent: prior societal defense efforts in the domains of air, land, and sea provide a historical basis for developing national approaches to cybersecurity.

5. Conclusion and Observable Implications

Just as military power assessments "focusing solely on materiel will radically over-estimate well-equipped but poorly handled armies" and "under-estimate poorly equipped by well handled troops", cyber-defense capability assessments focused solely on material factors will radically over-estimate the capabilities of well-resourced but poorly organized states while simultaneously under-estimating the comparatively less-well-resourced small states whose historical defense architectures more closely match the realities of the cyber era.[162]

States are not starting with a blank conceptual and institutional slate every time a new defense problem is introduced. Pre-existing defense postures and institutions, developed in specific geo-strategic environments, influence emerging state national cyber-defense approaches. Notably, those historical defense approaches can be maladapted for the realities states now face. As the well-worn proverb warns, we are best prepared to fight the last war. The closer that last war resembles the next, the better your foundations and the less need for costly and radical restructuring.

We should therefore observe the following in the subsequent five country case-studies that comprise Part II of this dissertation:

> *For the U.S., existing kinetic defense postures were maladapted to the reality of critical interconnectedness leading to a sharper disjuncture between historical national defense approaches and the societal cyber-defense problem they now faced.*
>
> *For the Mice that Roar, existing kinetic defense postures served as an important bedrock from which to build due to conceptual and operational overlap between existing defense postures and the realities of addressing critical interconnectedness in the era of cyber conflict.*

Notably, as a group, the Mice that Roar demonstrate overlap between the societal defense postures adopted by relatively small imperiled states and a cyber-defense posture centered on addressing critical interconnectedness. The U.S., in contrast, is an outlier with limited historical overlap between its prior defense posture and the operational requirements of cyber-defense. As we transition into these case studies, keep in mind the six conceptual and operational categories required of any cyber-defense posture.

[162] Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*. loc. 185

- Threats to national security not limited to kinetic, military operations
- The homebase as a location for conflict
- Citizens as security actors
- The private sector as security actors
- The breadth and character of the economy as a national security imperative
- Strategic and operational oversight, coordination, and visibility across the defense-ecosystem

For each of the Mice that Roar, their kinetic defense postures overlap with various configurations of these categories and, as a consequence, provide important foundations upon which to build. The U.S. case, in contrast, is a story of disjuncture, where these conceptual and operational realities are largely absent from historical approaches to national defense.

Chapter 3
The Research Design:
Case Selection and Data Collection

1. Introduction

The argument presented in this dissertation is supported by two and a half years of within country, cross-national case study research across five countries chosen to provide theoretical leverage (Estonia, Finland, Israel, and Singapore in comparison to the much larger U.S.). Qualitative fieldwork examined (1) the components of cyber capability and cyber vulnerability driving national defense needs and, given that, (2) how these states allocated and organized resources in an effort to attain capabilities and address particular vulnerabilities and (3) the decision processes behind and evolution of the various strategic and operational choices undertaken. Conducting in-depth case studies allowed me to trace the process and development of cyber-defense postures within and between countries and to demonstrate how existing defense postures shapes the organization and efficacy of subsequent cyber-defense postures, for better or for worse.

I selected these particular countries because they provided important leverage between cases to assess how a subset of relatively small states find themselves as leaders in national cyber-defense alongside far larger states like the U.S. These five countries are all leaders in national cyber-defense but vary substantially on factors that have been identified as potential drivers of variation in national defense capabilities pre-cyberspace, including the threat environment (e.g. geographic region, including proximity to and the character of potential rivals), size (e.g. population, economic development, kinetic military capacity, and territory), duration of time (e.g. how long they have been pursuing national cyber-defense capabilities), degree of cyber-dependence (e.g. penetration of internet across a population, digitization of core functions, etc.), degree of homogeneity (e.g. diversity, or lack thereof, within a given population); and the vibrancy of cybersecurity industry domestically (e.g. the breadth, scope, size, and innovativeness of cybersecurity firms).

The four relatively small states selected for analysis – Estonia, Finland, Israel and Singapore – also provide important within-case variation for evaluating the argument presented in this dissertation. In addition to varying as a group from the U.S. in terms of the type cyber-defense postures they pursued, they also vary from each other in terms of the unique character of each kinetic societal defense posture they subsequently leveraged into cyberspace. While each of these cases have a societal defense approach that provided a conceptual and operational foundation for pursuing a societal defense approach to national cyber-defense, there was not complete overlap between their kinetic defense posture and their desired cyber-defense posture. As a consequence, each of these Mice that Roar found areas where their models cannot be directly leveraged and therefore find themselves hampered by historical experience.

In sum, by leveraging between and within case variation, the in-depth case research completed here illustrates the limitations of alternative explanations for addressing why these mice roar, develops and evaluates the argument presented in this dissertation, and demonstrates how the core dynamics animating this argument across states can also be observed within the states as they develop a cyber-defense posture.

In order to maximize transparency in the research design underpinning the argument presented in this dissertation, the remainder of this chapter will describe, in depth, the case selection and data

collection methods utilized in this research project. The chapter concludes with a discussion of the complexities and limitations present in cyber-defense research and an overview that places the research design into direct conversation with the argument presented in the prior chapter and the empirics that fill follow in subsequent chapters.

2. Case Selection

Case selection for this project served two primary purposes. The first set of cases – Finland and the U.S. – served primarily as exploratory cases[163]. The second set of cases – Israel, Singapore, and Estonia – served as diagnostic cases[164] to test the theory developed in the exploratory cases and to illustrate its generalizability and utility across varying regions, threat environments, and pre-existing kinetic societal defense postures.

Notably, in addition to the theoretical reasons for case selection outlined in the next section, analysis of all five of these cases has intrinsic importance[165] as leaders in national cyber-defense – both in terms of the academic study of the strategic and operational dynamics at play in this 5th domain of conflict but also in terms of the policy insights that can be distilled from them and shared between countries seeking to bolster the security of their populations in the cyber era. They offer some of the richest histories of emerging cybersecurity policy development due to their commitment to and relative success in this domain.

2.1. Exploratory Cases: Finland and the U.S.

Through detailed historical analysis of the process of adopting a cyber-defense posture within and between these cases these three states, I first identified variation in the type of cyber-defense postures states had adopted and uncovered that for some states, kinetic models of national defense not only closely mirrored the essential features of an effective cyber-defense posture but also that states, for better or worse, directly leveraged pre-existing kinetic defense approaches into their national cyber-defense postures.

Two initial explanatory cases – the U.S. and Finland – were selected for theoretical as well as practical reasons.

First, the U.S. and Finland provide significant variation in size while holding the outcome constant (leaders in national cyber-defense). There are three alternatives for why small states appear as leaders alongside a far larger historical power, the U.S.: (1) small states are punching above their weight, (2) the U.S. is punching below its weight, or (3) both one and two are occurring at the same time. As a consequence, examining variation between a large – the U.S. – and relatively small state – Finland –

163 Exploratory cases are selected for the purposes of theory development. In this research design, exploratory cases were selected in order to work "backward from a known outcome to its possible causes" (Gerring, p65). The known outcome in question is relatively high cyber-defense capability. The causes, given that traditionally theorized drivers do not adequately explain observed variation, remains to be determined. For more information on the role and selection of exploratory cases in case study research, refer to John Gerring, *Case Study Research: Principles and Practices*, Second Edition. Kindle Edition. (Cambridge University Press, 2017).

164 In contrast to exploratory cases, diagnostic cases help to "confirm, disconfirm, or refine" the theory developed in the exploratory case studies (Gerring, p98). For more information on the role and selection of diagnostic cases in case study research, refer to Gerring, 2017.

165 According to John Gerring, cases selected for intrinsic importance fall into two broad categories: "obvious world historical significance" and "important for a specific group of readers". These five cases are significant for both reasons. First, as leaders they hold importance as scholars trace a historical trajectory of cybersecurity capability evolution over time. Second, given their relative success, they serve as important points of historical reference for other states seeking to address cybersecurity concerns within their own countries. For more information on case selection based on intrinsic importance refer to Gerring, 2017, p 42.

allows a structured comparison of factors other than size that potentially drive national cyber-defense outcomes.

Second, Finland represents an extreme case. As a late starter in cyber-defense[166], Finland had to rapidly deploy a cyber-defense posture that then very quickly rivaled a far larger U.S. Taking these two cases together, on the one hand, you have the far larger U.S. with a longer duration of policy development and on the other you have the far smaller Finland with a far shorter duration of policy development. As a consequence, whichever factors shaped how these Mice Roar in cyberspace, Finland should have them in spades given the speed through which it became a leader.

Third, unlike Israel and Estonia, Finland has not been subject to now commonly accepted idiosyncratic explanations for the organization and efficacy of its cyber-defense posture. As an understudied case, it allows for most robust collection of new data without the accompanying density of pre-existing theories. Finland, therefore, provides important leverage for moving beyond ad hoc and/or country specific explanations that do not travel beyond those countries' unique circumstances.

Fourth, and on a practical note, the research design required to tackle the questions presented in this dissertation required substantial access within countries. That access takes on greater significance when one considers the sensitivity of the topic at hand and the associated difficulty of securing interviews with individuals willing to talk openly about the development and the strengths and weaknesses of an emerging national defense posture. In both the U.S. and Finland, I had significant existing networks and institutional support to assist in collecting comprehensive and accurate data. The importance of domestic support, institutional affiliations, and the ability to leverage existing contacts and networks cannot be overstated. Access can make or break a research project of this kind.

2.2. Diagnostic Cases: Israel, Singapore, and Estonia

The second set of cases – Israel, Singapore, and Estonia – served as diagnostic cases to test the theory as well as assess generalizability. These three cases serve as valuable diagnostic cases for five reasons.

First, Israel and Singapore were selected as most similar cases – a history of being imperiled and the need to overcome size as a source of vulnerability – to assess whether they too are leveraging existing conceptual and operational defense approaches to organize a societal defense architecture in cyberspace. In other words, if the argument developed captures why Finland was able to roar in cyberspace, then it should, likewise, be able to explain the development of a national cyber-defense posture in other states who faced societal defense problems and subsequently built out kinetic societal defense architectures in response. Israel and Singapore are two such states.

Second and in addition, both of these cases speak to the broader generalizability of the theory presented here. They vary from the U.S. and Finland as well as from each other on potential drivers of variation in national defense capabilities pre-cyberspace, including the threat environment, size, duration of time spent on national cyber-defense, and the character and vibrancy of cybersecurity industry domestically.

166 Finland first began to develop their cyber-defense posture in the late 2000s and early 2010s as compared to Israel, which began in the late 90s and early 2000s. The U.S., like Israel, began its policy development in late 90s and early 2000s.

Third, Israel, in particular, also represents a hard case for testing the theory presented here. Unlike Finland, which pursued a resilience-based national defense strategy, Israel's kinetic defense strategy more closely resembled the U.S.'s with its focus on deterrence (although a far more offensive flavor than the U.S.'s approach). As, such by illustrating how Israel has been able to leverage existing societal defense architecture directly into cyberspace, this case in particular highlights the importance not just of the strategy at the conceptual level but also in how strategies are operationalized (which actors are security actors and how they coordinate and cooperate toward that strategic goal). In other words, while Israel's defense posture more closely resembles the U.S. at the strategic level, the operationalization of its deterrence posture more closely resembles Finland by leveraging all of society in the implementation of that deterrence strategy.

Fourth, although also a diagnostic case for my theory, the addition of the Estonian case serves a distinct function than that of Israel and Singapore. Unlike the other Mice that Roar examined in this dissertation, Estonia gained its independence from the USSR in 1991. Estonia came of age in the cyber era.[167] As a consequence, it was building out its kinetic defense posture alongside its cyber-defense posture. This allows for a unique test of my theory. My dissertation represents a fundamental shift in how we understand the organization and efficacy of national cyber-defense efforts by placing states' geopolitical position and pre-existing defense architectures at the center of the analysis alongside the core strategic and operational dynamics facing all states. Given that Estonia is a precariously placed relatively small state, the theory would predict the adoption of a kinetic societal defense architecture alongside a societal defense architecture focusing on cyberspace to support its national security strategies. If Estonia did not exhibit synchronicity between its kinetic and cyber-defense postures, it would present an important challenge to the argument presented here.

Fifth and finally, Israel and Estonia represent important cases given that they have both been the subject of research that has led to well-known but largely idiosyncratic explanations for why they have found themselves punching above their perceived weight when it comes to national defense in cyberspace. If my argument provides analytic insights into the evolution of cyber-security policy and the postures pursued by Israel and Estonia, it illustrates that they, while wholly unique in many ways, are also unique in their membership amongst a subset of relatively small states: the Mice that Roar. In other words, they further demonstrate that the Mice that Roar are not leaders in national cyber-defense solely due to a grab-bag of idiosyncratic variables but instead for a systematic and generalizable set of variables.

3. Data Collection

Data collection consisted of (1) archival research focused on both primary and secondary sources; (2) extensive in-depth, elite interviews[168] with 95 individuals central to or experts in cybersecurity policy formation and ongoing operations in each country; and (3) observational data collected through attendance of and/or active participation in formal and informal meetings with policy-

[167] For a detailed history of the early days of the internet, refer to Barry M. Leiner et al., "Brief History of the Internet | Internet Society," The Internet Society, 1997, https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

[168] 95 individuals were formally interviewed across five countries: Finland-32, Israel-17, Singapore-17, Estonia-15, and U.S.-14. A few subjects were interviewed more than once, usually in an effort to corroborate information acquired after their first information. These numbers do not count the numerous informal, deep background conversations that occurred over the past four years or insights garnered from observation of and/or participation in formal and informal meetings with policy-focused researchers, policy makers, and industry members focusing on improving cyber-defense capabilities within and across states. Interviews ranged in duration from an hour to two hours with a few lasting far longer.

focused researchers, policy makers, and industry members focused on assessing the state of and opportunities for improvement in cyber-defense capabilities within and across states.

The study of cyber conflict has historically been hindered by questions over access to and the reliability, accuracy, and utility of data.[169] This can sometimes result in research that hinges off anecdotal evidence or limited written, unclassified or declassified documents. These approaches miss large swathes of potential data; data that, importantly, offers significant insight into outcomes and processes that would otherwise be overlooked or mischaracterized. In this context, utilizing a three-pronged data collection strategy provides a distinct advantage when studying cyber conflict and the evolution of cyber-defense postures. Five advantages to this approach are particularly noteworthy.

First, cybersecurity and conflict - both as an academic field and the policy space – is nascent, relatively and objectively. As U.S. General James Mattis stated in a meeting at Stanford, "while states have been waging war on land and sea for thousands of years and in the air for a hundred, we have only been waging war in cyberspace for the last 20 or so years".[170] As a result, there are less documents in general, and less public documents in particular than in these other domains of conflict available to researchers. The U.S. has by far one of the largest publicly available repositories, bolstered by the efforts of the National Security Archive's Cyber Vault Project,[171] while other states have more limited sets of data points[172] to draw from.

This is further complicated by concerns over the nature of missing data: such as classified data as well as unreported, under reported, or over reported types of events. In an effort to address these concerns, I augment the written record with extensive elite interviews and access to policy meetings and briefings. This allowed for a breadth and depth of data collection that would be absent without the undertaking of extensive within country and across country case fieldwork. As a consequence, this project offers an unusual empirical contribution by collecting frank, rich commentary directly from cybersecurity and national defense practitioners across five distinct countries.

Second, there is frequently a wide-gulf between, on the one hand, what strategy documents claim a country recognizes as an issue and the solutions they will pursue and, on the other hand, what that country does in practice and the degree to which they do it. For example, many democratic countries will recognize the importance of norms, working with industry, cooperating with allies, closing the skills gap, etc. Yet, the degree to which they pursue these goals in practice, the models they utilize to do so, and the resources they expend operationalizing those goals varies significantly across countries. Utilizing numerous in-depth interviews alongside observations garnered from policy meetings and briefings to augment the existing written record allows this research project to speak more directly to what states are doing in practice rather than simply what they have identified as important in theory.[173]

[169] This is a concern that has animated the sub-field of cyber conflict and security studies. Melissa K. Griffith, "Why Cyber Conflict as an Academic Discipline Struggles to Make Its Mark in Political Science," *Council for Foreign Relations' Net Politics and Digital and Cyberspace Policy Program*, September 6, 2018.
[170] Meeting, Stanford University, CA, 2020.
[171] "Cyber Vault," National Security Archive, https://nsarchive.gwu.edu/project/cyber-vault-project.
[172] In English or otherwise.
[173] This takes on greater importance when we recognize the ways in which public facing strategy documents are created and the myriads of purposes public documents serve in contrast to the processes through which strategies are identified and operationalized in practice.

Third, there is significant variation on how states record and disseminate policy. For example, there are numerous public-facing documents in the U.S. related to national approaches to cyber-defense. In contrast, Israel does not routinely publish such broad public-facing formal documents, choosing instead to focus on internal guiding principles and shared understandings in order to avoid rigidity in national defense efforts and to encourage agility and evolution of core concepts and approaches over time.[174] While in the U.S. you can point to the first national cybersecurity strategy as a core signpost in the evolution of the American cyber-defense posture, If one were to analyze the paper trail in Israel in the same manner, you would mistakenly assume that there is little official strategic consensus on national cyber-defense. In reality, there is significant strategic consensus and operationalization of that consensus over time. Extensive interviews bring to light these national policy quirks and helps shape the approach to archival work (i.e. what materials to gather and where to look for them). Pursuing both simultaneously, allows each approach to augment and support the other for a more robust historical analysis within and between countries.

Fourth, written primary and secondary source material offer limited utility when asking why or how a decision was made or an evolution occurred. In this circumstance, elite interviews provide important insight into the process through which these polices were created, implemented, and revised over time. They bring you into the process through which policy unfolded by interviewing individuals who wrote a specific strategy or have intimate knowledge of how the strategy was written and can point to decisions that were discarded, championed by only a few, or unanimously supported. For the process of tracing the history of cyber-defense posture development in each of these countries, these insights prove invaluable.

In conclusion, carrying out extensive within country interviews and participating in and observing formal and informal briefings and meetings significantly augmented the written primary source and secondary source records allowing for greater nuance and accuracy in tracing the decision processes behind and the various strategic and operational choices over time. Moreover, by triangulated across three distinct data collection methods, and specifically collecting a substantial amount of new data through interviews, I have increased "our ability [as researchers] to tease knowledge from the imperfect data available to us".[175]

3.1. Written Record

The first data stream for this dissertation was the written record: comprised of primary and secondary source material. This included but was not limited to government strategic documents, presidential orders, court case documents, legal code, meeting minutes and documentation, government reports/assessments, third party reports/assessments, organization documentation, (i.e. mission, mandate, budget, etc.), news reporting, press releases, and prior academic or industry research. These resources were accessed electronically from government or public repositories[176] when possible or in hard copy within country when necessary. The written record provided an important foundation upon which to expand in interviews or meetings as well as a data stream through which information gleaned from interviews and meetings could be corroborated or expanded.

[174] Author's Interviews. 2019.
[175] Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*. loc. 335.
[176] such as the National Security Archive's Cyber Vault. "Cyber Vault."

3.2. Semi-Structured, Elite Interviews

Anonymity is often an indispensable, and occasionally the only, means through which to collect data on a state's current national defense posture: the evolution of core concepts, strategies, institutions, and operations as well as core strengths and persisting limitations. Given the sensitivity of national defense capabilities in general[177] and the sensitivities unique to national cyber-defense activity and capabilities,[178] while some interview subjects agreed to be interviewed on the record many preferred to remain anonymous. While, at first glance, omitting some names and not others would seem to be an appropriate solution in theory, doing so would not adequately consider the processes being studied or the countries within which these processes are occurring in practice. There are a limited number of people who could plausibly speak to the development of a state's cyber-defense posture, especially in the relatively small countries that make up the bulk of this research. Oscillating between on-record and anonymous sources throughout this dissertation would, in practice, provide anyone familiar with these countries' significant insight into the identities of those who wished to remain anonymous.

As a consequence, I have omitted almost all references to names, specific interview dates, and locations in this manuscript in order to protect the subjects' identities. The few exceptions to this were interviews with individuals on-record over matters of public knowledge where their role in the policy development process was so unique, central, and widely known in scholarship, white papers, and news reporting that presenting information reported from them would be universally identifiable. Fortunately, this very limited set of circumstances apply only to a few interviewees who have previously been and continue to be very public about their role in and thoughts on the development of cyber-defense capabilities within their country.

As intelligence and cybersecurity scholar Professor Amy Zegart acknowledged in her own research, anonymity comes with clear benefits and drawbacks for both data collection and analysis.[179] "Protecting a source's identity encourages candor and prompts some individuals to speak who otherwise would not. […] On the other hand, anonymous sources are protected from having to defend their assertions and confront their biases in the light of day."[180] To mitigate the potential drawbacks, Zegart identified three responsibilities for any researcher incorporating anonymous interview data into their research: (1) to take particular care with the selection of interview subjects, (2) to consider potential biases interviewees may bring with them into the interview, and (3) to use other sources of information (interviews, archival, etc.) to verify information a source provided you.[181] In my own data collection and analysis, I have considered and made a significant effort to address each of these responsibilities.

First, I have paid specific attention both to the number and the diversity of interview subjects selected across and within countries in order to emerge with as accurate and compressive a view of the development of cyber-defense postures as possible. Ninety-five semi-structured-elite interviews were conducted over the course of two and a half years. Subjects included current or former government officials across the national government bureaucracies; officials serving on behalf of their country within international organizations or institutions; staff within cybersecurity specific

177 which resides at the intersection of national security strategy, operations, and tactics
178 intersection with intelligence, that there is significant costs associated with being caught flat footed so real draw backs to indicating that you don't have a good grasp on an issue, classification, etc.
179 Amy Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11*, Kindle Edition (Princeton University Press, 2009)., p14.
180 Zegart. p14.
181 Zegart. p14.

agencies, institutions, or organizations within a country; individuals within industry working on or in cybersecurity; industry organizations or partnerships with a cybersecurity mission; and researchers within universities and think tanks.

Second, interviews, were semi-structured allowing for greater tailoring of questions to the specific position each interviewee held and the slice of the cybersecurity problem they had first-hand knowledge of and could directly speak to in depth. These interviews were comprised of a series of core questions asked across most interviewees, questions specific to the positions held by and expertise of the interview subject, questions specific to the country in question, questions tailored to confirm or provide further details on information gathered through other means (seeking corroboration), and questions that specifically arose within the context of the interview either for clarification or to allow for additional elaboration. The format of questions ranged from broad, open-ended questions intended to spark conversation to select statements/claims that subjects were then asked to explain if and why they agreed or disagreed in as much detail as possible. Whenever feasible, interview subjects were also asked about their experiences in or observations of other countries' approaches to cyber-defense. All interviews were documented through extensive note-taking, a few were recorded with permission from the interviewee.

Third, rather than take an interview subject's comments at face value, I weighed their views against those expressed by other interview subjects as well as information gathered from other data sources such as archival research and, whenever possible, access to briefings and meetings. No single data-input or interview source stands alone in this analysis or is assumed to be accurate without further investigation and corroboration.

In countries where I had greater access to and diversity of information available through primary and/or secondary written materials or through observation of the policy process or policy focused meetings, the number of interviews needed to triangulate between multiple sources and reliably trace the historical process of developing a cyber-defense posture were less than in countries where fewer documents were public, less secondary material was available, and due to access issues (foreign national or language barriers) observational data was more limited. In the latter instance, elite interviews were more comprehensive in scope in order to develop and asses the argument presented in this dissertation. For example, I completed the fewest interviews in the U.S.: a country with the most extensive primary and secondary paper trail and the country I had the most access to the policy process as well as formal and informal meetings that directly hit on topics of direct importance to this research project. In contrast, I completed the largest number of interviews in Finland: a country with a limited paper trail and a case that served as the first exploratory case outside the U.S.

Interviews by Country	
Finland	32
Israel	17
Singapore	17
Estonia	15
U.S.	14
	Total = 95

3.3. Access to Meetings and Briefings

The third data collection method consisted of observation of and/or participation in policy and industry briefings and meetings. These meetings ranged from off-record candid discussions on one extreme, Chatham House rules meetings in the middle, and on-the-record public panels/lectures on the other extreme. Events with senior policy officials and/or industry leaders also ranged in terms of

attendance, format, and location including large public conferences,[182] smaller invite only conferences and presentations at think tanks or universities,[183] and invite only workshops and briefings frequently held at think tanks and research centers.[184] Information collected from these events and meetings helped augment the written record and corroborate information gleaned from elite interviews. They also served as an important validity check when specific concerns or processes that I was tracing through other data collection methods were being mirrored back to me in these briefings as policy and industry experts laid out the state of play in their particular agency, department, or organization.

3.4. Complexities and Limitations to Cyber-Defense Data Collection

Not all cybersecurity policy is public. There is simultaneously a public and private face, which results in some cybersecurity efforts falling outside the public domain due to their perceived sensitivity. This division between privately available and publicly available information has two important implications for any research on national defense in general and this research in particular.

First, a portion of data will remain outside the public sphere and, therefore, unavoidably fall outside this analysis. For example, depending on the granularity of the information discussed in an academic context, limitations or weaknesses inherent in a state's current approach can be used against the state in question in the real world. This provides incentives not to reveal information that may later be weaponized.

The absence of privately held data challenges conclusions drawn based off publicly facing data if and when the activity occurring behind closed doors is qualitatively different than the activity that is visible publicly. This is a challenge all academic research faces, to some degree. However, it is worth noting that there may be less activity in the private domain than we might otherwise assume. Marking something confidential can hide both a plan or activity from public sight as well as a lack of plan or activity from public sight. One Finnish interviewee referred to this as "classifying an empty box"[185] and indicated that in new or incredibly complex domains like cybersecurity, this practice becomes more likely.

Second, this concern can be amplified when the ratio between privately available and publicly available information skews more toward privately held in certain countries: for example, Finland and Singapore.

Finnish security policy is centered on the defense of society, ensuring that this defense does not provoke a larger neighboring state (i.e. Russia) which poses both a kinetic military threat and economic challenge. This has historically led to a largely quiet and publicly limited set of discussions and security efforts. Finnish officials have pointed publicly to the importance of maintaining good relations with Russia, while also maintaining that this approach is not appeasement, since Finland does maintain capabilities for its defense.[186] This specific emphasis on tailoring public security policy,

[182] e.g. the RSA Conference in San Francisco, CA; Cycon in Tallinn, Estonia; CyCon US in the Arlington, VA; CYBERWARCON in Arlington, VA; CEPS Ideas Lab in Brussels, Belgium; and Cyberweek in Tel Aviv, Israel.
[183] e.g. the Center for Long-Term Cybersecurity (CLTC), the Center for International Security and Cooperation (CISAC), and the Cyber Conflict Studies Association (CCSA).
[184] e.g. at the Wilson Center, Atlantic Council, Centre for European Policy Studies, Brookings, Carnegie, Center for New American Security, New America, and Center for Naval Analysis.
[185] Author's Interview, 2018.
[186] Reid Standish, "How Finland Became Europe's Bear Whisperer," *Foreign Policy*, March 7, 2016.

rhetoric, and posturing, in order to avoid aggravating a particular regional power was also strikingly reflected in interviews. Finns frequently referenced 'potential threats from the East' as shorthand for a consistently unnamed Russia. For Finland, efforts in any security space walk a fine line between publicly and privately addressed issues and concerns.

Singaporean security policy also walks this fine line. Located to the south of a far larger Malaysia and to the north of a far larger Indonesia, Singapore's economic success hinged on being a hub for financial and commercial activity in the region without exacerbating historical rivalries with its neighbors. Moreover, Singaporean society is fairly hierarchical. For example, unlike the other countries I interviewed in, several potential interview subjects across the government funneled my request to a handful of individuals sitting in a specific agency: the Cyber Security Agency of Singapore (CSA). In many of these same email responses, potential subjects indicated that they knew who I had already been in contact with (emailed) before I had even set foot in country. Interview answers were also the most uniform – both in terms of content and the specific language used – across government, industry, the press, and academia in Singapore. Unlike in the other four countries where I had conducted fieldwork, in Singapore there was a clear and well-rehearsed narrative echoing throughout many of my interviews. For Singapore, efforts in any security space walk a fine line between publicly and privately addressed issues and concerns.

The three-pronged data collection approach underpinning this research project seeks to address these concerns, in part, by diversifying data collection sources, corroborating between those sources, and introducing the nuance of how countries talk about their approaches in addition to the approaches themselves to the subsequent analysis. Significantly, the ways in which countries shape their narrative can be informative for understanding how they conceptualize and operationalize a security architecture given that observed interview dynamics – i.e. hierarchical with a singular narrative – play out in government, business, and societal processes more broadly.

In conclusion, given these limitations, this dissertation does not pretend to offer a comprehensive analysis of all government cybersecurity efforts. Rather it seeks to provide an overview of dominant, publicly observable approaches. These approaches provide an important foundation for future analysis and provide insight into the types of activities that are likely also occurring in tandem behind closed doors. However, they are just that: dominant and publicly observable.

4. Reviewing the Research Design

In conclusion, the cases selected allow for important within and between case variation needed for the development and evaluation of the argument presented in this dissertation. Taken together these five countries provide important between case variation not just in terms of their size but also across other factors that could potentially impact cyber-defense capabilities such as their geographic region/threat environment, how long they have been developing cyber-defense capabilities (time), as well as their cybersecurity expertise within industry and the degree to which cyberspace has permeated their day-to-day life. Within case variation – tracing where components of their defense posture mirror the necessities of a cyber-defense posture and where they diverge – provides an additional opportunity to assess the strength of my argument.

Overview of Case Characteristics

	SIZE					TIME	TECHNOLOGY	
	Total Area	**Population**	**GDP (purchasing power parity)**	**GDP per capita**	**Global Firepower Index**	**Year of First National Cyber Security Strategy**	**Internet Penetration (% of Population)**	**Most Innovative Cyber security Firms**
U.S.A. (North America)	9,833,517 sq km 4th globally	329,256,465 3rd globally	$19.49 trillion 2nd globally	$59,800 19th globally	1st out of 137 countries	2003[187]	95.6 %	350 out of 500 Ranked 1st
ESTONIA (Europe)	45,228 sq km 133rd globally	1,244,288 157th globally	$41.65 billion 116th globally	$31,700 64th globally	112th out of 137 countries	2009[188]	97.9 %	0 out of 500
FINLAND (Europe)	338,145 sq km 66th globally	5,537,364 117th globally	$244.9 billion 62nd globally	$44,500 38th globally	63rd out of 137 countries	2013	94.0 %	2 out of 500
ISRAEL (Middle East)	21,937 sq km 153rd globally	8,424,904 98th globally	$317.1 billion 54th globally	$36,400 54th globally	17th out of 137 countries	2002[189]	81.6 %	42 out of 500 Ranked 2nd
SINGAPORE (Asia)	719.2 sq km 191st globally	5,995,991 112th globally	$528.1 billion 38th globally	$94,100 7th globally	59th out of 137 countries	2013	88.2 %	2 out of 500

* NOTE: Total Area, Population, GDP (purchasing power parity), and GDP per capita are from the CIA World Factbook. Population represents 2018 estimates while both GDP figures represent 2017 estimates. The Global Firepower index assessments are from the www.globalfirepower.com and represent the 2019 rankings. Internet Penetration figures are from www.internetworldstats.com and represent the 2019 assessments. The 500 most innovative cybersecurity firms in 2018 was compiled by Cybersecurity Ventures and can be located at www.cybersecurityventures.com.

By leveraging a three-pronged approach to data collection, this dissertation seeks to overcome limitations to data collection that can hamper national defense analysis in general and national cyber-defense analysis in particular. This approach provides ample opportunities for corroboration and triangulation[190] between multiple sources. Through extensive data collection, this dissertation provides unique insight into how and why a defense posture evolved in practice within five distinct country cases.

Although this research design leverages a small number of cases (N of 5), through rigorous explanatory (aimed at theory building) and diagnostic (aimed at theory testing) case selection and data collection, I hope to convince readers that (1) the argument developed here is valuable for understanding outcomes within the cases presented in this dissertation and (2) that the cases

187 U.S. White House, "The National Strategy to Secure Cyberspace," 2003.
188 European Union Agency for Cybersecurity (ENISA), "National Cyber Security Strategies - Interactive Map," accessed July 2, 2020, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
189 As repeatedly explained to me during interviews in Israel, Israel avoids strategy documents such as those found in other countries. As a consequence, I am coding Israel by the first agency tasked with this mandate, but awareness of and the development of a national approach to national cyber-defense pre-dates this creation of the National Information Security Authority (NISA) to the 1990s.
190 For a more detailed discussion of methodological triangulation, refer to Donald Polkinghonre, *Methodology for the Human Sciences* (State University of New York Press, 1983). and Colin Elman and Miriam Fendius Elman, eds., *Bridges and Boundaries: Historians, Political Scientists, and the Study of International Relations* (MIT Press, 2001).

examined provide plausible grounds for believing my argument has wider utility for explaining the organization and efficacy of cyber-defense postures more broadly while also (3) strengthening our understanding, theoretically and empirically, of the cyber-defense problem states currently face.

PART II

The Advantage of Being Small and Precariously Placed

Chapter 4
Big vs. Small: The United States and Finland

1. Introduction

Finland, at the eastern most border of the European Union (EU), launched a working group to develop a national cybersecurity strategy in 2012[191] and released its official Cyber Security Strategy in 2013.[192] Yet, it had already begun to gain international attention for its cyber-defense capabilities as early as 2012/2013, a trend which continued throughout the 2010s.[193] What explains Finland's apparent meteoric rise as a leader in cyber-defense and cybersecurity at the national level ranking along the far larger U.S.?

As states try to solve for critical interconnectedness in the cyber era, some historical patterns of national defense are better suited to the operational realities of cyber-defense than others.

For Finland, as a state who had historically faced a societal defense problem and built out a corresponding societal defense architecture, the strategic and operational realties of cyber-defense represented a difference in kind and not in type.

The U.S., in contrast, was faced with a sharp disjuncture between the operational features of its kinetic defense posture and the operational requirements of cyber-defense. Instead of facing a security environment where conflict is waged outside the homebase, the military and intelligence community are the primary security actors, and industry plays a security role in so far as it is part of the military industrial base, in an era of cyber conflict the U.S. faces an environment where military and/or intelligence agencies cannot be relied on as the sole or even primary defense actors and both public and private actors must be integrated into a cohesive, real-time national defense posture.

Given a dominant focus on the U.S. within the nascent field of cyber conflict scholarship, this experience of a sharp disjuncture has largely been assumed to be a systemic feature of the threat space. In reality, the degree to which cyber-defense represents a novel type of defense posture – a departure from historical experience - is best understood as situational. Not all defense postures were equally maladapted to the realities of cyber-defense. It just so happens a core disadvantage of being a superpower is that this type of defense problem appears novel because of the historical military and economic strength they have enjoyed. Small and precariously placed have not had that luxury, a disadvantage that has now become a strength as states globally begin are now grappling with the national security implications of increasing critical interconnectedness in the cyber era.

[191] Interviews with two members of the working group and its existence was corroborated by other interviewees.
[192] Finland's 2013 Cyber Security Strategy has been followed by two implementation programs, the most recent of which is the Implementation program for Finland's cyber safety strategy 2017-2020.
[193] Recall from the introductory chapter in this book, in 2012, the Finland topped the Brussels-based think tank Security and Defense Agenda index of state's cybersecurity preparedness levels. In 2013, the Cyber Readiness Index (CRI) 1.0 revealed a similar mix of small and large countries earning higher scores, including Australia, Finland, Japan, the Netherlands, Norway, the U.K., and the U.S. The U.S. came in at number nine. In 2017, Finland was acknowledged as the most cyber secure country in the EU and topped the UN's Global Cybersecurity Index rankings alongside the far larger U.S.

Importantly, given their small size and geographically precarious position, Finland has historically deployed a distinct model for national defense that seeks to address high levels of vulnerability across the homebase (or homeland) by pointedly emphasizing both public-private and civilian-military coordination and cooperation. In other words, Finland became a significant provider of national cyber-defense for its population because it has been able to leverage an existing societal defense architecture to address this new kind of societal defense problem.

Given Finland's historical geopolitical position, it has built out a corresponding defense posture that emphasizes defense of society by maintaining society-wide resilience in the event of a crisis. Finland's concept of comprehensive security (*kokonaisturvallisuus*) is animated by a systems-based approach, which emphasizes the importance of interdependencies between individuals, firms, industries, universities, research organizations, and government ministries in achieving security. In comprehensive security, as in the sub-category of cybersecurity, the responsibility for and the safeguarding of the vital functions of society are jointly held by private and public actors, industry and government, defense forces and citizens.

Early national cyber-defense efforts have mirrored this systems-based approach focusing on cooperation between various ministries, between public and private actors, and between private and private actors. The end result is a web of overlapping clusters tasked with specific responsibilities and characterized by deep and frequent information sharing, training and exercises, and coordination of operations during and after times of crisis. Therefore, for Finland, cybersecurity, like its parent category of comprehensive security, is based on a concept centered on maintaining critical resilience in and defense of society. Significantly, given this focus on civil society's role for the provision of security and the recognition that threats do not need to be military in nature to cause significant harm to and impose high costs on broader society, Finland's comprehensive security approach provides a conceptual and operational foundation that is well suited to the realities of addressing cybersecurity at the national level.

In sharp contrast, the U.S., a superpower focused on balancing and global power projection, is not preciously placed. It has not in recent history faced a societal defense problem or robustly maintained the societal defense architecture it developed during WWII.[194] American citizens and industry do not historically need to be on a "warfooting"[195] alongside the military and intelligence apparatus in the domains of air, land, and sea. As a consequence, for the U.S., cyber-defense represents a new type of defense of problem: one that requires a largely novel conceptual framework and operationalization of that framework in practice.

2. The U.S.: How Historical Strength can be a Disadvantage in Cyber-Defense

"We weren't in the business of whole of society defense."
- Former U.S. Government Official[196]

The U.S. is widely regarded, alongside Israel, as one of the first movers in this area, publishing its first cybersecurity strategy in 2003 (The National Strategy to Secure Cyberspace drafted by the

194 See Chapter Two for a more detailed discussions of large states facing societal defense problems
195 A term used by a Finnish officer in the Ministry of Defense to refer to the role of industry as an explicit security actor and not just as a support for the military through the defense industrial complex. Author's Interview, 2018.
196 Lunch meeting with former US government official, 2019.

Department of Homeland Security (DHS)).[197] Within the pages of that first strategy, the U.S. recognized that it faced what I argue is a type of societal defense problem in the cyber era: "[s]ecuring cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people."[198] Yet, developing a deploying a mature model to address this reality has proven to be uniquely challenging given the degree to which such a model represents a departure from prior national defense efforts.

2.1. Historical Background: Great Power Competition

Unfortunately for the U.S., in contrast to the Mice that Roar, its historical approach to national defense was maladapted to this reality of cyber-defense. Historically, the U.S. defense posture (post-WWII) was primarily geared toward great power competition[199] (balancing and deterrence through Mutually Assured Destruction (MAD)),[200] and projecting power abroad. Conflict was something waged elsewhere, not within the U.S. territory. In fact, the U.S. had not fought a war in its territory since the 1800s. National security was the responsibility of the military and intelligences services not the American people more broadly. Security threats were largely military in nature, though post-9/11 this had been expanded to irregular deployment of force by non-state actors and concerns over the psychological impacts of terrorism on the population. 9/11 had also resulted in the creation of the Department of Homeland Defense (DHS) an agency responsible for the internal aspects of security such as border control and terrorism. Notably, the U.S. counter-terrorism effort centered prevention with a strong intervention abroad and preemption flavor.[201] In addition, industry's connection to national defense goals was limited and fell within three broad categories: the defense industrial base, R&D investments through programs such as the Defense Advanced Research Projects Agency (DARPA),[202] and contractors to support operations.[203] In short, in the U.S., the responsibility for national security was not jointly held by private and public actors, industry and government, militaries and citizens and conflict was something that primarily occurred elsewhere, outside its borders, or was fended off through preventative measures.

[197] U.S. White House, "The National Strategy to Secure Cyberspace."
[198] U.S. White House. p. vii.
[199] Idrees Ali, "U.S. Military Puts 'great Power Competition' at Heart of Strategy: Mattis - Reuters," *Reuters*, January 19, 2018.; Hal Brands, "One War Is Not Enough: Strategy and Force Planning for Great Power Competition | American Enterprise Institute - AEI," *Texas National Security Review*, March 1, 2020.; U.S. Department of Defense, "The National Military Strategy of the United States of America," 2015.; and U.S. Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," 2018.
[200] Robert Jervis, "The Dustbin of History: Mutual Assured Destruction," *Foreign Policy*, November 9, 2009.
[201] Terrorism and to a more limited degree, climate change (which is now become highly politicized across the two-party system) resulted in the U.S. scoring "limited" in the category of "threats to national security not limited to kinetic, military operations. Though neither terrorism nor climate change led to a robust focus on non-traditional security threats more broadly or the inclusion of phycological aspects of defense robustly at either the strategic or operational level within the homebase/homeland.
[202] Formerly, he Advanced Research Projects Agency (ARPA). Th name changed to DARPA in 1972, reverted back to ARAP in, and then returned to DARPA from 1996 onward. "ARPA Changes Names," DARPA, accessed July 20, 2020, https://www.darpa.mil/about-us/timeline/arpa-name-change.
[203] Congressional Research Agency, "Defense Primer: Department of Defense Contractors Contractors as Individuals," 2020.

2.2. Developing a Cyber-Defense Posture: A Conceptual and Operational Disjuncture

Yet, it now found itself facing an imperative national security problem that required exactly that. Recall, the national security threat stemming from cyberspace is one where (1) the vulnerabilities are society-wide, embedded within the functioning of civil society, government, and the economy and (2) the resources states need to deploy in order to prevent an attack, defend against an ongoing attack, or recover from a previous attack are largely housed outside the military and even the government itself, i.e. within industry and the civilian population. Therefore, in order to address the core pressing national security concern facing states seeking to provide defense for their populations in the cyber era (critical interconnectedness: their dependence on and the interconnectivity of cyberspace), states must structure national cyber-defense in a manner that does not rely on military or intelligence agencies as the sole or even primary defense actors while simultaneously integrating both public and private actors into a cohesive, real-time national defense posture.

Given the U.S.'s size and geopolitical position as a great power, this represented a new type of defense problem and would require a largely new type of defense architecture. As an important consequence of that disjuncture, the U.S. was faced with an existing national defense architecture that was maladapted to the realities of national defense in the cyber era: namely, a posture in which conflict is waged outside the homebase, the military and intelligence community are the primary security actors, and industry plays a limited security role. As one former U.S. policy official remarked, "we weren't in the business of whole of society defense."[204]

This mismatch lead to a cyber-defense posture that was defined by what one academic referred to as "messy" and another as "crowded"[205] despite the U.S. being frequently referred to as one of the earliest movers in the field.[206] More specially, the U.S. has been plagued by institutional complexity and density, a strong military and intelligence focus, limited success in operationalizing strategy (particularly as it relates to the private sector), a recognition that it need it needs to leverage its citizenry for defense purposes but also uncertainty over the best mechanism through which to pursue such an arrangement in practice, and a lack of clear leadership and oversight.

First, a large number of departments and agencies hold a piece of the cybersecurity portfolio: primary spread across and within the Department of Defense (including USCYBERCOM), the National Security Agency (NSA), the Department of Homeland Security (DHS) (including the Secret Service (focus on financial crime) and the recently created Cybersecurity and Infrastructure Security Agency (CISA)), and the Federal Bureau of Investigations (FBI). The U.S. cyber-defense ecosystem is characterized by silos.

While their remits are separable on paper to a degree, the large number of actors and the scope and scale of cybersecurity threats have resulted in uncertainty in practice. For example, when speaking to a Department of Homeland Security (DHS) official about who would be responsible for which types of incidents, they admitted that, in practice, it often "depends on who they [a company or

204 Lunch meeting with former US government official, 2019.
205 Informal conversation with fellow academic experts at CyCon 2018.
206 Piret Pernik, Jesse Wojtkowiak, and Alexander Verschoor-Kirss, "National Cyber Security Organisation: United States" CCD COE (Tallinn, 2016).

industry player] chose to contact" within the government infrastructure.[207] This institutional complexity and density was also reflected in my interviews in Estonia, Finland, Israel, and Singapore. One Finnish cybersecurity expert working in incident response at the national level remarked that they know who to speak to in their neighboring countries but when it came to the U.S. there was too much turnover in personnel and too many institutional options.[208] A second Finn echoed this concern stating that perhaps the best strategy was to reach out to someone they knew and then have them direct them on from there.[209]

Second, as previously noted, one of the biggest differences between the U.S.'s existing approach to national defense and the necessities of cyber-defense relates to the private sector and a strategy that leverages resources across society to bolster the defenses of the homebase. While DHS (which was named the official lead of cybersecurity efforts located within the civilian sector in 2003) [210] is tasked with providing cyber security support to critical infrastructure sectors,[211] it lacks a robust set of tools for doing so. It currently has no regulatory power over critical infrastructure, instead leaving that power distributed across the various regulatory authorities responsible for each sector. As a consequence, the relationship between critical infrastructure and DHS remains largely voluntary, with the most robust cooperation occurring with the defense industrial base (with which there is a long history and legal framework that can be leveraged).[212] Critical infrastructure providers have also expressed concerns over severe limitations to the U.S. approach in addressing the security, resilience, and preparedness of the critical functions of the state and society citing a pattern of lack of communication,[213] skilled professionals, and resources. This concern was shared the United States' General Accountability Office (GAO). GAO released a report in 2013 "noting that the private sector had not fully engaged with the government's cybersecurity strategy and had not done enough to protect critical infrastructure against cyber threats arguing that the government had simply expected the private sector to follow voluntary, yet costly and challenging guidelines."[214]

These persisting limitations regarding leveraging industry as security actors in practice as part of a cohesive, real-time defense posture was a significant focus of the US's second cybersecurity strategy (published 15 years after the first strategy), [215] This 2018 strategy, established the Cybersecurity and Infrastructure Security Agency (CISA) in attempt to more robustly tackle the persisting challenge of addressing a deeply vulnerable homebase in an era of cyber conflict. Despite this restructuring, which elevated the prior mission of the National Protection and Programs Directorate (NPPD) under DHS into a standalone federal agent operated by DHS, the relationship with industry remained largely voluntary and fundamental concerns – such as building trust,[216] sharing useful and actionable information between government and the private sector, and integrating the private sector into a cohesive nation-wide crisis response framework – continue to dog efforts. This institutional landscape and persisting limitations to the operationalization of defense of society in-

[207] Author's Interview, 2019.
[208] Author's. Interview, 2018.
[209] Author's Interview, 2018.
[210] DHS is also tasked with coordinating the security of civilian government networks.
[211] Singer and Friedman, *Cybersecurity: What Everyone Needs to Know*. p200–201.
[212] Author's Interview with Government official in DHS. 2019.
[213] Charlie Mitchell, *Hacked: The Inside Story of America's Struggle to Secure Cyberspace* , *Rowman & Littlefield Publishers*, Kindle Edition, 2016: p81-100.
[214] Lim Wei Chieh, "Policy Analysis: Singapore's Public-Private Partnerships for Cybersecurity in the Critical Infrastructure Sectors — Challenges and Opportunities" (Lee Kuan Yew School of Public Policy (LKY School), National University of Singapore, 2017).
[215] U.S. White House, "National Cyber Strategy of the United States of America," 2018.
[216] For example, refer to Jory Heckman, "CISA Focuses on Building Agency Trust in Data as Part of Upcoming CDM Dashboard," *Federal News Network*, June 9, 2020.

depth led one Israeli government official to argue that while Israel has been actively building out critical infrastructure protection and an approach to safeguard the economy and civil society for over 16 years now, the U.S. only really began this effort in earnest in the last 2-3 years (a period that overlaps with the creation of CISA).[217]

The persistent limitations of these efforts have also been reflected in the closed-door meetings with U.S. policy makers, academic experts, and industry professionals focusing on public-private cooperation and coordination. As one example, in one meeting I attended an official sitting next to me with over a decade of experience in government working in this space began preempting the buzzwords seconds before they were mentioned in the wider conversation: 'what we need to do is build *_trust_* trust', 'security isn't enough, we need to be *_resilient_* resilient too', 'it is not enough to ask for industry to cooperate, we need to offer *_incentives_* incentives', etc. As we walked out of the meeting together they expressed their frustration, claiming that these were all well-known limitations to the U.S. system and noting that we needed to move on from rehashing the problems to building out solutions.[218] The U.S. has taken the necessary first step of recognizing the important role the private sector must play as security actors within a broader national cyber-defense posture, but given a lack of conceptual and institutional overlap in this area, the U.S. has struggled to develop a mature model for achieving that recognition in practice.

The areas where engagement with the private sector is strongest also happen to be the areas where there are pre-existing foundations. As previously mentioned, the relationship between critical infrastructure and DHS remains largely voluntary except where there is a long history and legal framework that can be leveraged: the most robust cooperation occurring with the defense industrial base.[219] The same pattern can be seen in R&D investments. As Aggarwal and Reddie note, venture capital has served as an important mechanism to bolster U.S. capacity within the market historically and that has been leveraged to address cybersecurity concerns: "Washington uses an increasingly prominent investment vehicle – venture capital – to provide government support to projects of importance to national security, including cybersecurity. […] The founding of Palantir in 2003 with $2 million in venture capital funding from In-Q-Tel – led by a group of former CIA officials – serves as the prototypical example of this pattern of interaction."[220] Both in terms of engagement with critical infrastructure and in deploying R&D to bolster capacity, the U.S. cooperation has been most robust in areas with strong historical legacies that the U.S. can has deliberately and explicitly built upon.

Having a vibrant cybersecurity sector does not automatically translate into a robust cyber-defense posture. This requires mechanisms for leveraging industry expertise into government but also out into industry and civil society. In other words, it is not enough to have technical and process solutions available. States need to structure their engagement with industry in a manner that provides visibility into those ideas, allows them to select particularly promising ideas to either further develop or leverage most as is, and then structure and disperse those ideas across a complex ecosystem. The U.S. has made some strides in this area through the work of DHS but also by standing up innovation centers within agencies such as the Directorate of Digital Innovation (DDI)

217 Author's Interview. 2018.
218 Closed door meeting in Washington D.C. 2019
219 Author's Interview with Government official in DHS. 2019.
220 Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: The US Case." p461.

within the NSA, which DDI focuses on accelerating digital innovation across the intelligence community.[221] Yet, notably, Aggarwal and Reddie argue,

> This type of interaction between government and industry that is focused on a particular area of demand reflects a historical pattern. Indeed, amid postwar downsizing following WWII, Op-20-G (a naval intelligence agency) alumnae spun off Engineering Research Associates (ERA) to continue the development of early computational machines on government contracts without an official bidding process in what was the first example of this practice. This relationship between private contractors with close ties to government continued to grow over the course of the Cold War era.[222]

In short, while the U.S. has been able to leverage areas where it has historic foundations, those foundations have not proven robust enough to address the need for a public-private cooperation and coordination for cyber-defense. As U.S. Secretary of Commerce Penny Pritzker noted in her 2016 remarks to the Commission on Enhancing National Cybersecurity, this has consistently been a challenge: "[t]oday, our cybersecurity posture is failing to keep pace with the incredible innovations of our time".[223]

Fourth, while the role of industry in cyber-defense has been expanded to include a recognition that the character of the economy can be a national security imperative, this recognition has not been accompanied by nuanced or robust policy beyond the defense industrial base. Take, for example, the ongoing debate over 5G in the U.S. There is widespread recognition that "concerningly, the entire life-cycle of development, deployment, operation, and maintenance of network infrastructure, services, and devices will introduce new potential sources of vulnerability and opportunities for malicious activity, intentionally or otherwise" and that security of supply must, therefore, be a priority.[224] Yet, as David Forscey and Herb Lin pointed out in their Lawfare article, the U.S.'s current approach - 'just say no' to Chinese technology - is not an effective strategy for supply chain security if it is not accompanied by robust domestic market or allied country alternatives across the 5G ecosystem. In other words, for the U.S. to exclude Chinese technology from certain areas of its critical infrastructure, it would need to leverage marketcraft, or industrial policy, for national security purposes within the economy more broadly than the more recent historical focus on the defense industrial base. Such marketcraft would need to target innovative solutions for civilian infrastructure alongside government, including military and intelligence, infrastructure.

Strikingly, despite having the most robust and diverse domestic ICT and cybersecurity market, the U.S. has not been able to leverage those industry resources in a dynamic and agile fashion for the defense of society. Nor has it been able to develop a suite of domestic alternatives to foreign products within some of its most critical of infrastructures given that marketcraft and national security remain institutionally siloed and largely conceptually distinct lines of effort rather than deeply intertwined in purpose or practice. These efforts are further hindered given that in recent year's even the term 'industrial policy' has become increasingly partisan and, therefore, controversial.

Fifth, the U.S. tilt toward the military and intelligence apparatus and away from civilian and industry players remains apparent in the cybersecurity budgets of these agencies. In 2017, the DoD's fascial-year cybersecurity budget totaled $7.224 billion. The allocated budget rose to $8.497 billion for

[221] Aggarwal and Reddie. p451.
[222] Aggarwal and Reddie. p451.
[223] Penny Pritzker, "U.S. Secretary of Commerce Penny Pritzker Details Cybersecurity Challenges Faced by Cabinet Secretaries in Speech to Commission on Enhancing National Cybersecurity" (U.S. Department of Commerce., 2016).
[224] Griffith, "5G and Security : There Is More to Worry About than Huawei." p2.

2019.[225] Notably, neither of these figures include the NSA's cybersecurity budget, which is not publicly available. In comparison, DHS's 2017 budget only totaled $1.6143 billion, which rose to $1.7246 billion allocated for 2019.[226] While these are all large numbers in comparison to any budgets Estonia, Finland, Israel, and Singapore could muster, they also demonstrate a sharp disparity between the prioritization of cyber-defense within military and intelligence functions and the prioritization of civilian government networks, critical infrastructure, and private sector focused efforts. As previously noted, the defense and intelligence community have also been able to leverage existing, though limited in the context of cyber-defense, frameworks when building out a cyber-defense posture through the defense industrial base and R&D within the intelligence community.

Sixth, given that the U.S. has not historically relied on citizens more broadly in defense of the state (except in periods of warfare where there is a draft) and it does not have a universal, public education system, it lacks two core mechanisms utilized by the Mice that Roar through which to leverage citizens as security actors. Both the concept of citizens as security actors and the operational realties required to leverage them as such in practice are largely novel for the U.S. As a result, education initiatives have been focused less on the citizenry as whole and instead on addressing specific aspects of the skills gap within government and industry. One such example is the National Initiative for Cybersecurity Education (NICE) under the auspices of the Department of Commerce's National Institute of Standards and Technology (NIST).[227] Established in 2012, NICE is a joint effort by the federal government, industry, and academia to bolster cybersecurity education in order to address workforce needs. Another example is the DoD's Cyber Scholarship Program (CySP), which bills itself as "both a scholarship program for the DoD, and a capacity building tool for the nation."[228] CySP offers financial support for students enrolled in universities designated as a National Center of Academic Excellence in Cybersecurity in exchange for working in the DoD post-graduation as well as educational support for current DoD employees. Notably, this effort first funnels talent into the government, specifically the defense apparatus, before allowing them to either continue to work in government or leave government for industry.

The lack of conceptual and institutional foundations regarding citizens as security actors has also led to calls for a national level initiative and efforts at the subnational level. Notably, many of these efforts specifically mention existing institutions within some of the Mice that Roar that do leverage citizens in defense of the state in practice as well as some potential existing institutional foundations more broadly within U.S. that could underpin such an effort conceptually and operationally. Take, for example, calls to create a Civilian Cybersecurity Corp, which would be "modeled after a blend of cybersecurity organizations in other nations and proven models in other domains of security and safety inside the United States, specifically the Civil Air Patrol, Coast Guard Auxiliary, or Volunteer Firefighters."[229] Notably, despite a lack of a national level organization, efforts within the U.S. to leverage citizens more broadly in defense of the state in an era of cyber conflict have occurred at the local level rather than the national level within some U.S. states. For example, Ohio created its own

225 Office of Management and Budget, "21. Cyber Security Funding," in *An American Budget: Analytical Perspectives* (U.S. Government Publishing Office, 2017), 273–287: p274.
226 Office of Management and Budget. 274.
227 U.S. National Institute of Standards and Technology (NIST), "National Initiative for Cybersecurity Education (NICE)," accessed July 28, 2020, https://www.nist.gov/itl/applied-cybersecurity/nice.
228 U.S. Department of Defense, "Cyber Scholarship Program (CySP) ," accessed July 28, 2020, https://public.cyber.mil/cysp/.
229 Natasha Cohen and Peter Warren Singer, "The Need for C3: A Proposal for a United States Cybersecurity Civilian Corps," *New America Report*, October 25, 2018.

Ohio Cyber Reserve (OhCR) in October of 2019.[230] The OhCR plays two roles within Ohio: first, it helps bolster education initiatives in the area with reservists serving as "mentors for high school cyber clubs" and second, created teams of trained civilians "to assist eligible municipalities with cybersecurity vulnerabilities and provide recommendations to reduce cyber threats".[231] However, state versus federal jurisdiction in the event of a cyber incident represents just one more silo plaguing the U.S. system. Moreover, efforts at both the state and national level to leverage citizens as security actors remain nascent and underdeveloped.

Seventh, and finally, this approach lacks comprehensive strategic and operational oversight, coordination, and visibility. While the position of a White House cybersecurity coordinator was created in 2016 to begin to address this issue, the position was eliminated just two years later in 2018. The importance of the position was articled by a commission established by President Obama, which had "urged elevating the cybersecurity coordinator job and turning the position into an assistant to the president, on par to the assistant to the president for counterterrorism and homeland security — a reflection that various federal agencies did not have clear lines of authority or clear strategies in cybersecurity."[232] After its elimination, legislators introduced an act in an attempt to codify a similar position within the White House through a National Office for Cyberspace in the Executive Office of the President.[233] They argued that "the White House needs a senior coordinator who can rise above inter-agency rivalries and has the ear of the president".[234]

This view is consistent with other assessments of the current state of the U.S. cyber-defense posture. For example, the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia described the U.S. approach to cybersecurity policy to date as "piecemeal measures" rather than comprehensive in nature.[235] Notably, as of 2016 alone, over 50 statutes addressed cybersecurity concerns and priorities from a wide diversity of angles and "[m]ost of the existing documents address national priorities from narrower cyber security areas, which furthermore leads to variance in terms of priorities and structure, and also fails to specify how they link to or supersede other policy."[236]

230 Ohio National Guard Public Affairs, "Ohio Gov. Mike DeWine Signs Cyber Reserve Legislation," *Ohio National Guard Adjutant General's Department*, October 25, 2019.
231 Ohio National Guard Adjutant General's Department, "Ohio Cyber Reserve," accessed July 28, 2020, https://www.ong.ohio.gov/special-units/cyber/ohcr/index.html.
232 Nicole Perlroth and David E. Sanger, "White House Eliminates Cybersecurity Coordinator Role," *New York Times*, May 15, 2018.
233 Sean Lyngaas, "Lawmakers Introduce Bill to Save Top White House Cyber Job after Bolton Eliminated It," *Cyber Scoop*, May 15, 2018.
234 Lyngaas.
235 Pernik, Wojtkowiak, and Verschoor-Kirss, "National Cyber Security Organisation: United States."
236 Pernik, Wojtkowiak, and Verschoor-Kirss. p7

2.3. Conclusion

The U.S. cyber-defense posture remains highly siloed and fragmented between a series of departments, agencies, and commands. There are three important consequences of this approach. First, the U.S. lacks a cohesive strategic vision and architecture for and oversight over cyber-defense efforts. Second, the U.S. lacks a cohesive or streamlined mechanism needed for real time crisis response in complex situations. Third, although the U.S. identified the importance of leveraging all of society in order to address a uniquely vulnerable homebase in the cyber era as early as 2003, the operationalization of those strategies have remain severely limited in practice.

The U.S. Pivot from Great Power Competition to a Societal Defense Architecture		
Components of National Cyber-Defense	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**
Threats to national security not limited to kinetic, military operations	LIMITED	YES
The homebase as a location for conflict	NO	YES
Citizens as security actors	NO	RECOGNIZED
The private sector as security actors	NO	RECOGNIZED and DEVELOPING
The breadth and character of the economy as a national security imperative	LIMITED	RECOGNIZED
Strategic and operational oversight, coordination, and visibility across the defense-ecosystem	YES	DEBATED

None of this is to imply that significant progress has not been made or that cybersecurity experts from the operator up to the policy maker are not dedicated to addressing national defense in this area. Rather, their best efforts are running up against and are being hampered by the 'newness' of this defense problem for the U.S. Given the severity of the disjuncture between historical defense approaches and the realities of deep vulnerability born from critical interconnectedness, it is not surprising that there have been suggestions that the U.S. should look beyond national security models to structure a whole of society effort such as natural disaster response and public health.[237]

Importantly, as the remainder of the case studies in PART II demonstrate, it is not accurate to claim that national defense in air, land, and sea did not require states to leverage resources across its government, industry, and citizenry to cohesively address deep vulnerability. It just so happens, however, those models for national defense lay out the great powers and can instead be found in small, precariously placed states. These lessons hold as much importance for small states as they do

[237] Though, given the U.S. crisis management of covid-19 the same limitations may be found in these other spaces as well (lack of a cohesive whole of government and whole of society approach).

for great powers. As Secretary of Defense James Mattis cautioned in 2018, "[i]t is now undeniable that the homeland is no longer a sanctuary."[238]

3. Finland: A Resilience-Based Societal Defense Architecture

"Resilience is in our DNA."
– Two Senior Finns within the Ministry of Defense[239]

What explains Finland's apparent meteoric rise as a leader in cyber-defense and cybersecurity at the national level? For Finland, national security concerns stemming from critical interconnectedness share conceptual and operational foundations with historical national security concerns as a result of being a small, precariously placed state.

This section proceeds in three parts. First, I provide background on Finland's national defense posture. This includes background on Finland's geostrategic position, defense strategy, and defense architectures (how the strategy was operationalized). Second, I illustrate how this foundation was directly leveraged into Finland's cyber-defense posture and that it conceptually and operationally overlaps with the structural realties of cyber-defense. Third, I review several persisting challenges as Finland continues to build out a cyber-defense posture that addresses increasing critical interconnectedness.

3.1. Historical Background: Size as a Kind of Societal Defense Problem

For Finland, which gained its independence from Russia in 1917, the early years of independence were fragile and characterized by conflicts against far larger and well-resourced neighboring states. During this period, two particular wars animated Finnish military history and captured the national imagination: the Winter War (1939–1940) and the Continuation War (1941–1944).[240] Notably, both of these wars feature a far larger, Russia, and were fought in close historical proximity. Even more notably, despite being the defeated party in the Continuation War,[241] Finland was able to maintain its independence as a democratic state on Russia's doorstep throughout the Cold War. This outcome was far from certain and surprising given Finland's relative size. As Michael Peck, contributing writer for the National Interest, remarked, "the popular story of the Russo-Finnish conflict of World

238 "U.S. National Defense Strategy | Wilson Center," Woodrow Wilson Center, 2018, https://www.wilsoncenter.org/article/us-national-defense-strategy?gclid=CjwKCAjwltH3BRB6EiwAhj0IUPANMronOUeCHyVki1f1M8VAmOrroUO4Q498nFyhamCOHYMGyGmsuBoCEHwQAvD_BwE.

239 Author's interviews with a Senior Finnish Officer and Official tasked with Cybersecurity and Comprehensive Security respectively within the Ministry of Defense, 2018.

240 For more information on the Continuation War, refer to Vesa Nenye et al., *Finland at War: The Continuation and Lapland Wars 1941–45*, Kindle Edition (Osprey Publishing, 2016).

241 What one interviewee referred to as 'Lady Finland losing its left arm'. If you look at the map above, you can see that the territory of Finland loosely resembles a woman with her right arm raised above her head. There was a similar strip of territory to the east similarly positioned at the start of the Continuation War. That arm extended up to the arctic ocean but by the end of the Continuation War, Lady Finland lost its left arm and its border with the arctic ocean. Author's Interview, 2017.

War Two remains a David versus Goliath tale of outnumbered but nimble Finnish ski troops zipping around massive but clumsy Soviet divisions."[242]

In the period directly following the end of WWII and throughout the Cold War, Finland found itself as a neutral buffer state between the East and West. This left Finland in the position of facing a military threat and economic threat directly on its border from a far larger state with which it had a history of conflict, while also being explicitly constrained in its ability to externally balance that threat through bandwagoning with the U.S. and a collection of European states through the North Atlantic Treaty Organization (NATO). As Will Inboden, executive director of the William P. Clements, Jr. Center for History, Strategy, and Statecraft at the University of Texas-Austin, explained:

> "Finlandization," originally a term of derision that eventually became a term of art, described Finland's status as a neutral buffer state during the Cold War. Reflecting Finland's precarious geography of a long shared border with the Soviet Union, further complicated by a shared history of some years under Russian territorial control, the term Finlandization represented an implicit bargain by all parties in the Cold War conflict to resist any provocative steps to change the status quo. For the West this meant not inviting Finland into NATO; for the Soviet Union it meant not invading or otherwise seizing control of Finland; for the Finns themselves it meant keeping their heads down, accepting a significant measure of Soviet influence on their domestic governance and foreign policy, and not making any overt efforts to align with the West.[243]

Even after the end of the Cold War and the fall of the USSR, Finland has officially remained outside of NATO's formal membership structures and thus not officially part of the collective defense opportunities and benefits afforded to member states. Though, it has participated in NATO's Partnership for Peace Program since 1994.[244]

Finnish security policy is centered on the defense of society, ensuring that this defense posture does not provoke a larger neighboring state (i.e. Russia) which poses both a kinetic threat and economic challenge. As consequence, Finnish officials have pointed publicly to the importance of maintaining good relations with Russia, while also maintaining that maintaining good relations is not appeasement since Finland does maintain capabilities for its defense.[245] This specific emphasis on tailoring public security policy, rhetoric, and posturing in order to not aggravate a particular regional power who represents a substantial national security concern was also strikingly reflected in interviews. Finns frequently referenced 'potential threats from the East' as shorthand for a consistently unnamed Russia. One academic and reservist I interviewed referenced a joke that a senior Finnish political leader had made several years prior: "threats could come from anywhere: the north east, the south east, the mid-east".[246] For Finland, efforts in any security space walk a fine line

242 Michael Peck, "How Finland Lost World War II to the Soviets, But Won Peace | The National Interest," *National Interest*, August 19, 2016.
243 Will Inboden, "Is Finland Rejecting 'Finlandization'?"," *Foreign Policy*, December 1, 2014.
244 Finnish Defense Forces, "NATO's Partnership for Peace Programme - Puolustusvoimat The Finnish Defence Forces," accessed July 20, 2020, https://puolustusvoimat.fi/en/international-activities/natos-partnership-for-peace-programme.
245 Standish, "How Finland Became Europe's Bear Whisperer."
246 Author's Interview, 2018.

between publicly and privately addressed issues and concerns stemmed from its relative size and geostrategic environment.

Keeping this historical context in mind, as a relatively small country bordering a much larger power, Finland's defense posture has developed out of the following concern: how can a smaller country, which in times of crisis and/or war would in effect be an island, ensure the performance of its economy, society, and defense forces in the face of external, aggressive action? Finland's answer is that to "safeguard its independence and territorial integrity",[247] public and private actors alike can be and often are security actors (*turvallisuustoimija*), critical in maintaining and providing for the vital functions of society (*yhteiskunnan elintärkeä toiminto*) in times of crisis. National security, therefore, is directly tied to the interdependencies between different actors as well as the management and harmonization of these various actor's goals and interests.

There are three important insights encapsulated in this concept of comprehensive security, as laid out in the country's Societal Security Strategies.[248] First, as a small country living next to a regional and historically active power, defense of society is a task that requires the mobilization of vast resources. This means that the responsibility for security cannot only be housed within the defense forces alone but also with civilian society being prepared for war even during peace time in order to ensure national survival in times of crisis.

Second, threats to national security do not need to be military in nature to be incredibly costly or crippling. Namely, a threat does not need to be tanks rolling across the border or the physical destruction of power lines by Russian forces. A winter storm that knocks out power in winter can be just as deadly and live Finland just as vulnerable. Therefore, the crux of comprehensive security is that, regardless of the cause of crisis, private and public actors must ensure and safeguard the continued delivery of certain functions in times of peace so they are resilient in times of conflict.

Third, the homebase is understood as a potential area of conflict (in fact, Finland is focused on absorbing Russian aggression into its territory while leverage geographic features of its territory to enable activity such as dispersed units on skis engaging in skirmishes and guerilla warfare, and continuing to fight as long as possible). Unlike the U.S., which has not had to fight a war on its own territory since the 1800s, for Finland not only is the homebase assumed to be deeply insecure but the security strategy specifically addresses it as a venue for conflict. Conflict and warfare are not something that happens somewhere else; it happens at home.

Comprehensive security planning in Finland is more than just political rhetoric. It includes the identification of specific infrastructure and services vital to resilience in a time of crisis while also detailing operational responsibilities to ensure that resilience ranging from the municipal to the national level for both private and public actors. Finland's most recent Security Strategy for Society identified three broad areas of activity: (1) regular threat and risk assessments that take into account the interdependencies and vulnerabilities within the entire system and not just within a specific sector or organization, (2) crafting and implementing operational guidelines and assigning responsibilities across all sectors and levels of government to be implemented during a crises, and

[247] "Security Strategy for Society" English Translation (2017). p18.
[248] The first societal security strategy was published in 2003, entitled "Strategy for Securing the Functions Vital to Society". This first strategy was followed up three years later in 2006 still using the same name. The name was changed for the third iteration in 2010 to "Security Strategy for Society". "Security Strategy for Society" was also utilized for the latest and fourth iteration released in 2017.

(3) crafting and implementing operational guidelines and assigning responsibilities to be implemented during the aftermath of or recovery period following a crisis.[249]

One central component of Finland's comprehensive security approach is a focus on maintaining the security of supply (*huoltovarmuus*), both in terms of essential infrastructure but also in terms of the goods and services they provide. The central organization responsible for coordinating security of supply, the National Emergency Supply Agency (NESA), is a public-private partnership. Charly Salonius-Pasternak, a Senior Research Fellow at the Finnish Institute of International Affairs and former International Affairs Advisor to the Finnish Defence Forces, explains the central role of the NESA in planning crises:

> The National Emergency Supply Agency (NESA) coordinates twenty-one 'planning pools' (examples include the media, healthcare, transport, communications, and so forth) to ensure that different sectors continually update plans, including for the way in which private sector competitors can deliver services through each other's logistics or service networks. In addition to this, NESA oversees through partnerships and contracts reserves of energy, foodstuffs, pharmaceuticals and other raw materials. It also plans and pays for redundancy and support arrangements for IT systems, financial services and communications.[250]

In addition to building models and assigning responsibilities for these "planning pools", the NESA carries out exercises with its array of public and private partners to better assure preparedness in times of crisis. Through NESA, industry is an explicitly security actor within the Finnish defense posture.

A central second component is the creation of shared understandings of the threat environment and mechanisms for collective action. Despite the reoccurring joke that Finland is a small country and that everyone knows each other, Finland has put significant effort into building strong networks and trust in order to allow for shared understandings of threats and coordinated action in addressing them. As previously discussed, building coordination and cooperation is a core component of the Societal Security Plans. In their strategic inception, these plans could best be described as an effort to modify the behavior of both private and public actors through an array of statuary requirements, government resolutions, and voluntary participation in established frameworks for national security purposes.

Moreover, this focus is mirrored through other specific deployments of this comprehensive security model, such as Finland's National Defence Courses. These courses are explicitly designed to 'improve cooperation between different sectors of society and facilitate networking of people working in the various fields of comprehensive security' by bringing together various leaders in industry with political and military elites.[251] These courses are held at a variety of levels ranging from national to regional. The national-level National Defence Courses are approximately a month in duration, providing ample opportunity for participants to gain a more nuanced understanding of Finland's foreign and security policy and begin to develop shared narratives around the national interest.

[249] "Security Strategy for Society."
[250] "Security Strategy for Society."
[251] The National Defence University (NDU), "National Defence Courses," 2018, http://maanpuolustuskorkeakoulu.fi/en/national-defence-courses.

A third core component of the Finnish societal defense posture relates to an explicit effort to improve the math between Russia and Finland by leveraging citizens as security actors. In additional to a standing military, Finland has a general conscription system, where a large percentage of the Finnish Defence Forces are comprised of reservists rather than career military personal. Service is mandatory for men (ages 18-60) and voluntary for women. The Ministry of Defence explained, pointing explicitly to the need to be capable of defending its territory without the assistance gained from a military alliance, "Finnish conscription meets the requirements of the security environment and generates sufficient resources for the Army, Navy and Air Force to act effectively in a crisis or war situation."[252] In other words, conscription (including a period of active military and reserve service) is "a cost-effective way of generating a large and capable reserve"[253] for the state to draw upon when need arises.

A forth, and final, core component of Finland's historical defense posture centers the breadth and character of the economy not just as a critical component of prosperity but as a national security imperative. Historically, for Finland, economic prosperity is as necessary for maintaining its long-term independence as capabilities tailored specifically to the conflict prevention, warfighting, and conflict cessation. This has largely taken three forms.

First, in pursuit of this goal and as a relatively small country with limited resources, Finnish market-oriented policies have long had a component of active market intervention.[254] It found success in "riding the wave"[255] of globalization through employing specific marketcraft (i.e. broad market interventions defined by Steven Vogel as "how and why governments make markets work"[256] through a "range of market-oriented policy actions"[257]). By the late 20th and early 21st century, this marketcraft had resulted in an export-led, knowledge-based economy comprised of three broad sectors (the ICT industry, the technology industry (minus ICT), and the forestry industry).[258] This effort leveraged a systems-based approach with contributions from and feedback effects between industry, educational institutions, and government. For example, the creation of a publicly funded, largely comprehensive education system, formed the bedrock of educational outcomes within the country and played an important role in Finnish efforts to transition to a knowledge-based and hi-tech economy.[259]

Second, there is a long history of 'government as customer' interventions in Finland including the notable role Nokia played in providing secure communication devices for the Finnish Armed Forces and in building out national communications infrastructure for the country as a whole.[260] This includes the creation of and government assistance with security of supply in critical sectors through NESA discussed above. This intervention targets goods and services that would not be provided, either in scope or in kind, by the market more broadly. However, due to national security concerns,

252 Finnish Defense Forces, "Finnish Conscription System - Puolustusvoimat The Finnish Defence Forces," accessed July 20, 2020, https://puolustusvoimat.fi/en/finnish-conscription-system.
253 Finnish Defense Forces.
254 The most recent internal devaluation is just one example. In this instance, the government struck a deal with labour to spur economic growth. For additional information refer to Tuomas Forsell and Jussi Rosendahl, "Finland Government Strikes Deal with Unions to Boost Stagnant Economy," *Reuters*, 2016.
255 Jyrki Ali-Yrkkö et al., *Riding the Wave: Finland in the Changing Tides of Globalization* (Helsinki: Research Institute on the Finnish Economy (ETLA), 2017).
256 Steven K. Vogel, *Marketcraft: How Governments Make Markets Work.*, Kindle Edition (Oxford: Oxford University Press, 2018). p1.
257 Vogel. p138.
258 Ali-Yrkkö et al., *Riding the Wave: Finland in the Changing Tides of Globalization*..
259 Ali-Yrkkö et al.
260 Yvos Doz and Keeley Wilson, *Ringtone: Exploring the Rise and Fall of Nokia in Mobile Phones* (Oxford: Oxford University Press, 2018).

the state has created a security market, or a supply market, in which these goods and services are generated during times of peace specifically so that they can be utilized in times of crisis.

Third, there is a long history of 'government as funder' in Finland such as research and development through Business Finland, now VTT Technical Research Centre of Finland, operating under the mandate of the Ministry of Employment and the Economy. VTT is a leading research and technology institution in Europe serving both the private and public sector. VTT explicitly frames itself as residing at the intersection of two priorities: driving economic growth and addressing "the biggest global challenges of our time and turn them into growth opportunities".[261] VTT, like much of Finnish marketcraft, deliberately ties economics and security policy – seeing much of innovation, though not all, as a dual opportunity. Notably, for a small country, pursuing security in a manner that also bolsters economic growth and prosperity is a smart use of limited resources (human capital and government funding alike).

In conclusion, Finland has historically faced a societal defense problem born stemming from geopolitical concerns and its relative size. In response, it has built out a corresponding defense posture that emphasizes defense of society by maintaining society-wide resilience in the event of a crisis. Comprehensive security (*kokonaisturvallisuus*) is animated by a systems-based approach, which emphasizes the importance of interdependencies between individuals, firms, industries, universities, research organizations, and government ministries in achieving security. Notably, in comprehensive security, the responsibility for and the safeguarding of the vital functions of society are jointly held by private and public actors, industry and government, defense forces and citizens.

3.2. Developing a Cyber-Defense Posture: Areas of Overlap and Departure

Cybersecurity is not an end goal in and of itself. Rather, security enables other types of activity while insecurity undermines those activities. Cybersecurity - whether it is being discussed at the level of the individual, the firm, the state, or regional or international organizations - is in its most basic sense about protecting and defending your own use of cyberspace. This was explicitly recognized on the first page of Finland's 2013 Cyber Security Strategy: "Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured".[262] Economic, social, and government activity rely on and leverage cyberspace for their day to day functioning. Insecurity (whether the goal of an attack is espionage, disruption, or financial gain) can destabilize day to day operations, undermine trust, and result in significant financial and national defense costs.

With this reality in mind, Finland has set out to "ensure the security [or functioning] of society".[263] For Finland, security of society includes a series of verticals or activities such as "management of Government affairs, international activity, Finland's defense capability, internal security, functioning of the economy and infrastructure, population's income security and capacity to function, and psychological resilience to crisis".[264] In order to maintain critical services and infrastructure resilience, the government hopes to limit single points of failure, contagion, and crises of confidence by building in resilience to systems and seeking to harmonize goals and activity between ministries and an array of relevant private actors. This requires that Finland not only recognize the interdependences between individuals, firms, industries, universities, research organizations, and

[261] VTT Technical Research Centre of Finland, "What Is VTT," accessed July 20, 2020, https://www.vttresearch.com/en/about-us/what-vtt.
[262] "Finland's Cyber Security Strategy," 2013. p13.
[263] "Finland's Cyber Security Strategy." p1.
[264] "Finland's Cyber Security Strategy." p2.

government ministries but that they explicitly leverage strong private-public networks and levels of trust for cooperation and coordination.

Sound familiar? It should. For cybersecurity and defense, as in comprehensive security, the responsibility for and the safeguarding of the vital functions of society need to be jointly held by private and public actors, industry and government, defense forces and citizens.

For Finland, leveraging existing conceptual and operational foundations for cyber-defense purposes was both explicit and intentional. In interviews with two Finns intimately familiar with the cybersecurity working group which shaped the country's national Cyber Security Strategy, the subsequent strategy was conceived of as a sub-category of Comprehensive Security. This working group looked around for a framework for addressing national cyber-defense and security concerns and directly leveraged the existing defense-posture given its clear overlap with the requirements of security in the cyber-era. "[W]e took comprehensive security and just extended it".[265] This smoking gun – the admission that the development of a cybersecurity strategy/cyber-defense posture was the product of a direct extension of the historical defense posture – is consistent with observable outcomes. There was no need and no incentive to start from scratch.

Finland's Cyber Security Strategy and two subsequent implementation programs[266] have explicitly acknowledged that "the Cyber Security Strategy does not change the tasks defined in the Security Strategy for Society".[267] Cyber-defense in particular and cybersecurity more broadly are explicitly spoken of as a subset of this broader goal within the strategic and implementation focused documents. Cybersecurity as an emerging concern, does not fundamentally alter the broad strategy for providing security for its population through a focus on comprehensive security. If anything, it cements the importance of public-private partnerships and a broad range of actors as security actors.

Instead of laying at odds with the conceptual and operation realities of comprehensive security, cyber-defense is integrated within the existing framework. Cyber-attacks are understood as introducing a new set of avenues for crises. Cybersecurity then becomes both a foundational factor underpinning societal security and resilience as well as a specific concern within essential services such as data-communication systems, networks, and services. Consequently, Finnish policy efforts have focused on how to operationalize cybersecurity resilience within these already existing strategic frameworks. The 2013 strategy, for example, pointed to the addition of a new coordinating mechanism to the existing delineation of tasks and assigned responsibilities between the private and public sector. The newly created National Cyber Security Centre Finland (NCSC-FI), located under the Finnish Communications Regulatory Authority (FICORA), was tasked with maintaining cybersecurity situational awareness, assisting relevant authorities, and providing information and guidance.[268] CERT-FI, and its mission to provide solutions for and gather information on information and security threats, was then incorporated within this national information security authority. The Finnish Defense Forces, separately, were tasked to "create a comprehensive cyber defense capability for their statutory tasks".[269]

[265] Author's Interview, 2018.
[266] Finland's 2013 Cyber Security Strategy has been followed by two implementation programs, the most recent of which is the Implementation program for Finland's cyber safety strategy 2017-2020.
[267] "Finland's Cyber Security Strategy." p20.
[268] "Finland's Cyber Security Strategy." p20.
[269] "Finland's Cyber Security Strategy." p8.

Cybersecurity also made its way into the NESA's robust mandate in a variety of manners.[270] First, the NESA describes cyber insecurity as a potential cause of disruption in the security of supply and resilience of critical infrastructure and services. Second, the NESA identifies specific cyber intensive industry and services such as data-communication systems, networks, and services as critical infrastructure. Third, the NESA plans and pays for redundancy and support arrangements within the ICT sector, such as IT and communications systems. Fourth, the NESA added the Finnish national computer security incident response team, CERT-FI, as one of the authorities under its framework responsible for maintaining the security of critical infrastructure and services. Fifth, it conducts exercises to simulate potential crises and system-wide responses with clear cybersecurity components, such as those currently run in cooperation with the Technology Industries of Finland.[271] These exercises are important because the mandate for the defense forces and the government is to protect their own networks, thus leaving the core responsibility for protecting civilian networks to industry itself.[272]

This trend toward levering pre-existing institutional structures is also mirrored through other specific deployments of this comprehensive security model, such as Finland's National Defense Courses. Although the cybersecurity industry historically was not a common target of these courses, they are being folded into this structure, including the recent addition of a shorter, pilot defense course focusing on cybersecurity. Ultimately, these courses provide an important foundation of trust and lead to strong informal networks between leaders across various sectors of society and government, which leads to greater opportunity and more robust coordination down the line.

Yet, even for Finland, its historical societal defense posture is not entirely well suited to the dynamics of national defense in cyberspace. To address many of these points of departure, Finland has successfully leveraged its pre-existing focus on public-private cooperation and coordination into new venues for cooperation.

First, for example, the Finnish Information Security Cluster (FISC), which through its defense working group brings together cybersecurity industry and the defense community. Unlike the traditional defense industry, which has had built up shared vision and trust with government and defense forces over many years of iterated interactions, the cybersecurity industry remained largely outside these networks. In fact, defense industry originally had its own defense motivated cybersecurity working group, which Pekka Blomberg (a former Chairman of Cyber Defense working group from 2013 to 2017) helped to establish within the Association of Finnish Defense and Aerospace Industries (AFDA) as early as 2010. However, with the creation of FISC in 2012 containing the Finnish Information Security companies which were largely absent from AFDA, the decision was made to merge the FISC defense working group and the AFDA working group. The decision to merge sought to avoid competing structures and to further break down barriers between cybersecurity companies, government, and the defense industry. The merged group was located under the FISC umbrella. Notably, the defense working group was and remains one of the most popular working groups in the cluster in terms of attendance.[273]

[270] Tero Kauppinen, "Cybersecurity of Supply" (National Emergency Supply Agency presentation at the FIIF JAM SESSION., 2015).
[271] For example, the current (as of spring 2018) Chief of Preparedness, Pasi Eronen, at Technology Industries of Finland focuses on the overall cybersecurity posture and preparedness within Finnish industry and works closely with the National Emergency Supply Agency (NESA) to organize national level cybersecurity exercises.
[272] The National Emergency Supply Agency (NESA), "Security of Supply in Finland," 2018, https://www.nesa.fi/security-of-supply/.
[273] Two author's interviews, 2018.

FISC, whose membership is comprised of "companies and organizations that provide nationally important information and cyber security products and services", provides an important avenue for relevant industry and government to further break down barriers and build up coordination in the pursuit of comprehensive security.[274] Beyond the narrower category of defense, the group focuses on a range of topics formalized into specific working groups, including the three original working groups: the industrial internet, growth, and the aforementioned defense. FISC sought, in part, to form a bedrock of trust and shared understanding in order to facilitate informal and/or voluntary cooperation between industry and government. Notably, FISC membership is comprised of Finnish firms such as Bittium and F-Secure but also many foreign multinationals such as Microsoft and Cisco.

A second example is how Finland has sought to bolster the existing level of cybersecurity competency within in its general population by leveraging the existing general conscription system, where a large percentage of the Finnish Defense Forces are comprised of reservists rather than career military personal. One advantage to this system is that the military itself is able to leverage expertise from a wide range of sectors in its defense given that these individuals work across all of Finnish society. Another advantage is that the defense forces themselves can substitute existing levels of education by altering how it trains these conscripts. In fact, starting in 2015, the Finnish Defense forces began to offer cybersecurity training to all its conscripts.[275] These conscripts are able to deploy this baseline knowledge in the context of their service requirement but also when they return back to their civilian sectors. In addition to this broad training, specialized training was offered to a smaller number of conscripts that then returned to cybersecurity jobs within industry. By utilizing a pre-existing defense structure to address a broader societal need for cyber hygiene and awareness, Finland has partially addressed two broader concerns simultaneously: bolstering and maintaining cybersecurity competency within the defense forces themselves and improving cybersecurity competency within the broader civilian workforce.

A third, example relates to the need to adjust laws and regulations domestically to emerging cyber-defense realities. The government has facilitated cybersecurity development and activity by increasing its role as a customer of the cybersecurity sector, both in terms of purchasing commercial products and in contracting with firms in the production of government specific products. One impediment to government purchasing specific cybersecurity technology has been existing restrictions on intelligence activity, which prohibited the interception of confidential communications without the suspicion of a crime. This in turn limits mass data collection and analysis, which is widely recognized as a pivotal step in threat assessment and detection. The parliament is currently debating intelligence reform - two laws and one Constitutional reform are under consideration - centering around mass data collection and analysis of confidential electronic communications.[276] If these restrictions were to be removed and these proposed intelligence laws adopted, the government could invest in and purchase specific sets of cybersecurity capabilities that it had previously been prevented from investing in. This in turn creates the potential for a broader domestic market for these products, allowing companies to sell within Finland in addition to abroad.

274 Finnish Information Security Cluster (FISC), "Mission," 2018, https://www.fisc.fi/.
275 Tommi Hermunen, "Finnish Defence Forces Starts Engaging Conscripts in Cyber Defense," English Translation of Hermunen's Original Article in Finnish, 2015.
276 Reuters Staff, "Finnish Government Calls for Urgent Approval of Intelligence Bill," *Reuters*, January 25, 2018.

A fourth, and final, example stems from research and development. Notably, traditional R&D venues have been leveraged as a specific service for both the public and private sector. For example, in cybersecurity, VTT specifically focuses on the design, development, and testing of cybersecurity capabilities and operations for its customers.[277] But it also operates the Cyber War Room, which "includes a mini-Internet simulation environment that is completely isolated from all other telecommunications and where the devices or software being tested can be subjected to highly realistic cyber-attacks in a controlled way" allowing for stronger cybersecurity testing and analysis.[278] This marks a shift from innovation funding through joint engagement with private sector and government partners to include developing and maintaining services for the public and private sector that allow for security innovation and testing.

In conclusion, At the strategic level, Finland has laid out a vision of cyber-defense centered around ensuring the continued functioning of society in the event of crisis – a goal that lays at the heart of almost all countries cyber-defense strategies including the U.S. The specific task remaining then was the operationalization of this strategy: spreading and applying technological and industry expertise to broad swathes of industry, civil society, and government; information sharing and coordination in response to threats and in determining responsibilities between public and private actors; pooling of resources to stay ahead of the evolving threat landscape, maintaining critical infrastructure and services, etc. In an effort to build and flesh out this operational space, Finland has relied on a previous and well-established form of government intervention: its comprehensive security approach enshrined in its Security Strategy for Society. This form of security intervention and policy relies on a uniquely Finnish, systems-based approach. As a consequence, Finland's approach to comprehensive security including security of supply has led to cooperation between public and private actors that is both deep and daily in character and requires little day to day enforcement. Cybersecurity, as an underlying condition for continued delivery and functioning of other core services and industry as well as an important component of the provision of security of supply, has been readily incorporated into this pre-existing structure.

Given the two previously discussed important insights stemming from a concept of comprehensive security, this Finnish approach to national defense provides an institutional foundation that is well suited to the realities of addressing cyber-defense at the national level given the necessity of civilian industry in obtaining security and the scope and depth of harm cyberattacks can cost on a society without a corresponding deployment of military means. For Finland, its prior societal defense posture served not as a constraining force that led to the use of national defense approaches that were maladapted to cyber-defense's realities but instead as an important strategic and operational bedrock from which to build. As a government official tasked with cybersecurity operations stated during their interview, "[w]hat you call PPP, we just call Finland."[279]

3.4. Persisting Challenges

In other areas, however, Finland's kinetic societal defense posture has stood in contrast to the realities of critical interconnectedness. Three persisting challenges, points of departure, for Finnish cyber-defense efforts were raised repeatedly in interviews.

[277] VTT Technical Research Centre of Finland, "Services: Cybersecurity," 2018, http://www.vttresearch.com/.
[278] VTT Technical Research Centre of Finland, "Security Testing and Analysis," 2018, http://www.vttresearch.com/services/digital-society/data-driven-solutions/cyber-andinformation-%0Dsecurity/security-testing-and-analysis.
[279] Author's Interview, 2018.

First, despite its existing cybersecurity ecosystem[280] and its implementation of cyber-defense within a comprehensive security framework, Finland's approach to cyber-defense remains highly sectoral, siloed, and lacking in centralized management. While not essential for national defense efforts in air, on land, and on sea, given that cyber-defense lies at a series of intersections and cyberspace is notable as a highly interconnected domain where single points of failure, cascades, and dependencies are highly concerning, security and resilience efforts require a real-time 'whole of society' response. This integrated and comprehensive response is inhibited by a siloed system, broken down into specific sectors without clear strategic or operational oversight.

This was one of the concerns raised in the 2017 government report entitled, "Finland's cyber security: the present state, vision and the actions needed to achieve the vision"[281] and was further explored in the 2018 government report entitled, "Strategic management of cyber security in Finland"[282] a year later. Both reports were completed for the Prime Minister's Office. This has also inhibited efforts to assess gross national activity in this space given the lack of a strong centralized oversight or management of cybersecurity activities occurring within various ministries. Despite its strength in cooperation and coordination, efforts are hampered without clearer strategic management of all the various efforts occurring at all levels of government and in cooperation with various industry partners. Creating a new institutional structure to provide that organization and visibility has proven to be a slower and more difficult task than extending the existing societal defense posture in the early 2010s. Notably, the drafting process of the next Cyber Security Strategy, which is currently underway, has included a desire to address this lack of strategic management or ownership over cybersecurity at the national level. The degree to which it will be effective and the exact formulation it will take, remain to be seen.

Second, a frequently cited concern in informal discussions and interviews with key member of industry, is that the government's focus on cooperation and information sharing has not been accompanied by significant, public financial investments in cybersecurity technology or capacity outside of government ministries and the defense forces (i.e. these interventions lack the significant financial investments present in the approaches of other states which are announcing large sums of money to be earmarked toward the creation of and maintenance of cybersecurity competency and capabilities – namely Israel). Within the Finnish approach to cyber-defense, financial commitments are distributed between and buried within various ministries' budget making an overall assessment of such commitments challenging. There are some efforts occurring within the EU as well such as the 2018 call for proposals for a €50 million pilot under Horizon 2020, which would focus on the development of a research and development network across EU member countries seeking to address cybersecurity industrial challenges.[283] However, looking to other international examples,

[280] Finland has a robust cybersecurity industry. Despite being a relatively small country, Finland boasts a strong and diverse set of cybersecurity players including dedicated cybersecurity companies such as F-Secure (formerly Data Fellows), SSH Communications, and Stonesoft (acquired by Intel in 2011); cybersecurity consulting companies such as Nixu and Trusteq (acquired by KPMG in 2015); and dominant industry players with a strong cybersecurity research and competency components such as Nokia and Bittium. Finnish cybersecurity providers have been recognized for their strength in a wide range of tools including antivirus, anti-malware, firewalls, cryptography, and security testing. Dominant industry players such as Bittium and Nokia have likewise provided secure telecommunications networks and devices, wireless networks, health service platforms, automobile manufacturing, IoT and wearables, etc. to both the Finnish government and the broader civilian population. For more information on the breadth and scope of that industry refer to Griffith, "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity."

[281] Martti Lehto et al., "Finland's Cyber Security: The Present State, Vision and the Actions Needed to Achieve the Vision" (For the Prime Minister's Office, 2017).

[282] Martti Lehto et al., "Strategic Management of Cyber Security in Finland," 2018.

[283] European Commission, "Commission Launches a Call for Proposals for a €50 Million Pilot to Support the Creation of a Network of Cybersecurity Competence Centres across the EU," 2018,

many Finnish companies felt that financial commitments to cybersecurity in the civilian space were relatively weak and that this represents a central challenge to the provision of cybersecurity for Finnish society writ-large.

Concerns over cost, and gaps between investments and needed investments, also animate much of the discussion over Finland's strategic focus on resilience. Notably, the cost and scale of comprehensive security in an era of cyber conflict is far higher than what was required of national defense efforts in the domains of air, land, and sea for two reasons. First, given critical interconnectedness, which is simultaneously increasing and deeply complex, the task of resilience has increased in scale and scope. Previously, resilience was understood as a largely hierarchical process, with pillars or planning pools traditionally supporting ongoing efforts in the midst of conflict. In cyber-defense, resiliency is grappling with a space that is not linear and instead a web of interactions that could lead to cascades, contagion, single points of failure, etc. Second, recall, cyber-defense is grappling with conflict occurring within two strategic spaces: at or above the threshold of armed conflict and below in the grayzone. Finland's societal defense architecture was framed around leveraging resources across the society in times of peace so that they would be available in times of crisis (military conflict but also other potentially catastrophic events such as natural disasters). In cyber-defense, those times of crisis may not be accompanied by a land invasion and may be more dispersed in nature (constant contact rather than discrete events). How do you "bring industry onto warfooting"[284] for cyber-defense in a manner that is effective at a cost the country can bear? This concern is likely to only get worse as the domain itself – cyberspace – grows and evolves.

Third, and finally, as a relatively small country, Finland faces a unique set of concerns related to its size. Most notably, the question of securing the product lifecycle. Unlike, security of supply concepts at the heart of NESA's work, which focus on stockpiling reserves and maintaining a certain domestic industrial capacity for technology essential to the defense of the state, questions of domestic capacity in cyber-defense are far broader and do not readily lend themselves to a stockpile model. Finland's Cybersecurity Implementation Programme for the years 2017-2020 has emphasized the importance "cyber self-sufficiency"[285] and the EU's 2017 Cybersecurity Package has similarly emphasized security autonomy. However, as a relatively small country with a limited population and resources, it is not possible for Finland to contain the entire security lifecycle of products. This means that domestic industry will continue to specialize and that the market will be augmented by products emanating from outside of Finland. Many of the dominant players in ICT are currently American, and increasingly Chinese. The question for Finland then becomes, what aspects of the product lifestyle can be sourced from Finnish companies? From what is leftover, what needs to be secured from outside Finland and what portion of those products can already be secured from other EU states or developed cooperatively within the EU? Galileo is an example of intervention and pooling at the EU level in the pursuit of a capability individual member states were unlikely to secure alone. Nicknamed the European GPS, Galileo seeks to provide EU members with an alternative to the U.S.'s GPS as well as China's Beidou and Russia's GLONASS.[286] Following this question of broader EU alternatives, the question for Finland then becomes how to import technology and rely on non-domestic providers of technology in the most secure manner possible. The reliance on

https://ec.europa.eu/programmes/horizon2020/en/news/%0Dcommission-launches-call-proposals-€50-million-pilot-support-creation-networkcybersecurity.

284 As one Finnish government official put it in Author's Interview, 2018.

285 Jaroslaw Adamowski, "Ukraine Conflict Puts Cyber-Security High on Agenda in Eastern Europe," *SC Magazine UK*, June 1, 2017.

286 European Commission, "Galileo," 2018.

global supply chains coupled with the specialization required of small, agile economies remain two economic realities that bring with them deep security concerns for Finland.

To summarize, while Finland has been able to heavily leverage existing approaches to national defense, there remain several areas where existing institutions are maladapted to the realities of cyber-defense and the prior defense posture does not provide an existing conceptual or operational foundation adequate enough in its prior form. In the three ways discussed above, the prior defense societal posture serves, in part, as hinderance rather than an advantage.

3.5. Conclusion

What explains Finland's apparent meteoric rise as a leader in cyber-defense and cybersecurity at the national level? As a type of societal defense posture, the strategic and operational realties of cyber-defense represented a difference in kind and not in type. And as a consequence, Finland was able to build a cyber-defense posture rapidly because it was doing so largely out of existing concepts, strategic doctrine, architecture, and patterns of behavior rather than needing to stand those concepts and architectures up from scratch. Areas where existing architecture fell short (e.g. strategic oversight, funding, and law) took longer to emerge both in terms of their importance but also in their implementation.

FINLAND **Resilience-Based Societal Defense Architecture**		
Components of National Cyber-Defense	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**
Threats to national security not limited to kinetic, military operations	YES	YES
The homebase as a location for conflict	YES	YES
Citizens as security actors	YES	YES
The private sector as security actors	YES	YES
The breadth and character of the economy as a national security imperative	YES	RECOGNIZED and DEVELOPING
Strategic and operational oversight, coordination, and visibility across the defense-ecosystem	YES	RECOGNIZED and DEVELOPING

Notably, despite strong foundations, there is not perfect overlap between historical approaches to security and present approaches to cybersecurity, even in Finland. This is true for two reasons. First, while both are kinds of societal defense problems, the national security imperatives that arise out of being small and precariously placed are not identical to those that arise out of increasing critical interconnectedness. Both point to a homebase that is uniquely vulnerable and can be a location for active conflict. Yet, in cyberspace the scale and scope of that vulnerability differs from concerns over territorial integrity and maintaining independence; cyberspace underpins the daily functioning of society through a complex web of interconnections). Both defense problems require states to build out a defense architecture that does not rely on military or intelligence agencies as the sole or even primary defense actors while simultaneously integrating both public and private actors into a cohesive, real-time national defense posture. Yet, in

the domains of air, land, and sea, conflict was largely understood as discrete – on or off – and primarily located at or above the threshold of armed conflict. In cyberspace conflict is defined more by a form of constant contact – jostling in and through each other's networks – and can rise to the level of armed conflict, occur alongside kinetic attacks that rise to the level of armed conflict, or fall into the gray-zone.

Second, though the small, precariously placed states discussed in this dissertation all face a societal defense problem, the precise features of that defense problem and the particularities of the defense postures states adopt vary. Finland, in facing a large potential adversary to the East, built out a societal defense posture centered around a strategy of Comprehensive Security and a defense architecture centered on bolstering resilience (e.g. NESA) and numbers (i.e. conscription) in times of peace for use in times of conflict or crisis. This defense posture serves two functions: deterrence by denial (decreasing the likelihood that a conflict would be successful for their adversaries or worth the incurred costs over time) and defense during crisis (the ability to effectively fight and successfully end conflicts when they arise). In sum, while there is general overlap between the societal defense problem small, precariously placed states face and the defense problem all states now face in cyberspace, there is also specific overlap and points of departure unique to each state's particular variation on a societal defense architecture. That general overlap and specific variation will be further fleshed out in the subsequent chapter examining the societal defense architectures of Israel and Singapore.

4. Concluding Thoughts and Reflections

The strength of Finnish national cyber-defense is grounded in their historic systems-based approach both to conceptualizing comprehensive security and in operationalizing that vision by targeting government intervention at multiple levels ranging from the national to the municipal. Provision of cybersecurity is inherently challenging because it lies at a series of intersections: the intersection between public and private interests and capabilities, the intersection between economic and security activity, the intersection between internal and external security, the intersection between civil and military responsibility, and often the intersection between war and peace. These characteristics have placed significant strain on states like the U.S. that have sharply delineated responsibility for security to its public sector, and most often its military and intelligence services in conjunction with political elites. Finland, in contrast, has traditionally understood its security to be located within these intersections.

Yet, significantly, given structural differences between the defense imperatives born out of being small and precariously place versus critical interconnectedness in the cyber era, challenges to building out an effective cyber-defense posture still exist for Finland and the other Mice that Roar. Moreover, these challenges persist not just because historical approaches were maladapted to address them but because they represent deeply challenging security problems even if starting from scratch was no object.

Chapter 5
Looking Beyond Northern Europe: Israel and Singapore

1. Introduction

The prior chapter detailed how Finland, unlike the U.S., had a societal defense architecture that pre-existed the development of its cyber-defense posture. As a consequence, Finland was able to leverage critical conceptual and operational overlap between its existing national defense posture and the development of a cyber-defense posture to its advantage while the U.S. found itself without such a legacy to build out defense in-depth of the homeland given the pressing national security concern of increasing critical interconnectedness. But does this insight travel?

In this chapter I establish that this is not simply a story of the advantages of being Finland, but rather a story that speaks to the advantages a subset of relatively small and precariously placed states have over great powers like the U.S. and other states who do not share their history. The inclusion of Israel and Singapore in this project illustrate that this argument helps us not just to understand Finland's, or potentially other Nordic States facing a threat from Russia, success in this space but that the argument travels more broadly.

Why these two cases? The reasons are three-fold.

First, Israel and Singapore provide important geographic and geopolitical variation. Israel, situated in the Middle East, found itself with four bordering neighbors and several states within the region more broadly with which there are historical rivalries. Singapore, situated in Southwest Asia, found itself with two neighbors with which there are historical tensions and now the emergent concern of a rising China.

Second, both states meet the scope conditions of the argument. They have faced a societal defense problem born of size – namely limited population and a lack of strategic depth – and both have built out a kinetic defense architecture that does not rely on military or intelligence agencies as the sole or even primary defense actors while simultaneously integrating both public and private actors into a cohesive, real-time national defense posture.

To preempt a common critique related to Israel and size. It has been suggested to me that Israel does not qualify as small because it now has nuclear weapons and a highly technologically advanced military. This critique conflates strategy with size. Importantly, given real limitations due to the size of both its population and territory, Israel pursued specific strategies to compensate. Recall, "[s]trategy is about getting more out of a situation than the starting balance of power would suggest. It is the art of creating power".[287] Arguing that a state, which has been largely successful in the pursuit of a defense posture with the explicit purpose of mitigating severe limitations due to its size, should now no longer be considered small conflates size with strategy and unnecessarily obscures many of the core factors motivating that strategy.

Third, the addition of these two states provides useful variation on timing. Unlike Finland, Israel is widely considered to be one of the earliest (if not the earliest) movers in this space both in terms of

[287] Lawrence Freedman, *Strategy: A History*, Kindle Edition (Oxford University Press, 2013). p1808.

recognizing the national security concerns present – dependence on and the interconnectivity of cyberspace – and in beginning to develop a national cyber-defense posture. Importantly, for Israel this provides a longer window for evolution and learning, but also shows how even as a first mover Israel was able to leverage a degree of conceptual and operational overlap. Singapore, in contrast, is perceived to be a late mover. Yet, this timing is also consistent with their historical approach to national defense: learn best practices from other states, adapt them to meet Singaporean needs, and then implement at speed across society from the top down. That legacy strength – implementation – allows Singapore to rapidly jump to the top of several cyber-defense capability assessments and enter international awareness as one of the leading rather than middling or lagging states in this space.

Third, Israel and Singapore provide useful variation on the variable of their respective defense strategy. As discussed in PART I of this dissertation, it is the operational legacies rather than the strategic legacies that provide these small and precariously placed states with a shared advantage in the development and deployment of a cyber-defense posture. Yet, Finland, as discussed above, does have important strategic advantages as well – namely a focus on the security and resiliency of critical functions. This raises the question of whether a societal defense architecture provides an advantage in general or merely when coupled with a 'comprehensive security' like strategy. The answer? Both.

Any strategy centering the security and resiliency of domestic critical functions will require strong public private, civilian military cooperation and coordination given that in advanced industrial democracies most of those industries are largely privately owned and operated and lay outside the direct jurisdiction of military and intelligence agencies. Finland's focus on resilience as a national security strategy does provide important foundations for pursuing a similar strategy in cyber-defense. In contrast, the utility of other strategies, such as deterrence, for cyber-defense have been the focus of significant and ongoing policy and scholarly debate. Notably, both Israel and Singapore have leveraged deterrence strategies (though different flavors) coupled with raising costs quickly if conflict arose. A lack of strategic depth made resilience to kinetic conflict occurring within the homebase over longer durations of time largely untenable. Rather than weigh into the strategic dynamics of cyber conflict more broadly, which is worthy of its own dissertation and has been the subject of many, with the addition of these two cases this dissertation illustrates how, irrespective of strategy, a subset of small states had an operational advantage over the U.S. given their prior defense posture.

2. Israel: An innovation-Based Societal Defense Architecture

"We took our existing innovation ecosystem and nudged it into cybersecurity. We went from start-up nation to cybersecurity nation."
- Senior Israeli Government Official[288]

Israel is widely considered one of the first movers in this space both in terms of making the transition from thinking about cyberspace not just as a domain for intelligence gathering activities or actively jamming the systems of enemy weapons platforms during periods of conflict, but in terms of the offensive opportunities afforded to states (frequently referred to as cyber weapons) more broadly. By the late 1990s, Israel had already recognized that its dependence on cyberspace in the civilian space (civilian critical infrastructure in particular) directly endangered their national security and that this new axis of possible attack needed to be robustly addressed. Why was Israel so quick

[288] Author's Interview, 2018.

out of the gate in this regard? What factors shaped how their cyber-defense posture evolved given that realization?

An important part of answer lays in the defense posture Israel adopted to address the pressing societal defense problem it faced as a small, precariously placed country: primarily civilians as security actors, innovation as a national security imperative, and agility born from tactical realities directly shaping national strategy.

As an important point of context, analysis of defense postures and national security strategies are uniquely challenging in the case of Israel. As previously mentioned in Chapter Three, unlike Finland that publishes formal public and internal facing strategic documents with regularity, "Israel has not published a formal, public national security document" in decades.[289] In fact, national leadership avoids publishing declarative documents. When I asked why, a senior IDF officer provided two reasons: first, you don't want to lock yourself in when agility is essential for responding to a rapidly evolving threat landscape and second, given that the threat space is rapidly evolving these documents would simply become outdated too quickly to make the effort worthwhile.[290] Another interviewee, somewhat jokingly hinted at a potential third reason: formal strategy would require getting Israelis to agree on a strategy and its operationalization so that it could be codified in the first place.[291]

This final observation, though made partially in jest, hits on an important trend in Israeli national security politics. Strategy, beyond a broad set of agreed upon strategic principles found in *Tfisat Habitachon* (the National Security Concept) [292] is not a predominantly top-down process. Instead, specific defense strategies in Israel emerge from lower level activity – from tactical and operational concerns – and then permeate up. This does not mean that Israel does not have an observable defense posture or that organizations and individuals do not mobilize around a set of core goals. Rather, there is not orderly movement toward the achievement of specifically framed and formatted strategies at the national level. In Israel, strategy is a more reactionary rather than prescriptive process. "Organizations and individuals respond to challenges without a centralized and clear decision-making process",[293] a dynamic driven largely by a persistent history of active conflict over a contested territory.

This section will proceed in three parts. First, I provide background on Israel's national defense posture. This includes background on their geostrategic position, defense strategy, and defense architectures (how the strategy was operationalized). Second, I illustrate how this foundation was directly leveraged into Israel's cyber-defense posture and that it conceptually and operationally overlaps with the structural realties of cyber-defense. Third, I review several persisting challenges as Israel continues to build out a cyber-defense posture that addresses increasing critical interconnectedness.

2.1. Historical Background: Size as a Kind of Societal Defense Problem

289 Lior Tabansky and Isaac Ben-Israel, *Cybersecurity in Israel (SpringerBriefs in Cybersecurity)*, Kindle Edition (Springer, 2015). loc. 397.
290 Author's Interview, 2018.
291 Author's Interview, 2018.
292 What Lior Tabansky and Isaac Ben-Israel refer to as grand strategy given that it ties economic policy and security policy together for the joint prosperity and security of the state. Tabansky and Ben-Israel, *Cybersecurity in Israel (SpringerBriefs in Cybersecurity)*.
293 Tabansky and Ben-Israel. loc. 401.

For Israel, which gained its independence in 1948, the early years of independence were fragile and characterized by active conflict. This period featured a series of Israel-Arab wars (military conflicts between Israeli and various Arab forces) that extended beyond the mid-1900s:[294]

- Israel's War of Independence (1947-1949)
    - Egypt, Iraq, Jordan, Iraq, Lebanon, Saudi Arabia, and Syria
- The Sinai Campaign/Operation Kadesh (1956)
    - Egypt
- The Six-Day War (1967)
    - Egypt, Jordan, and Syria
- The War of Attrition (1968-1970)
    - Egypt
- The Yom Kippur War (1973)
    - Egypt and Syria
- The Lebanon War/Operation Peace for Galilee (1982)
    - Lebanon
- The Gulf War (1991)
    - Iraq
- The Second Lebanon War (2006)
    - conflict escalated beyond Israel's borders with the involvement of Lebanon's Hezbollah Shiite militants

Importantly, while Finland's primary concern was territorial integrity and independence, Israel coupled those concerns with a perception that this would be accompanied by a real threat to the survival of its people. Given those stakes, one academic expert argued that "Israel cannot afford a single loss in a war" because such a loss could be catastrophic.[295] Israel would not be absorbed into its neighboring state(s); they could simply cease to exist. This sentiment was mirrored by an IDF official when he contrasted the security environment in Israel to some the other Mice that Roar by stating that Israel was not just fighting for its independence but its survival.[296]

Keeping this geostrategic context in mind, as a relatively small country with a history of conflict with all its neighbors and tensions with states in the region more broadly, Israel's defense posture has developed out of the following concern: how can a small country in a contested territory, which lacks both strategic depth and a large population, prevent the outbreak of and successful bring about cessation to conflict?

Israel's answer was three-fold. First, it needed to address its numerical inferiority by leveraging its entire citizenry as security actors and then overcome the remaining disparity through qualitative superiority in terms of training and equipment. Second, it needed to address its lack of strategic depth by containing fighting outside of the homebase as much as possible and bringing hostilities rapidly to a close (this was also an imperative given numerical inferiority). Ideally, however, given its

[294] For an overview of conflicts between Israel and its neighboring states refer to the Israeli Ministry of Foreign Affairs, "Israel's Wars," accessed July 24, 2020, https://mfa.gov.il/MFA/AboutIsrael/History/Pages/Israel-Wars.aspx. and Ray Sanchez, "Israel and Its Neighbors: Decades of War," *CNN*, August 13, 2014.
[295] Author's Interview, 2018.
[296] Author's Interview, 2018.

size and the potentially catastrophic consequences of conflict, it would be best not to need to fight a war in the first place. This led to a focus on nuclear deterrence and decreasing the likelihood of subsequent hostilities through decisive victories and imposing high costs in prior engagements.

There are three important insights encapsulated in this approach. First, as a small country in a precarious environment, national defense is a task that requires the mobilization of vast resources. This means that the responsibility for security cannot only be housed within a professional military alone but also with the citizenry as a whole being prepared for war even during times of peace in order to ensure national survival in times of crisis. Recall, this is an insight Finland and Israel share.

Second, the breadth and character of the economy is seen as a national security imperative. In order to overcome numerical inferiority, Israel leverages an innovation ecosystem geared around providing quality superiority (primarily through science and technology) for its defense forces. As a result, rather than thinking of the character and development of the economy as largely separate from the national defense sphere, a vibrant economy is seen an essential condition for national security. National defense and the economy are not separable.

Third, like Finland, the homebase is understood as a potential area for conflict. For Israel, the territory itself is actively contested. Conflict and warfare is not something that primarily happens somewhere else; it can happen at home. But unlike Finland, which has more strategic depth, Israel's focus is on preventing warfighting within the territory through advanced warning and pushing warfighting out of the homebase by projecting power rapidly into enemy territory.

Tfisat Habitachon is more than just political rhetoric in Israel. It is supported by a robust societal defense architecture that seeks increases the preponderance of resources in the form of soldiers and builds out a robust qualitative edge over potential rivals. This strategy has been operationalized through two key components: conscription and an innovation ecosystem.

The first key component an effort to bolster the preponderance of security actors during a time of crisis by leveraging the citizenry as a whole. In addition to a standing military, Israel has mandatory military service for citizens over the age of 18.[297] Compulsory service typically lasts two years and eight months for men and two years for women. After completing compulsory service, Israelis remain within the security apparatus, completing up a month of service a year, into their 50s.[298] This approach serves two purposes: "[t]he system of reserves frees up the vast majority of its soldiers to take an active part in society and the economy. At the same time, the army is able to mobilize hundreds of thousands of reserves within hours and the full strength of the army within 48 hours."[299] In other words, like in Finland, conscription (including a period of active military and reserve service) is a cost-effective way of maintaining "consistent and efficient preparedness for defense at any time" in a cost-effective manner.[300]

[297] There are some exemptions made or mitigating factors that might limit the duration of service. To learn more about the particularities of military service within Israel, refer to "Israel: Military Draft Law and Enforcement," Library of Congress - LAW, accessed July 26, 2020, https://www.loc.gov/law/help/military-draft/israel.php.
[298] Israeli Defense Forces (IDF) - Mahal, "IDF Background Information," accessed July 26, 2020, https://www.mahal-idf-volunteers.org/information/background/content.htm#reserve.
[299] Israeli Defense Forces (IDF) - Mahal.
[300] Tabansky and Ben-Israel, *Cybersecurity in Israel (SpringerBriefs in Cybersecurity)*. loc. 544.

The second key component is the national innovation ecosystem primarily in the areas of science and technology). Israel's economic policies, like Finland, have always had an element of active market intervention. As a country with limited human capital and scarce natural resources,[301] Israel found success in focusing its efforts on and building out an expert-led, knowledge-based economy heavily centered around science and technology. This innovation systems-based approach actively leveraged contributions from and feedback effects between industry, educational institutions, and government.[302] This includes the creation of a publicly funded, compressive education system; scientific infrastructure, R&D, government procurement (e.g. weapons systems), and a vibrant start-up culture.[303]

Second, similar to Finland, there is a history of 'government as consumer' and 'government as funder' activity. Take for example, weapons procurement by the Ministry of Defense but also active R&D funding organized and awarded by the Office of the Chief Scientist (OCS).[304]

Third, and in contrast with Finland, Israel's innovation ecosystem benefits from a series of feedback effects between industry and the defense forces. This feedback is a direct consequence of professional service, conscription, and reserve duty, which creates a revolving door between service and industry and civil society) coupled with a threat environment characterized by more recent and frequent conflicts. This feedback loop has two outcomes of particular note. First, innovation from within the MoD is spun out into innovation in the private sector. Take for example, electric car development and deployment within Israel, which sought to leverage a smart grid of charging stations and battery exchanges. A lingering problem was how to build a mechanism where you could safely and quickly swap out a battery without leaving it in a precarious position while driving. The solution was pulled directly from the military; "[t]hey employed the same hooks used to hold five-hundred-pound bombs in place on air force bombers. There's no room for error in a bomb-release mechanism; the battery would be just as secure, yet removable, in electric cars."[305] Second, training received and relationships built while serving is deployed in the private sector. Take for example the two founders of Fraud Sciences that occupy the opening pages of the first chapter of Dan Senor and Saul Singer's *Startup Nation*.[306] They served together in Israel's elite army Intelligence unit, 8200. Third, also identified in Dan Senor and Saul Singer's seminal dissertation, individuals were able to leave the service and pursue solutions to the types of problems they faced while serving. The revolving door, in and out of service through the reserves, allowed for vibrant interaction between the innovation ecosystem and the national security space. Innovation is not a goal in and of itself. It would be no use to the defense goals of the states if there was not mechanisms to transmit innovative solutions into the defense space. In addition to the more formal mechanism explored above, Israel's service model, which leverages citizens as security actors, allowed for a robust informal pathway of transmission.

301 For examples of scholarship on resources scarcity in Israel, refer to David H. K. Amiran, "Geographical Aspects of National Planning in Israel: The Management of Limited Resources," *Transactions of the Institute of British Geographers* 3, no. 1 (1978): 115; Eran Friedler, "Water Reuse - An Integral Part of Water Resources Management: Israel as a Case Study," *Water Policy* 3, no. 1 (January 1, 2001): 29–39; and Ira Sharkansky, *The Political Economy of Israe*, First Edition (Routledge, 2017).
302 For a detailed analysis of comparative innovation politics refer to Dan Breznitz, *Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland* (Yale University Press, 2007).
303 Refer to Manuel Trajtenberg, "R&D Policy in Israel," in *Economics of Science, Technology and Innovation Book Series (ESTI, Volume 23)*, ed. M. P. Feldman et al. (Springer, Boston, MA, 2001), 409–54; Jerome S. Engel and Itxaso del-Palacio, "Global Clusters of Innovation: The Case of Israel and Silicon Valley," *California Management Review* 53, no. 2 (2011): 27–49; and Dan Senor and Saul Singer, *Start-up Nation: The Story of Israel's Economic Miracle*, Kindle Edition (Twelve, 2011).
304 Gil Press, "How Startup Nation's Innovation Catalyst Masters The Art Of Public-Private Partnership," *Forbes*, July 20, 2015.
305 Senor and Singer, *Start-up Nation: The Story of Israel's Economic Miracle*. loc. 268.
306 Senor and Singer.

Fourth, an important feature of Israel's innovation ecosystem is the prevalence of startups. This allows for a creative churn that isn't possible in larger, multinational companies. The result is an agile creation and destruction process. Impressively, Israel, a young country with a small population and no natural resources, produces more start-up companies than large, peaceful, and stable nations like Japan, China, India, Korea, Canada, and the U.K.[307]

Notably, this defense posture is also mirrored in counter-terrorism operations within Israel. Lior Tabansky and Issac Ben-Israel note in their book, *Cybersecurity in Israel*, that "Israel commissioned its qualitative edge to counter the [intifada] threat. By using high technology to produce real-time intelligence, IDF and Shabaq gradually gained the capability to carry out rapid targeted preventive operations."[308] Like in conflict with its neighboring states, these types of rapid offensive operations are made possible by close territorial proximity. Moreover, this focus on technology enabled preemption was coupled with a direct effort to push the locust of hostility outside of the homebase, this time in the form of physical barriers. Three such barriers were built out over the past 15 years to address concerns over terrorism, migration, and political destabilization emanating from neighboring territories: a separation barrier between Israel and the Palestinian-controlled West Bank, a border fence on the Egyptian–Israeli border, and a fence along Israel's border with Syria.[309] Checkpoints provide an additional mechanism through which to limit access to the territory and Israeli population. Finally, counter-terrorism efforts within Israel feature a similar 'deter future action through raising costs' logic, demolishing the homes of their family members as one example.[310] [311]

In conclusion, Israel has historically faced a societal defense problem stemming from geopolitical concerns and its relative size. Though it varies from Finland in many regards, it too has developed a societal defense architecture to support its strategic goals. Two components – conscription and an innovation ecosystem – form the bedrock of this societal defense architecture in Israel. Both, notably, are efforts to operationalize a strategy (*Tfisat Habitachon)* that seeks to provide national security given the constraints of size. In short, Israel's defense posture sought to address a societal defense problem stemming from a small population with little strategic depth by leveraging resources across the society in defense of the state.

2.2. Developing a Cyber-Defense Posture: Areas of Overlap and Departure

Why was Israel, unlike Finland, a first-mover in this space? To what degree were they able to leverage their existing defense-posture, namely their societal defense architecture, in the development of a cyber-defense posture? I argue, as presented in the introduction to this section, that an important part of answer lays in the defense posture Israel adopted to address the pressing societal defense problem it faced as a small, precariously placed country: namely civilians as security actors, innovation as a national security imperative, and agility born from tactics feeding up into strategy.

307 Senor and Singer.
308 Senor and Singer. loc. 596
309 Amos Harel, "Israel's Walls," *Foreign Affairs*, February 17, 2017.
310 Jonathan Lis and Yaniv Kubovich, "Defense Ministry: Israel Has Destroyed 45 Homes of Terrorists' Families in Last 3 Years," *Haaretz*, January 11, 2018.
311 For a more detailed accounting of Israeli counter-terrorism activity refer to Avi Dicter and Daniel L Byman, "Israel's Lessons for Fighting Terrorists and Their Implications for the United States," Brookings' Analysis Paper, March 2006.

Major Gen. (Res.) Isaac Ben-Israel, now a professor at Tel Aviv University, illustrated the latter two factors when he told me the story of when he first realized that Israel needed a defense posture that explicitly prioritized critical infrastructure protection. At the time, the early 1990s, he was a one-star general tasked with research and development in the Israeli Defense Forces (IDF). While this quote is longer than what would usually be included in a dissertation of this type, I have included it in its entirety here because of how well it illustrates a chain of events where a focus on technological innovation to address a tactical concern (how to disable Syrian air defense) led to the realization that Israel needed to address a new vulnerability it had opened itself up to through its dependence on, then a nascent, cyberspace. This realization subsequently led Ben-Israel, who had been promoted and was now in charge of R&D for the Ministry of Defense, to write a letter[312] to the Prime Minister and the Defense Minister (equivalent to U.S. Secretary of Defense) at the tail end of the 1990s, urging them to address this issue now before other states - namely countries hostile to Israel - realized that this was a critical vulnerability[313] and exploited it.

Ben-Israel, in his own words:

> And at that time - this was the beginning of the 90s, - [one of] our main enemies was […] Syria. And when we thought about how to fight Syria the main obstacle for us was the Syrian air defense missiles. […] So, I thought, the Syrian air defense is operated by computers. There are computers everywhere: at the level of the battery, at the level of the brigade, at the level of the Syrian air defense. Let's try to hack into these computers and use that as a weapon to prevent them from using those weapons against our aircraft. It didn't work.
>
> It didn't work because today when you say computer, you know what you refer to: standards, one or two operating systems, few not more than five different computer programming languages. At that time, every computer was different from the other. And we found ourselves – and of course those missiles that I mentioned were made by Soviet industry and everyone built a different computer - and I found myself with the huge problem of trying to get the intelligence needed in order to plan hacking into one of these computers.
>
> But, nevertheless, I founded this new unit in 93 [a new unit in the IDF focused on offensive cyber-operations] and after a few, say four or five years, of trying to develop cyber weapons, we came to the conclusion that in the case of war it may be difficult to hack into the computers of Syrian air defense or Syrian combat aircraft. But we can much more easily hack into the computers of Syrian power production, for example.
>
> Civilian critical infrastructure. Okay, there will be a war, and if we can shut off the electricity in Syria that is also good. It is much easier to do because the civilian industry usually bought their computers from IBM or HP – western vendors – and secondly, they [civilian critical infrastructure] had no awareness at all to issues like the need for protection.
>
> So, we looked at the map of the Middle East. And asked ourselves, what country in the Middle East is really vulnerable to this new type of attack, this new type of weapon. You

312 This letter was latter published, in a sanitized publicly available form, in 2000 in Hebrew. More than ten years later at Tel Aviv University, he re-wrote that sanitized version with Lior Tabansky, which was published in English

313 At the time, Ben Israel stated that you could hardly find any manual control of anything in Israel, they monitor computers who do the work of monitoring everything else in critical infrastructure. This was already a state that was comparatively highly depending on cyberspace for its daily and combat functioning. Author's Interview, 2018.

> cannot take a cyber weapon and attack a piece of desert in Sudan. You need computers there. But, unfortunately, most of the countries around us in the beginning of the 90s were not developed enough to use computers to control their power production or other critical infrastructure. There was only one country in the Middle East that was developed enough and, therefore, vulnerable enough. And this was Israel. Only us.[314]

Ben Israel's letter sparked a wider conversation within the government and defense establishment and after some subsequent work done by the National Defense Council, it was decided that Israel needed a national level cyber unit, which would be in charge of cyber-protection of critical infrastructure. That unit, the National Information Security Authority (RE'EM or NISA), was set up in 2002. Because this was considered to be a problem of national security but contained within the homebase, this unit was built out under the auspices of the internal security service, namely the Israel Security Agency (acronym Shabak but also known as the Shin Bet - a two-letter Hebrew abbreviation of "Security Service"). This organization was limited in scope: its remit to instruct and protect vital computerized systems of selected public and private civil organizations (several exceptions were made at the time, such as for finance because there was concern that Israeli security apparatus involvement in that sector would undermine the international attractiveness of companies).[315]

Israel's geostrategic environment (which unlike Finland's featured more recent and frequent conflict) coupled with core features of its historical defense posture - in this instance moving conflict out of their territory into enemy territory, innovation as a national security imperative, and dynamics at the tactical level feeding up and directly informing national security policy – cumulated in an early recognition of the realities of critical interconnectedness and kickstarted efforts to build out an Israeli cyber-defense posture.

Yet, it was not until ten years later, with the establishment of the Israel National Cyber Bureau (INCB) in 2012, which reported directly to the Prime Minister, that Israel had the institutional foundations necessary to develop national cybersecurity strategy more broadly.[316] The INCB emerged as the direct result of a national Task Force (the National Cyber Initiative in Hebrew), which was set up by the Prime Minister to address national security concerns in cyberspace beyond the narrower remit of protecting vital computerized systems. With this objective in mind, the Task Force recommended the establishment of the INCB with a dual mandate: (i) to devise a national cybersecurity policy and strategy and (ii) to strengthen domestic capability and advance Israeli leadership within the emerging cybersecurity market. To achieve the latter, Israel honed in on building out and maintaining an innovation ecosystem to support national security efforts in cyberspace going forward. As a consequence, the remit of the INCB included a broader focus: not just on security computer systems in select civilian and government infrastructure (RE'EM) but on replicating the successes of the existing innovation ecosystem for cybersecurity and cyber-defense purposes. In other words, pursuing a systems-based approach that directly linked economic growth/prosperity and national security.

Importantly, in operationalizing this new mandate – not just defense as a task of the security and intelligence apparatus but as supported by a robust and agile domestic economy focused on

[314] Author's Interview, 2018.
[315] Author's Interview, 2018.
[316] National Cyber Directorate, "Israel National Cyber Security Strategy in Brief," *State of Israel's Prime Minister's Office*, September 2017.

innovation – Israel was able to leverage a central element of its societal defense architecture directly into its approach to cyber-defense and cybersecurity more broadly. While there is a foundation of citizens as security actors similar to Finland's, it is the innovation ecosystem that provided the greatest utility. So much so, in fact, that one senior government official with intimate knowledge of the development of a cyber-defense posture remarked, "we took our existing innovation ecosystem and nudged it into cybersecurity. We went from start-up nation to cybersecurity nation."[317] In fact, this nudge was deemed so successful, that a second Task Force was recently set up to duplicate its success, but this time with a focus on the security implications of Artificial Intelligence (AI).[318]

Within the innovation ecosystem effort[319] there are three strengths of particular note. First, Israel succeeded in developing a vibrant technical and process-based expertise within the private sector. Israel, as of 2018, boasted a $92 billion cybersecurity market.[320] Stunningly, "[i]n 2018, Israeli startups received $1.19 billion or almost 20% of global VC investments in cybersecurity, up 47% from the previous year" and "surpassed China last year as the hottest spot for VC investments in cybersecurity companies outside of the U.S.[321] In a 2018 ranking of the 500 most innovative cybersecurity firms compiled by Cybersecurity Ventures, Israel was ranked second only to the U.S. with 42 out of 500 firms. [322] By any measure, has developed and maintained a robust cybersecurity market. The core assumption behind this effort is that Israel cannot know what exact solutions it will need in the near or distant future (no state can). But by maintaining a vibrant innovation ecosystem, serving as the catalyst for innovation, it can increase the likelihood that when the need arises, solutions (or the foundations for solutions) will be available for them to leverage. As one academic and former government official noted, what you want is a lot of half-baked ideas floating around that you can pluck out of the mix and rapidly develop as the need arises.[323]

Second, this approach allowed for an amplification of existing lines of effort by leveraging in tandem private and public actors from industry, civil society, and government. For example, Israel introduced cybersecurity into the core curriculum for all high school students. It built out research centers within Universities that cut across traditional disciplinary siloes to address questions that span technical network defense to deterrence as a national security strategy. On such example is Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center, which includes approximately 250 researchers many of whom join the Center after active roles within government.[324] Israel also doubled down on government investment as an important part of this ecosystem, but like in prior iterations not the sole or even the largest source of finances in the market. The Office of the Chief Scientist (OCS) has been in the business of public-private partnership since its creation in 1965. One particular success of this partnership is the development and maintenance of an ecosystem, "that gives back at least 5 dollars for every dollar you put in".[325]

317 Author's Interview, 2018.
318 CyberWeek Conference Remarks. Israel. 2019 and mirrored in the National Law Review article: Michael T. Renaud, Marguerite McConihe, and Derek E. Constantine, "Will Israel Become a Leader in AI Protections?," *The National Law Review*, June 10, 2019.
319 For a more detailed examination of the innovation ecosystem and the cybersecurity innovation ecosystem refer to Lior Tabansky and Isaac Ben-Israel, "The National Innovation Ecosystem of Israel," in *The National Innovation Ecosystem of Israel. In: Cybersecurity in Israel. SpringerBriefs in Cybersecurity* (Springer, Cham, 2015), 15–30; David Yin, "Secrets To Israel's Innovative Edge," *Forbes*, June 5, 2016; and David Yin, "What Makes Israel's Innovation Ecosystem So Successful," *Forbes*, January 9, 2017.
320 Gil Press, "Israeli Startups Shine In The $92 Billion Cybersecurity Market," *Forbes*, February 26, 2019.
321 Press.
322 The full ranking can be found at "500 Most Innovative Cybersecurity Firms in 2018."
323 Author's Interview, 2018.
324 Figure provided by Issac Ben-Israel as an estimate of the center's size.
325 Press, "How Startup Nation's Innovation Catalyst Masters The Art Of Public-Private Partnership."

Third, and finally, this effort benefits from Israel's service requirements by pulling talent into the security and intelligence apparatus and then back out into industry. Take, for example, 8200: Israel's previously secret intelligence and cybersecurity unit comprised primary of 18-21-year-olds carrying out mandatory military service. Those serving in 8200 simultaneously bolster capabilities of the Ministry of the Defense while also sparking subsequent innovation within the broader domestic market. As Avishai Abrahami, formerly assigned to 8200 and a cofounder of Wix, explains, "[j]ust from my generation, there are more than 100 guys from the unit that I personally knew who built startups and sold them for a lot of money […] There was a team of ten people in one room in the unit. I call it the magic room, because all of them created companies where the average market cap is a half-billion dollars."[326] Another example is the Talpiot Program: "If Unit 8200 takes the top 1% of the best candidates, Talpiot takes the top 1% of that 1%. This program is the most advanced and intense technical training in the IDF."[327]

But the evolution of Israel's cyber-defense posture does not end in 2012. Notably, in 2015, a further opening of the aperture of the national cyber-defense apparatus occurred. Per the recommendation of the national Task Force and as a consequence of the strategic and operational development and planning that occurred within the INCB, it became apparent that Israel needed to address the security and resilience of its government, economy, and society more broadly and not just the narrower remit of protecting the computerized systems of a subset of vital civilian and government infrastructure (the task of RE'EM). The National Cyber Security Authority (NCSA) was formed to fill that gap. The NSCA was charged with the defense of cyberspace. Its remit was three-fold: (i) the overseeing the operational cybersecurity efforts at the national level (allowing for a cohesive response to cyber-attacks); (ii) operating the national CERT (CERT-IL); and (iii) systematically addressing resilience of the Israeli economy through regulation, organization, preparedness, and incentivization (as one Israeli advised a series of European policymakers in a meeting in Brussels, "if you want to bolster security and resilience of your economy, you have to finance it).[328] As a point of comparison, when it came to conceptualizing risk as systemic (not just a matter of computer security for a subset of selected civilian and government infrastructure), it took Israel 13 years after taking the first steps to secure critical infrastructures from cyber-attacks (RE'EM) to create an institution focused on and responsible for bolstering society-wide security and resilience. In contrast, it took Finland about a year to build out such a structure for cyber-defense (NESA), largely because it was able to leverage an existing conceptual foundation of resilience as a national security imperative and architecture operationalizing a response to that very concern.

Furthermore, it was not until 2017, that Israel addressed one important and until that point persistent silo. Three organizations each tasked with a different piece of the cyber-defense posture: the RE'EM, the INCB, and the NCSA. Up to this point, the innovation ecosystem work was housed largely under the auspices of the INCB. The critical infrastructure protection work, in contrast, was housed under the auspices of the RE'EM and the INCB. The broader operational framework for cyber-defense focused on the security and resilience of economy and civil society was undertaken by the INCB. All three were relatively new organizations set up to address the unique national security challenges posed by cyberspace and critical interconnectedness. With the establishment of the Israel National Cyber Directorate (Ma'arach or INCD), which combined the RE'EM, INCB, and NCSA under the auspices of a single institution, Israel for the first time in its history, had a single institution

[326] Richard Behar, "Inside Israel's Secret Startup Machine," *Forbes*, May 11, 2016.
[327] Darknet Diaries, "Unit 8200," Podcast Episode Transcript, December 15, 2018, https://darknetdiaries.com/transcript/28/.
[328] Meeting in Brussels on security and resilience. 2018.

with oversight over both the defense and resilience of the critical functions of society but also the innovation ecosystem (the systems-based approach for developing and deploying high quality capacity across the defense and intelligence agencies but also civil society more broadly). As two interviewees intimately familiar with the trajectory of this policy development lamented, it had taken Israel almost ten years of concentrated institutional effort at the national level (from the creation of the Task Force to the establishment of the INCD) what Singapore did in two (the establishment of the Cyber Security Agency).[329]

2.3. Persisting Challenges

The Israeli cyber-defense story is one both of an extension of an existing societal defense approach and the persisting limitations of and challenges to that approach for addressing critical interconnectedness in the cyber era. The foundations, areas where overlap allowed Israel to leverage an existing national defense approach into the development of a cyber-defense posture, have previously been discussed. The challenges are three-fold.

One central challenge stem from the largely tactics/operations heavy approach[330] to strategy development in particular and national security more broadly – in Israel, the tail (or in this case perhaps tails would be more accurate) wags the dog. Take for example the development of critical infrastructure protection in Israel. The Information Security Authority (RE'EM) emerged out of tactical necessity: the need to disable Syrian air defense in the event of conflict so that Israeli aircraft could rapidly shift the locus of conflict/actively contested space within Syria.

Unlike Finland, which regularly publishes strategic documents and has a tradition of abiding by them in practice,[331] the Israeli defense posture is broadly defined at the national level through *Tfisat Habitachon* but then built out in depth through actions emanating from tactical necessity and operational circumstances. While this approach has the added benefit of agility and innovation in a changing threat environment, it is also limiting because it makes cohesive, uniform action across government, industry, and the civil society challenging. As one Israeli joked, if there are ten Israelis in a room you will have far more than ten opinions and they will all be certain they are right.[332]

This decentralized approach was mirrored in the interview experience more broadly. Namely, most spoke to their very specific piece of the system and why cyber-defense had evolved the way it did in that particular area (in sharp contrast with Singapore where the focus was on the national narrative and it was harder to tease out the sub-strata evolutions). There was also active disagreement when interview subjects were asked about national-defense below the level of *Tfisat Habitachon* and beyond the observable institutions and regulations (e.g. the IDF, Shin Bet, or the RE'EM). For example, when I inquired into the absence of resilience within the broader defense posture of Israel historically (recall this was one of Finland's strengths at it developed its cyber-defense posture), I was given widely divergent answers: no, it had never been a core pillar (unless you consider

329 Author's Interviews, 2018.
330 For an example of how tactical decisions can drive strategy within the U.S. refer to Melissa K. Griffith, "Is the Strategic Corporal on Your Twitter Feed?," *Net Politics and Digital and Cyberspace Policy Program from the Council on Foreign Relations*, July 12, 2017.
331 When speaking about EU regulations – specifically GDPR coming into force – a senior government official lamented that if something is written down, Finns will rigorously follow it: "we are very German in that regard". Whereas another EU country would not be as stringent and therefore not incur the same logistical costs or economic constraints. This same trend come in when speaking to technical cybersecurity experts working within government. Two interviewees emphasized the importance of not being too specific in national security strategies and documents because this would restrict action within industry and civil society to exactly what was written down even if circumstances change.
332 Author's Interview, 2018.

phycological resilience when living under constant threat the central crux of the concept); no, a form of it had been debated at some point during the Intifadas within the Ministry of Defense but was never formally adopted or implemented; sort of, although it had never been formally adopted it was understood to be important by some in practice; and yes, it must have been at some point but they were uncertain about when or where it would have been incorporated prior to the cyber-defense efforts in this area.[333]

Notably, despite being one of the earliest movers in this space, it was not until 2012 with the establishment of the Israel National Cyber Bureau (INCB) that Israel had the capacity to develop a cybersecurity policy and strategy at the national level. And it wasn't until 2017 with the creation of the Israel National Cyber Directorate (INCD) that Israel had a cyber-defense posture that prioritized security and resilience of critical infrastructure, reducing risk within the broader population, and leveraging the innovation ecosystem as a critical component of national defense cohesively and in-depth. In other words, despite being a first mover in this space, it took over ten years of concerted national level effort before Israel was able to develop a dedicated government agency overseeing Israel's cyber-defense posture within the economy and civil society more broadly.[334]

A second persisting challenge rests soundly within the innovation ecosystem architecture and points to the limitations of translating this historical model into one that can adequately address the structural realities of cyber-defense.

These limitations are two-fold. First, the innovation ecosystem allowed for industry and civil society to formally and informally support the military and intelligence apparatus in defense of the state. In turn, it reciprocally supported innovation and economic growth within the private sector. In cyber-defense, however, industry spinning innovative solutions into government in support of national security needs and government spinning talent and products back out into industry is only one part of the equation. The other part is both industry and government spinning out security solutions into industry and civil society more broadly. This requires government not just to nudge the existing ecosystem but to create and foster pathways for security solutions to flow out into industry and civil society and as well as into the national security apparatus housed within the government. While creating organizational oversight through institution formation is one important part of the solution, this does not address the informal and more agile mechanisms of knowledge transfer (the revolving door for example) leaving one of the most vibrant and agile mechanisms largely under-developed.

Third, domestic capacity takes on greater significance given rising concerns over supply chain security. Like Finland, Israel incorporates many products from abroad into the development of products at home, including infrastructure. Several interviewees raised American dominance and concerns arising over Snowden.[335] Interestingly, however, only one interviewee raised concerns about China and the prevalence of Chinese technology within critical infrastructure.[336] They remained deeply concerned that this issue (as it related to China but also more broadly) had not been taken seriously enough within Israel both in terms of recognizing the scope and scale of the problem and subsequent security concerns it raises but also in terms of operationalizing a strategy to robustly and not just performatively address those concerns.

[333] Author's Interviews, 2018.
[334] National Cyber Directorate, "Israel National Cyber Security Strategy in Brief." p 6.
[335] Author's Interview, 2018.
[336] Author's Interview, 2018.

2.4. Conclusion

In conclusion, even in a state whose defense strategy leverages deterrence and rapid escalation outside of the homebase, we can see important conceptual and operational overlap between the realities of cyber-defense and the realities of national defense as a small, precariously placed state. Like Finland, Israel has faced a societal defense problem stemming from its size and precarious geopolitical position. As a consequence, it has built out a defense posture that is operationalized through a societal defense architecture: where the responsibility for and development of defense capacity are jointly held by private and public actors, industry and government, defense forces and citizens. Unlike Finland, Israel pursued an innovation-based societal defense architecture in an effort to overcome its small population size, lack of natural resources, and limited strategic depth. Also, unlike Finland, Israel's geopolitical position featured more recent and frequent conflict. While there are clear disadvantages to living in a contested territory, "[s]ecurity is a subject that can be taught theoretically, but nothing is a substitute for a real hands-on experience and we've got lots of it."[337] In short, Israel's geostrategic environment coupled with core features of its historical defense posture – i.e. moving conflict out of their territory into enemy territory, citizens as security actors, innovation as a national security imperative, and dynamics at the tactical level feeding up and directly informing national security policy – resulted in an early recognition of the realities of critical interconnectedness and kickstarted efforts to build out an Israeli cyber-defense posture. Yet, in areas where Israel did not have historical legacies to directly leverage (i.e. resilience and comprehensive action and strategy at the national level), the cyber-defense posture required sustained political effort over years.

ISRAEL **Innovation-Based Societal Defense Architecture**		
Components of National Cyber-Defense	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**
Threats to national security not limited to kinetic, military operations	NO	YES
The homebase as a location for conflict	YES	YES
Citizens as security actors	YES	YES
The private sector as security actors	NO	YES
The breadth and character of the economy as a national security imperative	YES, ROBUST (Innovation Ecosystem)	YES
Strategic and operational oversight, coordination, and visibility across the defense-ecosystem	YES	ECOGNIZED and IMPLEMENTING

[337] Peter Sucio, "Why Israel Dominates in Cyber Security," *Fortune*, September 1, 2015.

3. Singapore: An Implementation-Based Societal Defense Architecture

"If Israel is herding cats, Singapore is herding sheep."
– A Singaporean cybersecurity expert[338]

In contrast to Israel, Singapore's societal defense posture leverages a long-standing learning model focused on identifying, adapting, and implementing best practices in a cohesive, top-top manner across all aspects of the society. Therefore, while in Israel you observe extensions of the model happening more rapidly while the transition to a nationally organized comprehensive approach to cyber-defense required sustained national efforts in depth over a longer time frame to achieve, in Singapore you see the identification of those lessons (largely from the Israeli experience) and then the implementation of them in terms of standing up new agencies and launching a comprehensive cybersecurity strategy in relatively short order. The upside to this model is agility in a changing threat landscape given the ability to pivot into new concepts and architectures as well as the ability to shift 'innovation' costs or 'learning pains' to other states. Persisting challenges, however, emanate from the level of trust in government and cohesion needed to sustain such robust state-led approach and the reality that pivoting requires in cyber-defense often requires more than just a top-down approach can offer (namely in the area of innovation).

This section's structure mirror's the prior sections on Finland and Israel proceeding in three parts. First, I provide background on Singapore's national defense posture. This includes background on their geostrategic position, defense strategy, and defense architectures (how the strategy was operationalized). Second, I illustrate how this foundation was directly leveraged into Singapore's cyber-defense posture and that it conceptually and operationally overlaps with the structural realties of cyber-defense. Third, I review several persisting challenges as Israel continues to build out a cyber-defense posture that addresses increasing critical interconnectedness.

3.1. Historical Background: Size as a Kind of Societal Defense Problem

For Singapore, which gained its independence from the U.K. jointly merged with Malaysia in 1963 and then from Malaysia in 1965, the early years of independence were precarious but not characterized by active inter-state conflict.

Importantly, while Israel's primary concern was territorial integrity, and the survival of its population, Singapore's primary concern was avoiding being absorbed by a neighboring state or being destabilized from within. Given multi-ethnic, multi-racial diversity, Singapore's first Prime Minster, Lee Kuan Yew, identified "build[ing] a nation out of a disparate collection of immigrants from China, British India and the Dutch East Indies" as his biggest challenge. Notably the 1960s and 1970s did emphasize how volatile these faultlines could be through a series of ethnic riots.[339]

[338] Author's Interview, 2018.
[339] Louisa-May Khoo, "Living with Diversity the Singapore Way Inclusion through Intervention," *Urban Solutions*, no. 10 (January 2017).

Yet, similar to Israel, Singapore also found itself in a position with limited to no natural resources, a small population, and a severe lack of strategic depth. Singapore is an island, 27 miles in length and 13 miles wide[340] ranking 191th globally in terms of size,[341] **with** a population smaller than 109[342] other countries largely condensed into a single sizable city. To the north lay the much larger Malaysia, a country Singapore had only recently succeeded from, and to the south a significantly larger Indonesia with the world's 4th largest population at its disposal.[343] As one Singaporean interviewee remarked, Indonesia would simply need to have its population stand on the coast and pee in Singapore's general direction to put them underwater.[344] In short, Singapore's diversity, "size, location, and proximity relative to the established and emerging powers of Asia" left it precariously placed geopolitically.[345] Notably, however, unlike Israel and Finland, since gaining its independence from Malaysia in 1965, it has not engaged in large-scale warfighting with any of its neighboring states.

Keeping this geostrategic context in mind, as a relatively small country apprehensive of two far larger neighboring countries with which it had a history of tension, Singapore's defense posture has developed out of the following concern: how can a relatively small, multi-ethnic state which lacks natural resources and strategic depth, maintain its independence and cohesion?

Singapore's answer was two-fold. First, it needed to address its numerical inferiority by leveraging its entire citizenry as security actors and then overcome the remaining disparity through qualitative superiority in terms of training and equipment. Second, it needed to address its lack of strategic depth by dissuading potential adversaries from engaging in conflict in the first place (deterrence). In other words, Singapore needed to be able to leverage all the resources at its disposal to overcome its numerical disadvantage in order to dissuade potential adversaries from engaging in conflict in this first place because the cost of success would simply be too high. This was not a deterrence by denial strategy.[346] It was more of a dissuasion by "we will take you with us so don't try it" strategy. This strategy was dubbed the Poisonous Shrimp after Singapore's first prime minister Lee Kuan Yew argued that "[i[n a world where the big fish eat small fish and the small fish eat shrimps, Singapore must become a poisonous shrimp,"[347] The inherent limitation here being, that for a poisonous shrimp to inflict harm on an adversary, it has to first be eaten.

In order to operationalize its Poisonous Shrimp defense posture, Singapore reached out to the global community to ask for assistance in setting up a defense posture as a newly independent state (the beginning of an importing and adapting best practices trend that has characterized Singapore's approach more broadly than just defense going forward). Far larger powers declined – namely India, Egypt and Britain – but Israel answered, sparking an over 50-year history of cooperation and exchange.[348] [349] This relationship with Israel in its early years of independence was irreplaceable. In

340 Kaushik Roy, *Sepoys Against the Rising Sun: The Indian Army in Far East and South-East Asia, 1941-45 (History of Warfare)*, Lam Edition (Brill Academic Pub, 2016). p124.
341 "East Asia/Southeast Asia :: Singapore," CIA World Factbook, accessed July 26, 2020, https://www.cia.gov/library/publications/the-world-factbook/geos/sn.html.
342 "East Asia/Southeast Asia :: Singapore."
343 "East Asia/Southeast Asia :: Singapore."
344 Author's Interview, 2019.
345 Kuper, "Taking a Closer Look at Singapore's 'Poison Shrimp' Defence Doctrine."
346 Nye lays out four types of deterrence and dissuasion. One of which is denial. For more information, refer to Nye Jr, "Deterrence and Dissuasion in Cyberspace."
347 Kuper, "Taking a Closer Look at Singapore's 'Poison Shrimp' Defence Doctrine."
348 Sharyn Mittelman, "Israel and Singapore – out of the Shadows," *The Jerusalem Post*, June 6, 2016.
349 Notably, Israel was not the only small, precariously placed country to answer the call. Taiwan did as well.

2016, Singapore's Prime Minister Lee emphasized its importance when he declared that "[w]ithout the IDF, the SAF could not have grown its capabilities, deterred threats, defended our island, and reassured Singaporeans and investors that Singapore was secure and had a future."[350] Interestingly, in an effort to be discrete and avoid increasing tensions[351] in the region, early Israeli advisors were famously referred to as Mexicans.[352]

Ultimately, Singapore developed a Total Defense architecture, which recognized that national defense would require "not only the Singapore Armed Forces (SAF) but also the civilian population. Through Total Defence, every sector of society is mobilized and has a part to play to ensure Singapore's security."[353] Total Defense comprised of six pillars: military, civil, economic, social, digital, and psychological defense. Under this umbrella, Singapore also implemented a national service requirement for all male citizens and permanent residents 18-50 years-old.[354] Taken together these pillars speak directly to both military and non-military threats to national the security and survival of the state.

Notably, as the quantity and quality of its national defense technology grew (largely through weapons and weapons systems acquisition),[355] Singapore shifted its posture away from the Poisonous Shrimp to the Porcupine. The assumption now is that Singapore would be able to successful defend against an attack rather than simply being subsumed.[356] The Total Defense operationalization remained, however.

There are three important insights encapsulated in this approach. First, as a small country in a precarious environment, national defense is a task that requires the mobilization of vast resources. This means that the responsibility for security cannot only be housed within a professional military alone but also with the citizenry as a whole being prepared for war even during times of peace in order to ensure national survival in times of crisis. Recall, this is an insight Finland and Israel share.

Second, the breadth and character of the economy is seen as a national security imperative. Economic defense, one of the six pillars of Total Defense, centered on "the government, business and industry organising themselves to support the economy at all times."[357] Here economic prosperity and national security are seen as intertwined. To this end, Singapore has a strong tradition of marketcraft with the government playing a significant role as a funder, provider, and/or organizer in education, healthcare, housing, and pensions. The state also, in a largely top-down manner shifted incentives to encourage the flourishing of certain industries, which was essential in the development

350 Mittelman, "Israel and Singapore – out of the Shadows."
351 Concerns over increasing tensions has been mirrored in Singapore's reluctance to publicly address offensive operations in general and cyberspace in particular. Notably, Singapore is the only country where I was unable to secure interviews within the Ministry of Defense. Despite numerous personal introductions from interview subjects to individuals within the MoD and repeated attempts on my part, all requests were denied. I was able, instead to secure a set of limited written answers to a few questions. But Singapore's position was very clear; they will not discuss in any detail the military or intelligence aspects of national cyber-defense, offensive or otherwise.
352 Mattia Tomba, *Beating the Odds Together*, *Beating the Odds Together: 50 Years of Singapore–Israel Ties* (World Scientific, 2019).
353 Singapore Civil Defence Force, "Total Defence | SCDF," accessed July 26, 2020, https://www.scdf.gov.sg/home/community-volunteers/community-preparedness/total-defence.
354 Ministry of Foreign Affairs Singapore, "National Service Obligation," accessed July 26, 2020, https://www.mfa.gov.sg/Overseas-Mission/Chennai/Consular-Services/National-Service-Obligation.
355 Narayanan Ganesan, *Realism and Interdependence in Singapore's Foreign Policy*, *Realism and Interdependence in Singapore's Foreign Policy* (Routledge Taylor & Francis Group, 2005).
356 Pak Shun Ng, "From 'Poisonous Shrimp' to 'Porcupine': An Analysis of Singapore's Defence Posture Change in the Early 1980s," Strategic & Defence Studies Centre, 2005.
357 Singapore Civil Defence Force, "Total Defence | SCDF."

of a knowledge-based, high-value added economy and the creation of hub for international business (primarily financial and commercial).[358] More specifically,

> After gaining its independence in 1965, Singapore relied on state-led development in various key sectors to boost its economy, establishing state-owned enterprises known as Government-Linked Companies (GLCs) as part of its industrialization plan. This injection of state capital helped to compensate for the lack of private sector funds and expertise. In 1974, the government set up investment company Temasek Holdings to manage these assets so that the Ministry of Finance could continue to focus on its core policymaking and regulatory roles.[359]

This trend continues to this day. For example, in an effort to address the need for low cost housing, the 1967 Land Acquisition Act gave the state the power to acquire land at low cost for public use in order to address concerns such as affordable housing. Today, "90% of land is owned by the state as opposed to 49% in 1965" and approximately 80% of Singaporeans live in public housing.[360] In short, marketcraft in Singapore relied on a strong, centralized state and enjoyed widespread popular and political support. Moreover, very explicitly, economic development was a core security challenge that the entirety of the country, including government, was responsible for pursuing. Rather than thinking of the character and development of the economy as largely separate from the national defense sphere, a vibrant economy is seen an essential condition for national security and national security an essential condition for a vibrant economy.[361]

Notably, in exchange for economic prosperity, social services, and security, the government (a single ruling party) enjoyed widespread support from its population. Despite being a democracy, the People's Action Party (PAP) has dominated elections, which are compulsory. Its rule dates back to Singapore's Independence in 1965.[362] While other factors have contributed to the PAP's electoral success (e.g. a first-past-the-post electoral model, diversify requirements, and fractured opposition parties in Singapore) the PAP first became entrenched in power after "having overseen rapid economic growth and prosperity"[363] in the early years after independence and has maintained a period of unbroken rule from 1965 to present.

Both the hierarchical nature of Singapore and the trend toward consensus were mirrored in my interview experience. For example, and as previously discussed in Chapter Three, unlike the other countries I interviewed in, several potential interview subjects across the government funneled my request to a handful of individuals sitting in a specific agency: the Cyber Security Agency of Singapore (CSA). In many of these same email responses, potential subjects indicated that they knew who I had already been in contact with (emailed) before I had even set foot in country. Interview answers were also the most uniform – both in terms of content and the specific language used – across government, industry, the press, and academia in Singapore. Unlike in the other four countries where I had conducted fieldwork, in Singapore there was a clear and well-rehearsed

358 Linda Y C Lim, *Singapore's Economic Development: Retrospection And Reflections (World Scientific Series On Singapore's 50 Years Of Nation-Building)* , Kindle Edition (World Scientific, 2015).
359 Chieh, "Policy Analysis: Singapore's Public-Private Partnerships for Cybersecurity in the Critical Infrastructure Sectors — Challenges and Opportunities." p 4.
360 Abhas Jha, "'But What about Singapore?' Lessons from the Best Public Housing Program in the World," World Bank Blog, January 31, 2018, https://blogs.worldbank.org/sustainablecities/what-about-singapore-lessons-best-public-housing-program-world.
361 As a point of contrast, like Israel, given its limited domestic market size, Singapore sought to become a key international market. But unlike Israel, Singapore developed as a hub for international business (financial and commercial activity) seeking a foothold Asia rather than the export-oriented innovative incubator model pursued by Israel.
362 Aradhana Aravindan and John Geddie, "Explainer: Why One Party Dominates Singapore Politics," *Reuters*, July 5, 2020.
363 Aravindan and Geddie.

narrative echoing throughout many of my interviews. For Singapore, efforts in any security space walk a fine line between publicly and privately addressed issues and concerns.

Third, like Finland, a threat does not need to be a physical invasion to be undermine the security of the state. Given the diversity of the population and the vital role that consensus and cohesion play in security and economic policy, both psychological defense and social defense (non-military concerns) were identified as core pillars of a Total Defense approach to national security. In short, the crux of Singapore's Total Defense approach is that private and public actors must ensure and safeguard the security of the state, broadly defined.

In conclusion, Singaporean security policy walks a fine line of aggressively bolstering defenses without aggravating regional neighbors. Located to the south of a far larger Malaysia and to the north of a far larger Indonesia, Singapore's economic success hinged on being a hub for financial and commercial activity in the region without exacerbating historical rivalries or being subsumed.

3.2. Developing a Cyber-Defense Posture: Areas of Overlap and Departure

While Singapore is widely regarded as a relatively late mover in the development of a national cyber-defense posture, a sentiment that was repeatedly shared by interviewees in Singapore and abroad, there was an earlier recognition of the threat and institutional development as early 2005. These earlier efforts, largely a recognition of the importance of security in information and telecommunications technologies (ICT) coincided with an awareness of security risks globally. It was not until 2009 that Singapore established an agency to oversee the security of critical infrastructure (what Singapore refers to as critical information infrastructure), the Singapore Infocomm Technology Security Authority (SITSA) under the under the Ministry of Home Affairs (MHA) and not until 2013 when it launched a Cybersecurity Masterplan that widened the scope of concern beyond critical infrastructure to the economy and society more broadly and incorporated R&D as an important area of focus. Noticeably, these efforts mirror the Israeli development on paper.

Yet, while this this early history is publicly, though briefly, documented in government records and in Singapore's 2016 Cybersecurity Strategy, it rarely came up as a locust of cyber-defense activity within interviews across the Singaporean ecosystem. One senior scholar described these early years as tracking global trends but lacking in robust commitment or implementation[364] while one government official working in this area replied, "I am sure there was some cybersecurity activity there",[365] when I asked about SITSA as a predecessor to the 2015 Cyber Security Agency (CSA), which oversees "cybersecurity strategy, operations, education, outreach, and ecosystem development."[366]In the two interviews in which this earlier period was directly raised by the interviewee themselves, notably both interviewees had spent time within the CSA, it was described as patchwork and limited but an important foundation while the scope and scale of commitment begin to really pick up from approximately 2010 onward.[367]

364 Author's Interview, 2019.
365 Author's Interview, 2019.
366 "Cyber Security Agency of Singapore," accessed July 26, 2020, https://www.csa.gov.sg/.
367 Author's Interview, 2019.

This disparity between the story the Singapore's Cyber Security Agency (CSA) tells about the evolution of a defense posture within Singapore[368] and the one leading experts in industry, government, the press, think tanks, and academia tell about the start of the Singaporean cyber-defense story is striking. The CSA placed its origins as early 2005, most everyone else placed its origins around 2013 with the Masterplan, which later fed into the creation of the CSA just two years later. Interestingly, several Israeli's pointed directly to the handful of years preceding 2015 as well, pointing out that Israeli experts had played an important role in those years in advocating for a comprehensive strategy and for the creation of a single agency with the remit of the non-military and intelligence aspects of cyber-defense.[369]

Overview of Timeline	
2005	Infocomm Security Masterplan (ISMP) - Info-communications Development Authority (IDA)
2008	Infocomm Security Masterplan - Info-communications Development Authority (IDA)
2009	Singapore Infocomm Technology Security Authority (SISTA) - the Ministry of Home Affairs (MHA)
2013	National Cyber Security Masterplan - SISTA
2014	National Cyber Security Centre (NCSC) - SISTA
2015	Cyber Security Agency of Singapore (CSA) – part of the part of the Prime Minister's Office and is managed by the Ministry of Communications and Information
2015	Cybercrime Command - MHA
2016	National Cybercrime Action Plan (NCAP) - MHA
2016	Singapore's Cybersecurity Strategy – CSA
2019	The Protection from Online Falsehoods and Manipulation Act

While these diverging stories make for a difficult assessment of the origins of a cyber-defense posture within Singapore, I have, tentatively, placed the starting date around 2013 for the purposes of this analysis, given that this was the period that seemed to be most widely recognized and referenced at the time within Singapore and by countries with longstanding relationships with Singapore in this domain. In many ways the mid-2010s seem to be the widely agreed upon start of the story – given what one interviewee termed a series of cyber weather events[370] that created national policy imperatives – and then with the creation of CSA in particular.

Singapore's historical approach to national defense provided three important areas of overlap as they built out their cyber-defense posture.

First, in Singapore, as in Finland and Israel citizens play an essential defense role. This provides an important conceptual foundation for conceptualizing citizens as cybersecurity actors but it also gives Singapore an architectural advantage. Like most all the states studied in this dissertation, Singapore has developed strategic, operational, and tactical capabilities within their Ministry of Defense more broadly and armed forces in particular. Take for example, the Defense Cyber Organization, which set up a 'cybersecurity command centre'[371] and "arm[ed] itself with 300 specialists trained in cybersecurity skills to better safeguard its systems and networks" as well as "opened a school to prepare future recruits with relevant skillsets in cyberdefence."[372] Importantly, these training

368 The Cyber Security Agency of Singapore (CSA), "Singapore's Cybersecurity Strategy," 2016. p7.
369 Three Author's Interviews, 2018.
370 The 2010s had a series of cyber-attacks that began to grab government and public attention. They demonstrated the weaknesses of the current system and served as a catalyst for sustained, in-depth action. Take for example, the campaign of hacks by "The Messiah" against the government in 2013. For more information, refer to F.C., "Hacking in Singapore - Messiah Complicated | Banyan" *The Economist*, December 7, 2013.
371 Eileen Yu, "Singapore Arms up on Cyberdefence Experts, Opens Cyberdefence School," *ZDNet*, February 20, 2019.
372 Yu.

initiatives encompass both career armed forces personnel and national serviceman. The later, like in Israel and Finland, will cycle out of service into industry and civil society with the cyber-defense education they received during their tenure.

Second, like Finland, Singapore has historically understood that threats to national security do not need to be military in nature to be incredibly costly or crippling. In this case, however, the concern is not primarily winter storms but national cohesion. Out of the six pillars of Total Defense, social defense focuses on "people living and working together in harmony and spending time on the interests of the nation and community" while psychological defense concerns itself with "each person's commitment to and confidence in the nation's future."[373] As previously mentioned, given the demographic makeup of the country, and the importance of cohesion, unity, and compliance in national defense and national policy more broadly, Singapore has understood threats that destabilize trust or magnify faultiness to be national security imperatives. Sound familiar? It should. This concern is central to the question of information operations in the digital age. These conceptual defense foundations lay at the heart of the Protection from Online Falsehoods and Manipulation Act, which passed in May of 2019.[374] This act

> requires online platforms — including social networking, search engine and news aggregation services — to issue corrections or remove content that the government deems false. Media companies that fail to comply face a fine of up to a 1 million Singapore dollars (about $722,000). Individuals found guilty of violating the law, both inside and outside the tiny Southeast Asian country, could face fines of up to $60,000 or prison for up to 10 years.[375]

Notably, this law has been controversial both at home and abroad given concerns over free speech, stifling public discussion, and undermining a free press.

This conceptual foundation – that threats to national security could be non-military in nature – also made it a logical step to add a seventh pillar to Total Defense: digital defense. Notably, this pillar also directly leveraged the conceptual foundation of citizens as security actors; "every individual is the first line of defense against threats from the digital domain."[376]

Third, Singapore has been able to leverage the same approach it used to develop and operationalized its prior defense posture into the development and operationalization of its cyber-defense posture. Notably, in contrast to Finland, which heavily relied on existing institutional structures, Singapore's strength lies not in the existing institutions per say but in how those institutions came about. In this area there two components of particular note. First, a robust learning and implementation model that allows Singapore to identify, adapt, and then implement best practices at home. Second, a centralized, top-down approach to societal defense.

These two components (importing and implementing through a centralized, top-down approach) also provide useful insight into the diverging narratives described above. One potential explanation for this disparity emerged from an interview with a leading security expert in Singapore. They argued that "Singapore was a late mover" because it could afford to be. In contrast, "Israel moved far earlier because they had a pressing threat" and that early, rapid, and robust commitment meant that

373 Singapore Civil Defence Force, "Total Defence | SCDF."
374 Ashley Westerman, "'Fake News' Law Goes Into Effect In Singapore, Worrying Free Speech Advocates," *NPR*, October 2, 2019.
375 Westerman.
376 Singapore Civil Defence Force, "Total Defence | SCDF."

Israel today has "had time to develop maturity".[377] In contrast, Singapore took some important steps early on, keeping pace with international trends, but did not commit the full weight of its national infrastructure until other states (namely a longstanding security partner and a widely considered leader in this space) had the opportunity to develop best practices and Singapore had the opportunity to learn from them. Given limited resources, it was best to wait for other states to go through the messy policy evolution process rather than sink those costs into policy development as well. But once Singapore commits to a strategy, "implementation is fairly rapid".[378]

This emphasis on waiting to be able to import best practices and then implementing them rapidly from the top-down across the state, economy, and society dominated interviews. If Singapore had one national strength as a small country, importing and implementing best practices was widely acknowledged as it. The interviewees laid out a consistent story. Singapore is particularly good at "control c and control v" one Singaporean interviewee jested.[379] Another emphasized that Singapore always looks abroad for best practices to implement at home before transitioning to ask me about what lessons I had learned from the other countries I am studying.[380] A government official pointed out that within Singapore there is "high confidence in government" and that means "implementation is fast, things move very fast because of that unity".[381] One Singaporean cybersecurity expert deeply familiar with both the Israeli and Singaporean models even went so far as to say, "[i]f Israel is herding cats, Singapore is herding sheep",[382] a sentiment a Singaporean government official lamented was largely accurate.[383] An Israeli cybersecurity expert working in Singapore chuckled when I dropped the 'herding sheep' assessment into our interview before lamenting that as a consequence, Singapore was unequally situated to implement but not necessarily innovate.[384] Hence, the significant focus on learning from others and not moving first or robustly until that process had taken place. Singapore may be slow to respond, but it is rapid in its implementation. Unity, confidence in government, a strong central government, and a history of compliance arose time and time again as the core strength of the Singaporean system, allowing it to rapidly set up new institutions and develop a national cybersecurity strategy once those lessons emerged in other states, and fundamental to how it leveraged and organized across society for defense of the state.

This learning process is supported by observable evidence within Singapore as well. As previously mentioned, the timeline for development loosely mirrors Israel's, a long-standing security partner with deep personal and institutional ties. This was not a coincidence. Several leading experts in Israel mentioned that they had directly worked with Singapore advising them on the development of the CSA in 2015 and the Cyber Security Strategy that came out the following year. In fact, the language of the Singapore's Cyber Security Strategy mirrors the Israeli strategy to an uncanny degree, including the identification of four identical priorities: building a resilient infrastructure, creating a safe cyberspace for business and society, developing a vibrant cybersecurity ecosystem, and

377 Author's Interview, 2019.
378 Author's Interview, 2019.
379 Author's Interview, 2019.
380 Author's Interview, 2019.
381 Author's Interview, 2019.
382 Author's Interview, 2019.
383 Author's Interview, 2019.
384 Author's Interview, 2019.

strengthening international partnerships.[385] [386] Notably, developing a vibrant innovation ecosystem in general and a cybersecurity ecosystem in particular has been Israel's historical and present strength, not Singapore's. It is also an area where a top-down approach presents a significant challenge, a topic which will be discussed in more detail in the subsequent section of this chapter.

This historical approach to the adoption and implementation of national defense has allowed Singapore to implement cyber-defense cohesively and fairly rapidly. One senior Israeli illustrates this most clearly when they expressed frustration that after advising Singapore on the importance of a single, national agency to oversee the non-military and intelligence aspects of cyber-defense, Singapore beat them to the punch by launching the CSA two years before Israel managed to create the Israel National Cyber Directorate (INCD) in 2017.

The top-down, centralized approach is also apparent in the language the CSA has used to describe some of its efforts. Take, for example, Exercise Cyber Star, nationwide cyber crisis management exercise focused on critical infrastructure security and preparedness. As of 2019, Exercise Cyber Star had been held three times and had expanded to cover all eleven of Singapore's designated Critical Information Infrastructure sectors. Yet, despite a large number of critical infrastructure providers falling into the category of private and not public entities, these exercises have been billed as a Whole of Government exercise rather than Whole of Society.[387] One Singaporean cybersecurity expert pointed out that there isn't really public private partnerships in Singapore in terms of collaboration but rather a cooperation through a hierarchical structure that pushes out solutions across government and down into industry and civil society.[388]

As a consequence, Singapore's strength in cyberspace, is not primarily born out of strong conceptual or institutional legacies that pre-date cyber-defense. Instead, the overlap is primarily located in how Singapore structures and deploys its societal defense architectures. This top-down, rapid implementation-based defense architecture relies heavily on a strong central government coupled with significant consensus and compliance. It also, notably, mirrors Singapore's historic approach to national defense in particular and national policy in general.

3.3. Persisting Challenges

The foundations, areas where overlap allowed Singapore to leverage an existing national defense approach into the development of its cyber-defense posture, have previously been discussed. Yet, the overlap between the existing national defense-posture the realities of cyber-defense is not complete. Three challenges persist.

First, as previously alluded to, innovation remains a pressing challenge for Singapore. Unlike Israel that maintains a vibrant innovation ecosystem, Singapore's market is largely a hub of international companies leveraging its location within Asia. Moreover, hierarchical, top-down processes and innovation rarely go hand in hand. Solutions flow one way, rather than the revolving doors and

[385] A topic I did not heavily discuss in the Israeli case-study but has been a focus of their activity beyond bolstering domestic capabilities. For small states in particular, levering cooperation is often a national security imperative, though in cyberspace given its global nature, cooperation is widely agreed to be a national security imperative for all states to some degree.
[386] The Cyber Security Agency of Singapore (CSA), "Singapore's Cybersecurity Strategy." and National Cyber Directorate, "Israel National Cyber Security Strategy in Brief."
[387] Refer to Cyber Security Agency of Singapore (CSA), "CSA Leads Whole-of-Government Exercise to Respond to Cyber Attacks," Press Release, July 18, 2017, https://www.csa.gov.sg/news/press-releases/csa-leads-wog-exercise-to-respond-to-cyber-attacks.
[388] Author's Interview, 2019

largely flat institutional hierarchy seen in Israel. Finally, the business culture does not reward failure. In Israel, "every year we have something like 1,200 startups born. And every year we have something like 1,000 startups die." [389] Its chaos, but productive chaos. As one Israeli deeply familiar with the acquisition process in Israel pointed out the pace of innovation to deployment is markedly different in cyber-defense: traditionally it would take 4-5 years once a defense technology was identified for it to be developed, tested, integrated, and deployed. In contrast, a cyber tool, could be found in the field within the year. Even more importantly, that traditional technology would continue to hold utility for years to come, whereas that cyber tool's lifespan could potentially be very short given the constant evolution of this man-made environment.[390] Given this reality, churn – the creation of new ideas that may be useful for solving present or potential future problems – is far more essential in cyber-defense than it was in prior defense spaces. Yet, this type of churn is not celebrated, promoted, or valued within the Singaporean market. In addition to having consequences for the types of resources available to the state, this also points to and amplifies a difficulty facing small states in general: securing the supply chain when you are not the primary producer across the stack or a products lifecycle. In short, it is one thing to realize the importance of an innovation ecosystem. It is another thing entirely to implement one without strong historical foundations from which to build. Israel has those foundations. For the most part, Singapore does not.

Second, several individuals raised concerns that Singapore's security environment has not been precarious enough recently and its economic success too great to motivate an effective cyber-defense posture. In short, the situation is too good and the population is becoming complacent. The two interviewees who raised this concern, one in and one out of government, pointed to decades of relative security and coupled with high GDP. The younger generations, they lamented, did not remember what it took to provide that security or build out the economy. They only know economic prosperity and security. As a result, "the strawberry generation" (a reference one interviewee made because they bruise easily)[391] are not willing to accept the trade-offs necessary for bolstering security, even cyber-security. Recall, since its independence Singapore has not had to fight a war and has transitioned from a Poisonous Shrimp posture to a Porcupine posture with an eye toward potential regional threats and according to 2017 estimated by the CIA World Factbook, ranked 38th globally in terms of GDP and 7th globally for GDP per capita. While this lament centered around a strawberry generation may feel akin to the intergenerational bickering we see in our own countries, it does point to an important area of concern. Can states sustain a societal defense architecture without facing a clear and/or pressing existential threat? Or are the costs simply too high in an absolute sense or as a matter of domestic perception?

Third, consensus and trust in government are essential components of this current approach – implementation through a largely top-down process. Yet, there are signs that both may not be as robust as they have been in year's prior and for older generations. First, as previously discussed, while older generations remember what went into economic development and were willing to make trade-offs to reap this benefits, younger generations do not remember those advancements and are less willing to continue to make those same tradeoffs. Second, electoral outcomes illustrate slight fraying as well. One government official pointed out that the elections in 2011 where a real shock to the pollical system. The governing party won all but six seats but the opposition party had made significant inroads compared to prior years. Despite a resounding victory for the governing party,

[389] Author's Interview, 2018.
[390] Author's Interview, 2018.
[391] Author's Interview, 2019.

the limited success of the opposition marked it out as a "watershed election" and represented "a distinct shift in [Singapore's] political landscape".[392] The almost near universal support the ruling party had historically enjoyed was now not quite so universal. A third example of a potential fraying of consensus is the ongoing debate over the Protection from Online Falsehoods and Manipulation Act, which passed while I was living in Singapore conducting interviews. It was one of the few areas that the 'consensus' in interviews was not as robust and a decision that average Singaporeans would actively question in conversations with me. Despite passing, it gained opposition not just abroad but domestically, and represented a shift in tone from prior policy areas.

3.4. Conclusion

In conclusion, Singapore's approach to national defense differs significantly from Israel's innovation-based societal defense posture and Finland's resilience-based societal defense posture. These differences do not mean, however, that Singapore does not have a societal defense architecture of its own that overlaps in core ways with the realities of cyber-defense. Singapore's relative strength lies in its ability to locate, adopt, and them implement best practices from other states quickly and cohesively across the state. This implementation-based societal defense posture allowed Singapore to rapidly create and launch the CSA, to import lessons from Israel and others, and to leverage its public private, civilian military resources in tandem for the defense of the nation. However, this historical foundation brings with it persisting challenges, namely in adopting an innovation ecosystem (a goal set in the Cybersecurity Strategy) and concerns over the viability of this approach long term.

SINGAPORE **Implementation-Based Societal Defense Architecture**		
Components of National Cyber-Defense	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**
Threats to national security not limited to kinetic, military operations	YES	YES
The homebase as a location for conflict	YES	YES
Citizens as security actors	YES	YES
The private sector as security actors	NO	RECOGNIZED and IMPLEMENTING
The breadth and character of the economy as a national security imperative	YES	RECOGNIZED and DEVELOPING
Strategic and operational oversight, coordination, and visibility across the defense-ecosystem	YES	YES

4. Conclusion

As small, precariously placed countries, both Israel and Singapore have placed a societal defense posture and built out a defense posture that leverages resources across the society in defense of the state. In both states, we can observe important conceptual and architectural foundations that overlap

[392] "Singapore Opposition Make 'landmark' Election Gains," *BBC*, May 9, 2011.

with the structural realities of cyber-defense. We also observe persisting limitations to their historical approaches, some of which speak specifically to their national context while others point to broader challenges facing all states regardless of foundations in this new domain of conflict. In short, the argument presented in this dissertation - as states try to solve for critical interconnectedness in the cyber era, some historical patterns of national defense are better suited to the operational realities of cyber-defense than others – travels beyond Finland and the U.S. to the Middle East and South Asia.

Chapter 6
Coming of Age in the Cyber Era: Estonia

Estonia is simultaneously "young and very small".
– A former Estonian government official[393]

1. Introduction

The preceding analysis of the development of a cyber-defense posture within the U.S., Finland, Israel, and Singapore illustrate how, as states try to solve for critical interconnectedness in the cyber era, some historical patterns of national defense are better suited to the operational realities of cyber-defense than others.

Estonia, self-dubbed E-Estonia, provides further evidence of overlap between a societal defense problem born of size and a societal defense problem born of critical interconnectedness. Unlike the other states studied in this dissertation, Estonia came of age in the cyber era. As a consequence, through an examination of Estonia's development of a cyber-defense posture, we can see these areas of overlap emerge in real time rather than retroactively.

Moreover, the edition of the Estonian story to this analysis also points to a deeper area of concern for great powers like the U.S. Yes, the U.S. is facing a more severe disjuncture between its historic kinetic defense posture and the realities of cyber-defense. Yet, even if the U.S. could start over, from scratch with no institutional and conceptual legacies, it would still face a significant challenge. Unlike Estonia, which has built out a societal defense posture cohesively (rather than adding cyber-defense into the mix decades later), the U.S. faces two different sets of defense problems – great power competition problem and a societal defense problem – with less strategic and operational overlap between their potential solution sets. This is not to say that these relatively small states are not also having to juggle important distinctions between a defense posture born from being small and precariously placed and a defense problem born from critical interconnectedness. Rather, their kinetic and cyber-defense postures represent a difference in kind rather than a difference in type.

2. Co-Development of a Kinetic and Cyber-Defense Posture

Like the other three Mice that Roar explored in Part II of this dissertation, Estonia is both small and precariously placed. However, unlike its neighbor to the north (Finland), Estonia lost its independence and was absorbed by the USSR during WWII. It did not regain its independence until the end of the Cold War, making it the youngest state examined in this project. It is also far smaller than Finland. As one Estonian interview subject remarked, "if Finland is small, Estonia is tiny."[394] As a consequence of its size, relative youth, and the emergence of this domain of conflict, Estonia co-developed a cyber and kinetic societal defense posture with each informing the evolution of the other rather an existing, robust societal defense posture being directly leveraged into a new domain of conflict.

[393] Author's Interview, 2018.
[394] Author's Interview, 2018.

After a brief period of independence before WWII (1918-1940), followed by Soviet occupation,[395] Estonia gained its independence from the Soviet Union in 1991. For context, ARPANET (the predecessor to the Internet)[396] had been invented almost ten years earlier in 1983 and that exact same year (1991) the World Wide Web became publicly available.[397] Estonia had re-gained its independence in the early years of the cyber era.

Overview of Timeline	
1991	Independence from USSR
1996	The Main Directions of the Estonian National Defense Policy [Total Defense and Territorial Defense Posture]
2001 & 2004	National Security Concepts [Total Defense that encompasses whole of society and Territorial Defense Posture]
2004	Estonia joins NATO
2006	Working Group on potential NATO Center of Excellence on cybersecurity formed within the Ministry of Defense
2007	Estonia moves the Bronze Statue - Cyberattacks
2008	First National Cyber Security Strategy (MoD)
2008	NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)
2009	Cyber Security Council established in the Government Security Committee
2010	The National Security Concept (NSC) and the National Defence Strategy (NDS) [Integrated Defense posture]
2011	Cybersecurity Portfolio transferred from the MoD to the Ministry of Economic Affairs and Communication
2011	Establishment of the Estonian Information System Authority (RIA)
2014	Second Cyber Security Strategy
2017	National Defense Concept [Comprehensive National Defense posture]
2018	Cybersecurity Law
2018	Sets up Cyber Command
2019	Third Cyber Security Strategy

For Estonia, these early years were primarily occupied with the task of building out an independent state and an advanced industrial economy on the doorstep of a far larger Russia. As one former Ministry of Defense official noted, this period was not characterized by strategic or operational maturity.[398] Another former government official recalled that "we didn't know what we were doing in the beginning" and that they had to "start from scratch".[399] So much so that this official recalled an incident where the U.S. withdrew a potential shipment of "used colt pistols" after the Finns advised that Estonia was still too young and providing them with arms might be "too provocative" for Russia.[400] Another Estonian government official described this period as "no people,[401] no plans, and no money".[402] One former Ministry of Defense official described the Defense Forces as a "mostly a rag-tag army" in the early years noting that the Commander of the Defence Forces was a retired U.S. Colonel (Aleksander Einseln).[403] Even early training (1992) for the professional staff relied on outside assistance; training was held in Finland.[404]

In 1996, the Estonian parliament approved the country's first national defense guidelines: a defense approach defined as a total defense and

[395] This is the term used by the vast majority of my interviewee subjects to describe this period.
[396] Ben Tarnoff, "How the Internet Was Invented," *The Guardian*, July 15, 2016.
[397] Martin Bryant, "20 Years Ago Today, the World Wide Web Was Born," *The Next Web (TNW) Insider*, August 6, 2011.
[398] Author's Interview, 2018.
[399] Author's Interview, 2018.
[400] Author's Interview, 2018.
[401] Estonia leveraged the diaspora, which returned home after regaining independence to assist with rebuilding the country.
[402] Author's Interview, 2018.
[403] Author's Interview, 2018.
[404] Republic of Estonia Defence Forces, "History – Estonian Defence Forces," accessed July 27, 2020, https://mil.ee/en/defence-forces/history-of-the-defence-forces/.

territorial defense model.[405] These two models first formally appeared in The Main Directions of the Estonian National Defense Policy, which was drafted by the Ministry of Defense five years after the Defense Forces had been formed and preceded any publication of a national defense strategy. These guidelines, however, cemented several conceptual foundations that would animate much of Estonia's defense posture going forward. Total defense pointed to the need of all citizens to act as security actors in defense of the state given limited resources and population. Territorial defense emphasized the importance of having a general force and a force broken down into constituent parts responsible for different parts of the territory. Given that much of the population, government, and industry was located in Tallinn, creating a viable organizational structure to defend the territory as a whole, especially the more remote areas bordering Russia, was essential. Notably, as one former government official explained, "the idea that all the people should participate in defending the country … it is nothing that just fell from [the] sky in 1996. It has always been here and it goes back to even the Cold War era and the previous Republic before the Soviet Occupation."[406]

Moreover, in addition to pointing to the importance of the citizenry to the defense of the state, these guidelines emphasized the importance of the Defense Forces in helping to address a wider range of issues than just those of a military nature: e.g. natural disasters and epidemics.[407] The aperture for national defense and national security was understood as far wider than kinetic invasion very early on in Estonia's development of a defense posture.

Yet, Estonia's defense posture during these early years very much remained nascent. As a former Ministry of Defense official noted, "people were looking to the Nordic model and the Anglo-American model but this was largely empty talk because the resources we had to devote were meager."[408] There were important conceptual foundations being laid down, but operationalization remained limited. This began to change in the early 2000s.

In 2001 and 2004 respectively, the government published two National Security Concepts, which summarized the state of security concerns, broadly defined, in Estonia as an important starting point from which to develop policy. Importantly, these documents widened the aperture of national defense from total and territorial defense in the face of military threats to a national defense posture that encompassed broader security concerns.[409] Namely, these documents sought to address the full range of "security policy aspects of various spheres of life, which all have an impact on the security of the Republic of Estonia. This means the inclusion into security policy in addition to the traditional military-political questions also domestic activities in the economic and social spheres".[410]

During this period (the 1990s through the early 2000s) Estonia also pursued an aggressive digitalization strategy in terms of the wider economy but most notable in terms of government and government services. As one former government official explained, Estonia faced two challenges when looking to build out state capacity and a thriving economy. The first was limited resources.

405 Viljar Veebel and Illimar Ploom, "Estonia's Comprehensive Approach to National Defence: Origins and Dilemmas," *Journal on Baltic Security* 4, no. 2 (February 7, 2019): 10–22.
406 Author's Interview, 2018
407 Tomas Jermalavičius et al., "Comprehensive Security and Integrated Defence: Challenges of Implementing Whole-of-Government and Whole-of-Society Approaches," 2014. p 48.
408 Author's Interview, 2018.
409 Jermalavičius et al., "Comprehensive Security and Integrated Defence: Challenges of Implementing Whole-of-Government and Whole-of-Society Approaches." p 48.
410 "National Security Concept of the Republic of Estonia ," 2004. p 3.

Digitalization allowed government services to be provided in a less resource intensive way. It was Estonia's answer to "how to actually govern the country, with 1.3 million people and scarce resources."[411] The second was legacy systems. After gaining its independence from the USSR, Estonia was left with old, legacy systems that could not effectively be updated. This required them to build out new systems in their place. Digitalization played an important role in that process.[412] In addition to e-governance and updating legacy systems, Estonia saw early successes with e-commerce, e-banking, and e-voting as well.[413] Today, Estonia is experimenting with digital embassies and e-residency.[414] With these transformations, Estonia went from a post-Soviet nation to what some have referred to as "the most advanced digital society in the world".[415] This critical dependency, however, also made national security imperatives in the cyber era a pressing concern.

In 2004, Estonia officially joined the North Atlantic Treaty Organization (NATO) operationalizing a deterrence strategy based on mutual assistance. With NATO membership secured, the government began to focus on building out both competency and presence in the alliance. Given the country's success with and dependence on digitalization, cybersecurity topped that list. As one former government official noted, in order to avoid provoking Russia, there was not going to be "U.S. troops on Estonian soil. No missile defense. So maybe something more neutral – like cyber".[416] A working group was set up under the Ministry of Defense to pursue a NATO Center of Excellence in Estonia focused on cybersecurity in 2006. In that same year, Estonia established its national CERT (CERT-EE) to monitor and assist states with computer incident response.[417]

One year later, Estonia moved a Soviet-era Bronze Soldier (a statue of a Russian soldier) from the city center of Tallinn to a war cemetery (also in Tallinn). This relocation was heavily disputed within Estonia, which still has a prominent Russian speaking population, and was condemned by Russia: "[f]or many Estonians, the Bronze Soldier represents 48 years of Soviet oppression. Meanwhile, Russians believe that the statue represents the triumph over the Nazis."[418]

The result was a series of cyber-attacks over three weeks targeting government networks and critical infrastructure, including domain names and telecoms.[419] As Jaak Aaviksoo, Estonia's Minister of Defence at the time, later explained, "[t]he attacks were aimed at the essential electronic infrastructure of the Republic of Estonia. […] All major commercial banks, telcos, media outlets, and name servers — the phone book of the Internet — felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation."[420] The cyberattacks did not occur in isolation, however. As a former official in the Ministry of Defense with intimate knowledge of these events clarified, the cyber-campaign was accompanied by riots in the streets, calls by Russian leadership for the Estonian government to step down, and concern that the Russian military might mobilize.[421] The moment felt

411 Author's Interview, 2018.
412 Author's Interview, 2018.
413 Nick Heath, "How Estonia Became an E-Government Powerhouse," *TechRepublic*, February 19, 2019.
414 Heath.
415 Ben Hammersley, "Become an E-Resident of Estonia," WIRED UK, March 27, 2017.
416 Author's Interview, 2018.
417 Republic of Estonia Information System Authority, "CERT-EE," accessed July 27, 2020, https://www.ria.ee/en/cyber-security/cert-ee.html.
418 Francis Tapon, "The Bronze Soldier Explains Why Estonia Prepares For A Russian Cyberattack," *Forbes*, July 7, 2018.
419 "How Estonia Became a Global Heavyweight in Cyber Security."
420 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *WIRED*, August 21, 2007.
421 Davis.

particularly precarious, even more so given that Estonia had only regained its independence from Russia just 16 years prior.

It just so happened, however, that Estonia had already gathered together some of the country's foremost cybersecurity experts into a working group within the Ministry of Defense and CERT-EE just a year prior. This formal network plus a wider informal network of cybersecurity experts across government and civilian sectors intensively worked the problem 24/7,[422] even undertaking the decision to temporarily severe the country's internet connection with the outside world. As one Estonian who had been stationed in the U.S. at the time remarked, suddenly they just didn't have access to their bank accounts (e-finance depended on that international connection) or much of anything else back home.[423] Estonia temporarily became an internet island. Notably, this informal network of experts was formalized with the creation of the Estonian Defence League's Cyber Defense Unit (*Küberkaitse Üksus*), a voluntary unit that explicitly built off the core responsibility of citizens as security actors present within the existing national defense posture, in 2010.[424]

That same year (2007), the Ministry of Defense took the lead on assessing what had happened, identifying lessons, and drafting the state's first cybersecurity strategy. They were handed this task for several reasons, each of which draws from interviewee's reflections on the decision. First, they had an existing working group (previously working on establishing a NATO Center for Excellence). This meant they had a foundation for the relevant community at hand. Second, cybersecurity was seen as a national security priority given the three-week long campaign they had just endured in 2007. Third, the MoD had the administrative capabilities needed, while other agencies were still in the process of building out such infrastructure. Fourth, this ad-hoc process faced serious time constraints given the preceding events and needed to be undertaken rapidly. The MoD was the easiest place to situate such an evaluation within the government given its central role in the preceding events. Fifth, and is often the case, personalities within the cabinet likely contributed to this decision. But, as one former government official remarked, "actually there was no one else who could do it, who had experience. Because the experience of handling this [2007] crisis was very much done by the Permanent Security of the Ministry of Defense and the private sector. At that time there was no RIA and only one CERT under the Ministry of Economic Affairs."[425]

As a result of this evaluation, in 2008 Estonia published its first Cyber Security Strategy, which laid an important foundation upon which to later build by identifying and protecting critical infrastructure, setting up an education ecosystem (centered on ten technical universities), and honing in on international cooperation.[426] That same year, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), which serves as a cyber-defense hub within the alliance, was stood up in Tallinn.[427]

422 One cybersecurity professional described in their interview the exhaustion they felt. Claiming that if they had not been able to get the situation under control when they did, people were going to fall over from near exhaustion and little sleep. Author's Interview, 2018.
423 Author's Interview, 2018.
424 Bruce Sterling, "Estonian Cyber Security," *WIRED*, January 9, 2018.
425 Author's Interview, 2018.
426 Republic of Estonia Ministry of Defence, "Cyber Security Strategy," 2008.
427 CCD COE, "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Cyber Defence Hub," accessed July 27, 2020, https://ccdcoe.org/.

Stemming from the 2008 strategy, a year later the Cyber Security Council was established in the Government's Security Committee[428] paralleling other sub-groups, such as terrorism, in order to better coordinate and manage national defense across the Estonian ecosystem. Their task was to "contribute to smooth co-operation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy."[429] At the heart of this strategy, as an official sitting within the Government's Security Committee emphasized, was a prevailing concern regarding Russia – the same concern driving the broader defense-posture.[430]

By 2010, with the National Security Concept (NSC) and the National Defence Strategy (NDS), had shifted the broader defense posture's focus from total defense to integrated defense.[431] The NSD explicitly noted that "[n]ational defence and the corresponding preparations are considered to be the tasks of many different institutions and people from the public and private sectors, including civil society."[432] The defense posture of Estonia had expanded to explicitly include six pillars: (i) military defense, (ii) civil contributions to military defense, (iii) assurance of internal security, (iv) international activity, (v) securing the continuous operation of vital services, and (vi) psychological defense. In the 1990s and early 2000s, national defense had been focused on overcoming limited resources by "civilian sectors supporting the military".[433] By 2010, national defense had formally expanded to include the security of civilian sectors as a national security imperative in its own right. The security of vital services (critical functions), a key aspect of the 2008 Cyber Security Strategy, had now officially made its way into the broader defense-posture, which was still heavily focused on the perceived Russian threat.

Recognizing the importance of civilian infrastructure and public-private roles and responsibilities in an era of cyber conflict and for cybersecurity more broadly, the cybersecurity portfolio was transferred from the MoD to the Ministry of Economic Affairs and Communication in 2011. 2011 also marked the birth of the Estonian Information System Authority (RIA), tasked with "ensuring the smooth and sustainable operation of a secure e-state" under the auspices of the Ministry of Economic Affairs and Communication.[434]

When I inquired into this decision, namely why the MoD gave away a rapidly growing portfolio, a key difference between the U.S. and Estonia emerged. In Estonia, the defense budget sits around 2% of GDP.[435] That percentage is not likely to significantly increase. With limited resources, taking on a portfolio like cybersecurity could prevent the defense apparatus from meeting other pressing national security challenges. Moreover, 2007 had illustrated the deep vulnerabilities of civilian infrastructure and that troops, in the kinetic sense, were not helpful in addressing an ongoing cyber-attack or sustained campaign. This had led to a shift in focus in 2008 away from the military, despite the MoD drafting that first strategy, and toward the civilian sector given high perceptions of need (a very vulnerable homebase and even more so given the transition to e-government and services).

428 Republic of Estonia Government Office, "The Coordination of National Security and Defence Management," accessed July 27, 2020, https://www.riigikantselei.ee/en/supporting-government/coordination-national-security-and-defence-management.
429 "How Estonia Became a Global Heavyweight in Cyber Security."
430 Author's Interview, 2018.
431 Jermalavičius et al., "Comprehensive Security and Integrated Defence: Challenges of Implementing Whole-of-Government and Whole-of-Society Approaches." p 49.
432 Veebel and Ploom, "Estonia's Comprehensive Approach to National Defence: Origins and Dilemmas." p 1.
433 Author's Interview, 2018.
434 Republic of Estonia Information System Authority, "Introduction and Structure," accessed July 27, 2020, https://www.ria.ee/en/information-system-authority/introduction-and-structure.html.
435 A requirement stipulated by NATO.

Given that focus, it made sense to shift cyber-defense (minus military and intelligence operations) under the auspices of the Ministry of Economic Affairs and Communication, which had an existing relationship with industry and could draw on a more diverse set of budgets (including the EU).

When I asked a government official sitting within the Ministry of Economic Affairs and Communication how it had secured this portfolio, they responded that the MoD "didn't want to do it. […] they did not want to spend [their budget] on economic measures and they didn't have competence [working with industry in this more expansive way]." The decision to shift venues had emerged out of the MoD while drafting the first strategy, and the Ministry of Economic Affairs and Communication would "need to take it and then grow competence".[436] As the new government ministry lead for the protection. preparedness, and resilience of the civilian sectors, the Ministry of Economic Affairs and Communication released Estonia's second Cyber Security Strategy in 2014.[437] By giving a non-military, internal security, or intelligence ministry the lead for the civilian aspects of cyber-defense, the Estonian model featured a mix between traditional security tools and economic tools; "they have their own traditions with how they interact with private sector and that more civilian activity" in addition to the tools the MoD could also bring to bear.[438]

By the mid-2010s, Estonia had moved beyond the conceptual foundations laid out in the 2008 strategy and into the operational specifics of protecting the homebase given critical interconnectedness. This included the establishment of RIA under the auspices of the Ministry of Economic Affairs and Communication. RIA was tasked with Crisis Management responsibilities[439] and supervision responsibilities[440] and houses the national CERT (CERT-EU),[441] Critical Information Infrastructure Protection (CIIP),[442] and the IT Baseline Security System (ISKE - based on the German model).[443] In addition to requiring certain best practices across the civilian sector and government, a notable feature of this operationalization included requiring government networks, critical infrastructure, and vital service providers to create risk assessments plans that map out their downstream dependencies and report them to be compiled and analyzed by RIA. The goal here was to map out the terrain and to gain intelligence necessary to begin to model single points of failure and potential patterns of cascading failures and contagion between critical infrastructure providers in the event of a cyber incident. In 2011 (part of the Emergency Response Act, which is regularly updated from 2008 onward), RIA crafted a cyber incident management plan for significant cyber-events as part of a broader series of incident management plans at the national level; RIA first tested that plan in a national level exercise in 2015.[444]

By 2017, these conceptual and operational shifts regarding resilient and secure critical functions were reflected within the broader defense posture. The new National Defense Strategy replaced the integrated defense posture with a comprehensive national defense model (*riigikaitse lai käsitus* – akin

436 Author's Interview, 2018.
437 Republic of Estonia Ministry of Economic Affairs and Communication, "Cyber Security Strategy 2014-2017," 2014.
438 Author's Interview, 2018.
439 Republic of Estonia Information System Authority, "Crisis Management," accessed July 27, 2020, https://www.ria.ee/en/cyber-security/crisis-management.html.
440 Republic of Estonia Information System Authority, "Supervision," accessed July 27, 2020, https://www.ria.ee/en/cyber-security/supervision.html.
441 Republic of Estonia Information System Authority, "CERT-EE."
442 Republic of Estonia Information System Authority, "Critical Information Infrastructure Protection CIIP," accessed July 27, 2020, https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html.
443 https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html
444 Author's Interview with former Estonian official with the Ministry of Defense and cybersecurity expert, 2018.

to Finland's Comprehensive Security model) focused on the dual missions of deterrence and resilience. Here, national defense was explicitly expressed as reliant on a whole of government and whole of society effort.[445]

In 2018, RIA's mandate further expanded with the passage of the Cybersecurity Act (drafted by RIA and the Ministry of Economic Affairs and Communications), which implemented the requirements of the EU Network and Information Systems Security Directive (NIS) in Estonia but also required (i) government networks and information systems and (ii) essential service and critical infrastructure to report significant cyber-security incidents to RIA. This bill also included, somewhat controversially,[446] the provision of law enforcement capacities to RIA in the event of a significant cyber incident.[447] Specially, it gave RIA the legal mandate to engage in investigations within private sector premises and systems.

The following year Estonia launched its third Cyber Security Strategy,[448] which focused on (i) development of the newly minted Cyber Command[449] (created in 2018 and mirroring USCYBERCOM) as part of the Defence Forces, (ii) the importance of consolidating resources and avoiding duplication, (iii) further efforts to integrate cybersecurity more cohesively into national defense planning documents, (iv) bolstering the underlying innovation ecosystem, and (v) a focus on bolstering and maintaining "an active and cohesive cybersecurity community" such as joint additional exercises with the private sector and technical information sharing.[450] In addition to continuing to build out domestic capacities through a systems-based approach this strategy marked a national recognition that cyber-defense "is a fast-changing area and the technology changes so fast that you cannot draft a strategy for more than 3-5 years. You have to actually change it."[451]

In conclusion, when I asked Estonians how the 2007 would have looked if they had happened today, they pointed to an institutional foundation that meant that Estonia would not need to rely on luck (happened to have set up a working group, for example) or a vibrant, informal network of cybersecurity experts rapidly coalescing in defense of the state. Instead the state – including government, industry, and civil society - are more secure, resilient, and prepared.

However, one former government official raised the concern that in exchange for this robust, formalized cyber-defense posture, Estonia may have lost some of the operational and tactical agility that had been essential to averting disaster in 2007.[452] They pointed specifically to the decision to sever Estonia's international connection, which cut off all in-bound traffic malicious or otherwise. This decision was tactical, undertaken not by senior leadership within the Ministry of Defense or the Prime Minister, but by operators sitting at station, staring at screens and typing away at keyboards. After speaking with individuals intimately familiar with the 2007 defense efforts at the level of the

445 Republic of Estonia Ministry of Defence, "National Security Concept," 2017. p 2
446 The comments demonstrate concerns from within segments of industry.
447 Republic of Estonia Riigi Teataja, "Cybersecurity Act," 2018.
448 Republic of Estonia Ministry of Economic Affairs and Communications, "Cybersecurity Strategy 2019-2022," 2019.
449 Piret Pernik, "Estonian Cyber Command: What Is It For? ," RKK ICDS Blog, November 26, 2018, https://icds.ee/estonian-cyber-command-what-is-it-for/. and Piret Pernik, "Report: Preparing for Cyber Conflict Case Studies of Cyber Command," December 2018.
450 Republic of Estonia Ministry of Economic Affairs and Communications, "Cybersecurity Strategy 2019-2022." p 17.
451 Author's Interview with government official, 2018.
452 Author's Interview, 2018.

operator, they all confirmed that this decision was made at station.[453] Today, any such action given the far-reaching consequences of creating an internet island would follow a more formal chain of command, which is a far slower process in a realm of conflict where speed is one of its defining characteristics.

4. Conclusion

In Estonia, we have a country that is simultaneously building out a societal cyber-defense posture and a national societal defense posture more broadly in tandem. There are clear feedback loops between and overlap that develops across these two postures. This iterative process illustrates the potential agility of smaller bureaucracies but also the conceptual and operational overlap between the defense postures states adopt when they are small and preciously placed and the defense postures all states are attempting to adopt in an era of cyber-conflict. In the case of Estonia, like in Finland, Israel, and Singapore, citizens and industry are understood to be security actors, the homebase is assumed to be deeply insecure, and security requires a network of resources across society leveraged in real time for crisis response.

ESTONIA **Co-Evolution of Societal Defense Architectures**		
Components of National Cyber-Defense	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**
Threats to national security not limited to kinetic, military operations	YES	YES
The homebase as a location for conflict	YES	YES
Citizens as security actors	YES	YES
The private sector as security actors	YES	YES
The breadth and character of the economy as a national security imperative	YES	RECOGNIZED and DEVELOPING
Strategic and operational oversight, coordination, and visibility across the defense-ecosystem	YES	RECOGNIZED and IMPLEMENTING

However, the Estonian experience also points to another challenge for states attempting to pivot to a societal defense posture in cyberspace: lack of an existential threat. 2007 wasn't just concerning because of the scale and scope of cyber-attacks targeting the state. Those activities were occurring in tandem with events in physical space and a deep abiding concern of potential Russian kinetic aggression or invasion. In many ways, the development of both a cyber and broader national defense posture were spurred on by a series of Russian aggression in the region.[454] Russia lay at the forefront of Estonian's minds. For example, one former Ministry of Defense official noted that applications to the Defense Forces radically increased after Russia invaded Georgia in 2008. The 2007 Cyber-attacks tapped into that existing concern as well – a

[453] Author's Interview, 2018. Their accounts are consistent with news reporting. For an example, refer to Davis, "Hackers Take Down the Most Wired Country in Europe."
[454] Benjamin Cooper, "Changes in Estonian Defense Policy Following Episodes of Russian Aggression," *Inquiries* 10, no. 10 (2018).

concern shared by all of the Mice that Roar – of a physically, precarious geopolitical position. The U.S., in contrast, does not face this same level of kinetic threat even as its homebase remains deeply insecure due to its dependence on and the interconnectivity of cyberspace.

PART III

Conclusion

CHAPTER 7
Contributions and Lingering Questions for Scholarship and Policy

"History does not so much repeat as echo […]."
- Lois McMaster Bujold[455]

1. Revisiting the Argument

As states try to solve for critical interconnectedness in the cyber era, some historical patterns of national defense are better suited to the operational realities of cyber-defense than others. This argument stems from the answer to two interrelated inquiries: (1) which factors drive national defense imperatives and underpin national defense capabilities in cyberspace and (2) which factors shape how successfully states adjust to the realities of national defense in the cyber era?

1.1. Evaluating Competing Explanations

At first glance, one might assume variation in cyber-defense capabilities is merely a resource story. Yet, the most economically and militarily resourced state, the U.S., is not far and away the leader when it comes to relative cyber-defense capabilities. In fact, consistent with the first puzzle presented at the start of this chapter, Makridis and Smeets found that resources (primarily GDP) was not a good predicator of one measure of cybersecurity capability: the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) rankings.[456] Even when we limit our evaluation of resources to cybersecurity industry, the U.S. should far outperform these smaller states. The significance of U.S. dominance in cybersecurity and the information technology industry more broadly should not be overlooked. The North American market, primarily driven by the U.S., comprises over half of global spending on cybersecurity[457] and more broadly, the Big Five tech giants (Alphabet, Amazon, Apple, Facebook, and Microsoft) are all American companies.[458] Moreover, in a 2018 ranking of the 500 most innovative cybersecurity firms compiled by Cybersecurity Ventures, the U.S. ranked first with 350 out of 500 firms while Israel came in second with 42 out of 500 firms. Finland and Singapore had 2 firms each make the list while no Estonian firms broke into the top 500.[459] These are just three realities not overlooked by the Estonians, Finns, Israelis, or Singaporeans. The fact remains, if this were primarily a resource story, due both to the quality and preponderance of resources these relatively small states should be significantly outperformed by the U.S. Yet, this is not the case.

Alternatively, one might assume cyber capabilities are primarily a story about states learning over time, with states that invested earlier rising to the top while those who invested later lag behind or struggle to put their resources to effective and good use. Yet, the leaders in cyber-defense capability span a variety of starting points. Some first or early movers like Israel and the U.S. can be found topping assessments. But they are joined there by states that could not be classified as first movers such as Finland and Singapore. Finland first began to develop their cyber-defense posture in the early 2010s as compared to Israel, which began in the late 90s and early 2000s. The U.S., like Israel,

455 Lois McMaster Bujold, *CryoBurn (Vorkosigan Saga)*, Kindle Edition (Spectrum Literary Agency, Inc. , 2011).
456 Makridis and Smeets, "Determinants of Cyber Readiness."
457 "Cybersecurity Market Report."
458 For a more detailed analysis of the American ecosystem see Aggarwal and Reddie, "Comparative Industrial Policy and Cybersecurity: The US Case."
459 The full ranking can be found at "500 Most Innovative Cybersecurity Firms in 2018."

began its policy development in late 90s and early 2000s. Singapore, notably, began in the mid-2010s. Importantly, these so-called 'later movers' rose to the top of assessments in relatively short order. Again, while learning clearly plays a role in policy development and evolution and that role can be seen within each country over time, the observable cyber-defense outcomes are not consistent with learning as the primary explanation for being a current leader.

Finally, one might assume relative capability is simply a function of variation in need. In short, states with the greatest threats emanating from cyberspace invest the heaviest in the development of cyber-defense capabilities. Yet, while variation in need is a good predictor of why some states are leaders and others lag far behind, it does not adequately explain why the commonly utilized variable of size does not appear to explain why some states are better equipped to address their need.[460] Why, given similar levels of need, do we observe the Mice that Roar ranking alongside far larger powers such as the U.S., which has far more resources to put toward addressing its cyber-defense needs. If leading states have greater levels of dependency on cyberspace when compared to states that are lagging behind, why haven't states with far more resources at their disposal far outperformed those with scarcer resources at their disposal?

Why then do mice roar in the cyber era? The answer lies, in large part, in the recognition of a second puzzle: why is cyber-defense seen as a less revolutionary defense problem by some countries while perceived as a largely novel defense problem by others? While at face value the two puzzles motivating this project may appear to be causally distinct, there is a single factor significant to both outcomes. A country's historical legacy –its geo-strategic environment and the defense posture it adopted in that environment – is as important to an analysis of cyber-defense outcomes as the core strategic and operational dynamics facing all states.

1.2. The Advantages of Being Small and Precariously Placed

The argument presented in this dissertation and supported by evidence gathered across five country cases consists of three constituent parts.

First, despite the field's repeated reliance on size as a measure for a state's defense capacity, we cannot accurately assess relative cyber-defense capability without taking seriously how states organize their resources in an effort to address the need they face (the threat environment they find themselves embedded within). States' cyber-defense postures – defense strategies and the defense architectures that support or operationalize those strategies in practice – shape why states develop certain resources and how they chose to deploy the resources they have at their disposal. As a consequence, defense postures are a critical component of defense capability and defense outcomes alongside the need or threat they face and the resources they can bring to bear.

Second, some defense postures are better suited for addressing the realities of national defense in the cyber era than others. Just as military capability in the twentieth century relied on a pattern of force employment that allowed militaries to reduce their exposure in response to increasing lethality[461], cyber-defense capability relies, in significant part, on a defense posture that allows states to leverage resources across their society in order to address a central problem they now face given

[460] In their 2019, Christos Andreas Makridis and Max Smeets found that states with a high dependence on cyberspace and a more threatening security environment were more likely to receive higher International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) rankings.
[461] Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*.

the realities of this domain: critical interconnectedness, i.e. their dependence on and the interconnectivity of cyberspace.

Third, importantly, states do not start with a blank conceptual and institutional slate every time a new defense problem is introduced or prior defense problems evolve. [462] Notably, however, pre-existing defense postures, developed in specific geo-political and domestic environments, can provide strong or weak foundations for the emerging national cyber-defense problem states now face. For the U.S., the conceptual and operational foundations underpinning its existing kinetic defense posture served largely as a weak foundation for the societal defense problem they found themselves in. In contrast, for the Mice that Roar, existing kinetic defense postures served as an important operational, and sometimes strategic, bedrock from which to build.

Why then, for a subset of relatively small states, do their pre-existing kinetic national defense approaches more closely resemble the desired solution set to national defense in cyberspace (a national defense posture that leveraged public and private actors in depth) than the pre-existing approaches found in far larger powers like the U.S.? Why are the national defense postures of historically great powers maladapted to the realities of national defense in the cyber era while those of historically weak states with limited resources provide core conceptual and operational foundations?

National cyber-defense is best understood not as an entirely novel defense problem facing states but as one kind of "societal defense problem": a national security threat where (1) the vulnerabilities are society-wide, embedded within the functioning of civil society, government, and the economy and (2) the resources states need to deploy in order to prevent an attack, defend against an ongoing attack, or recover from a previous attack are largely housed outside the military and even the government itself, i.e. within industry and the civilian population. Therefore, in order to address the core pressing national security concern facing states seeking to provide defense for their populations in the cyber era - critical interconnectedness - states must structure national cyber-defense in a manner that does not rely on military or intelligence agencies as the sole or even primary defense actors while simultaneously integrating both public and private actors into a cohesive, real-time national defense posture.

While for a great power like the U.S. this represents a stark departure from its kinetic national defense posture (strategies and the operationalization of those strategies in practice), for a subset of relatively small states, conventional (or kinetic) national defense similarly required a coordinated and focused effort across their society - the government, the private sector, and the citizenry. These societal defense architectures exist, in large part, precisely because these states were not historically strong and resource-rich. Importantly, the defense problem of deep vulnerability born from their relative size and geopolitical position has key conceptual and operational similarities with the problem of critical interconnectedness now facing all advanced industrial states in the cyber era.

In conclusion, as states seek to address the strategic and operational realties of national defense in cyberspace, historical experience matters. And for these mice that roar, the defense problem they faced as a relatively small state in a precarious security environment shares an important operational reality with the national cyber-defense problem they now face. By solving for significant geostrategic

[462] This concept is explored in depth in Chapter Two through a review of literature focusing on the stickiness of existing institutions and concepts over time.

vulnerability, these relatively small states also solved, in part, for critical interconnectedness. When it comes to cyber-defense, there are advantages to having been small and precariously placed.

2. Reviewing the Case Studies

Through the development of a rigorous research design and in-depth empirical analysis from five distinct country cases, I have sought to demonstrate that (1) the argument I developed is valuable for understanding outcomes within the five cases presented in this dissertation and (2) that the cases examined provide plausible grounds for believing this argument has wider utility for explaining the organization and efficacy of state cyber-defense postures more broadly while also (3) strengthening our understanding, theoretically and empirically, of the cyber-defense problem states currently face.

Each of the Mice that Roar – Finland (resilience), Israel (innovation), Singapore (implementation), and Estonia (co-evolution) – have important overlap between their kinetic defense postures and their cyber-defense postures. Recall, each of these states had strong historical foundations across six conceptual and operational categories required of any cyber-defense posture. The U.S., in stark contrast, did not.

2.1. Threats to national security not limited to kinetic, military operations

Several of the Mice that Roar had pre-existing defense concepts that recognized and systematically addressed national security threats beyond kinetic, military operations. Finland incorporated natural disasters, for example, into Comprehensive Security, while Singapore's Total Defense model prioritized social and psychological defense in addition to its armed forces and conscription. Estonia's defense posture in the 1990s included a recognition that pandemics and natural disasters represented could also be national security concerns and require the assistance of the state's Defense Forces in any national response. By the 2010s, the defense posture had expanded further to include national defense concerns such as psychological defense.

2.2. The homebase as a location for conflict

For all of the mice that roar, the homebase was assumed to be vulnerable (given their threat environment and limitations born of size) and a location for hostilities if conflict were to erupt. Actively defending a contested homebase is not novel, though historical models focused on territorial integrity, maintaining sovereignty, and/or national survival. In contrast, for the U.S., conflict and warfare traditionally occur elsewhere, outside its borders. Other than in the realm of nuclear weapons, national survival was not directly threatened. The U.S. had not fought a war within its own territory since the 1800s. While Estonia, Finland, Israel, and Singapore's defense postures centered homebase (or territorial defense), the U.S.'s defense posture centered great power competition.

2.3. Citizens as security actors

Similar to the prior category, all four of the relatively small states examined in this dissertation recognized the importance of leveraging its citizenry in defense of the national and developed defense architectures to utilize citizens as security actors in practice (e.g. conscription). The U.S., again in stark contrast, relied on a relatively small subsection of its citizenry for national defense. As a consequence, the U.S. was faced with the dual challenge of cultivating and institutionalizing a culture of service for national security purposes at the same time as developing and distributing cyber-hygiene best practices and creating a model that allows cybersecurity experts and practitioners to effectively come together in defense of the state in real-time.

2.4. The private sector as security actors

In this area, Finland had the strongest foundations given its Comprehensive Security approach and a robust historical focus on resilience. Estonia's Comprehensive National Defense posture closely mirrors Finland's model but unlike Finland, it is relatively early in the development and implementation stages of this particular iteration of its defense posture (first announced in 2017). Finland, in contrast, had a robust and mature model already in place prior to concerns over cyberattacks targeting critical functions of society, government, and militaries.

Israel found itself needing to pivot and incorporate concepts of resilience, continuity of the economy, and critical infrastructure protection into its national defense posture. Israel first recognized the importance of the private sector in terms of maintaining critical functions in the 1990s and set up its first institutional response in 2002 (establishment of RE'EM). Yet, it was not until 2015 with the creation of the National Cyber Security Authority (NCSA) that Israel had the ability to systematically address the security and resilience of its government, economy, and society more broadly and not just the narrower remit of protecting the computerized systems of a subset of vital civilian and government infrastructure (the task of RE'EM). This pivot was aided by a history of strong public private cooperation and coordination for national defense purposes and a history of agility born from tactical realities directly shaping national strategy.

Notably, Singapore was able to achieve a similar institutional transition as Israel in a far shorter time period by leveraging its own historical strength: importing lessons learned by far earlier movers in this space (largely from Israel) and implementing them rapidly in a top-down manner.

Like Israel and Singapore, the U.S. did not have a strong institutional foundation upon which to build in this area. However, unlike Israel and Singapore, which were able to leverage broader approaches to national defense and a consensus over a pressing national security imperative to push forward the transition process, the U.S. has struggled to break down its institutional silos and build out the necessary interactions between industry and government in order to leverage industry players as security actors in practice.

2.5. The breadth and character of the economy as a national security imperative

In this area, Israel has the strongest historical legacy from which to build. In order to overcome limited population and a lack of strategic depth, Israel deliberately and robustly pursued a qualitative edge over potential adversaries. To achieve this goal, innovation was prioritized as a national security imperative. The result was an expert-led, knowledge-based economy heavily centered around science and technology. This systems-based approach actively leveraged contributions from and feedback effects between industry, educational institutions, and government and centered agility (e.g. startup culture) and a so-called 'revolving door' between government, academia, and industry for the development and transmission of ideas and solutions. For Israel, national defense and the economy are inseparable

While Finland, Singapore, and Estonia have recognized the importance of an innovation ecosystem that provides agile security solutions not just for government and military but also for the civilian sector more broadly, they have relied most heavily in existing (linear and more limited) conduits for R&D such as "government as customer" and "government as funder" models. Their efforts have been hampered by concerns over lack of funding (in comparison to Israel) and the ability to develop a robust domestic market given the very real limitations of their relative market size. Singapore, in particular, has faced the additional challenge of fostering innovation in a highly hierarchical,

centralized system. Notably, however, for all three of these states, a vibrant economy is seen as an essential condition of maintaining their independence and robust forms of marketcraft are readily deployed to achieve that end.

Strikingly, despite having the most robust and diverse domestic ICT and cybersecurity market, the U.S. has not been able to leverage those industry resources in a dynamic and agile fashion for the defense of society. Instead, like Finland, Singapore, and Estonia, the U.S. has primarily relied on existing (linear and more limited) conduits for R&D. As one former U.S. government official and two current academics all separately joked in interviews, the U.S. seems largely allergic to industrial policy conversations (or at the very least such conversations have now become heavily politicized). Marketcraft and national security remain institutionally siloed and largely conceptually distinct lines of effort rather than deeply intertwined in purpose or practice.[463]

2.6. Strategic and operational oversight, coordination, and visibility across the defense-ecosystem
In this area, Singapore has the strongest historical foundations, which were leveraged into its cyber-defense posture. Singapore's relative strength lies in its ability to locate, adopt, and them implement best practices from other states quickly and cohesively across the state. This implementation-based societal defense posture allowed Singapore to rapidly create and launch the Cyber Security Agency (CSA) providing strategic and operational oversight, coordination, and visibility across the defense-ecosystem; to import lessons from Israel and others; and to leverage its public private, civilian military resources in tandem for the defense of the nation.

Despite its position as an early mover in this space with over 20 years of dedicated cyber-defense efforts, it was not until 2017, that Israel addressed one important and until that point persistent silo, which had hindered strategic and operational oversight, coordination, and visibility across the Israeli defense-ecosystem. Prior to 2017, three organizations each tasked with a different piece of the cyber-defense posture: the RE'EM, the INCB, and the NCSA. With the establishment of the Israel National Cyber Directorate (INCD), which combined the RE'EM, INCB, and NCSA under the auspices of a single institution, Israel for the first time in its history, had a single institution with oversight over both the defense and resilience of the critical functions of society but also the innovation ecosystem (the systems-based approach for developing and deploying high quality capacity across the defense and intelligence agencies but also civil society more broadly).

Estonia sought to bolster its capabilities in this area by establishing the Cyber Security Council in 2018. It sits within the Government's Security Committee in order to better coordinate and manage national defense across the Estonian ecosystem. Their task was to "contribute to smooth co-operation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy."[464]

Finland, has similarly recognized the important of strategic and operational oversight, coordination, and visibility through a series of reports for the Prime Minister's office, but as of yet, has not created a new or adapted an old institutional framework to fill this gap.

In the U.S. this area has been characterized by active debate, hard starts, and persisting institutional silos and fragmentation. Notably, in an effort to address the persisting lack of strategic and

[463] Conversations during or following up on policy meetings and briefings in the U.S., 2018 and 2019 respectively.
[464] "How Estonia Became a Global Heavyweight in Cyber Security."

operational oversight, coordination, and visibility, the U.S. established the cyber zraw, only for the position to be eliminated two years later.

2.7. Conclusion

As a group, the Mice that Roar demonstrate overlap between the societal defense postures adopted by relatively small imperiled states and a cyber-defense posture centered on addressing critical interconnectedness. The U.S., in contrast, is an outlier with limited historical overlap between its prior defense posture and the operational requirements of cyber-defense.

As a consequence, for Finland, Israel, and Singapore, this overlap allowed them to leverage existing conceptual and institutional foundations directly into their development of a cyber-defense posture rather than having to overcome institutional inertia and path dependence in order to effectively develop and pivot to new defense posture. For Estonia, this overlap allowed for the co-evolution of two largely complimentary and mutually reinforcing defense postures (one focused on the kinetic and focused on the cyber facets of national defense) over time. In contrast, the much larger U.S. had little to no overlap across these categories and instead has faced the daunting task of pivoting to a societal defense posture for cyber-defense rather than the less extensive task of extending and modifying an existing societal defense posture.

General Overview of Case Studies

	Finland		Israel		Singapore		Estonia		U.S.	
Components of National Cyber-Defense	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**	**Component of Kinetic Defense Posture**	**Component of Cyber-Defense Posture**
Threats to national security not limited to kinetic, military operations	YES	YES	NO	YES	YES	YES	YES	YES	LIMTED	YES
The homebase as a location for conflict	YES	YES	YES	YES	YES	YES	YES	YES	NO	YES
Citizens as security actors	YES	YES	YES	YES	YES	YES	YES	YES	NO	RECOGNIZED
The private sector as security actors	YES	YES	NO	YES	NO	RECOGNIZED and IMPLEMENTING	YES	YES	NO	RECOGNIZED and DEVELOPING
The breadth and character of the economy as a national security imperative	YES	RECOGNIZED and DEVELOPING	YES, ROBUST (Innovation Ecosystem)	YES	YES	RECOGNIZED and DEVELOPING	YES	RECOGNIZED and DEVELOPING	LIMITED	RECOGNIZED
Strategic and operational oversight, coordination, and visibility across the defense-ecosystem	YES	RECOGNIZED and DEVELOPING	YES	ECOGNIZED and IMPLEMENTING	YES	YES	YES	RECOGNIZED and IMPLEMENTING	YES	DEBATED

3. Contributions to Scholarship and Policy

While we know a great deal about the dynamics of kinetic conflict and security, we know comparably little about the dynamics of cyber conflict and security. This impedes both our academic understanding of effective national cyber-defense as well as our ability to construct effective cybersecurity policy. The contributions and implications of this dissertation fall into three buckets: (i) theoretical and empirical contributions to the study of cybersecurity, (ii) contributions to theory development within international relations and security studies, and (iii) the policy implications of this work more broadly. Each is explored in turn below.

3.1. Theoretical and Empirical Contributions to Cybersecurity Scholarship

By focusing specifically on smaller states, this dissertation makes four theoretical contributions to the study of cybersecurity in international security studies. First, it directly engages with and strengthens the emerging cybersecurity research centered on the unique importance of public-private, civilian-military roles and responsibilities for national cybersecurity purposes. Throughout this dissertation, I examine the structural conditions driving the necessity of a societal defense architecture – critical interconnectedness – as well as provide an explanation for observed variation in the adoption of these architectures and effectiveness of efforts to address this operational reality in the cyber era.

Second, it draws upon historical institutionalism and path dependence literatures within political science, highlighting the role that history plays in shaping current and future policy decisions and, in this specific instance, how existing security approaches can be maladapted to the realities of emerging security challenges. Through the five cases studies presented in this dissertation, I demonstrate how these relatively small states have been able to leverage existing conceptual and operational foundations while great powers like the U.S. have struggled to pivot toward a defense posture that addresses this structural reality.

Third, this dissertation helps to frame cybersecurity less as a path-breaking topic and, more appropriately, within the bounds of a well-studied topic in international security: the geopolitical dynamics of conflict and consequently, the geopolitical dynamics of national defense. Paradoxically, however, the U.S.'s historical strength served as an important disadvantage in the pursuit of national cyber-defense efforts because, as a great power, its geostrategic environment did not necessitate the development of and continued maintenance of a societal defense architecture. In contrast, for the Mice that Roar, being small and less resource rich served as an advantage because their historical geostrategic environments presented them with a societal defense problem that necessitated a coordinated and focused effort from their entire society - the government, the private sector, and the citizenry.

Fourth, while much of the focus within the nascent cyber-defense literature has been on how the strategic realities of cyberspace shape outcomes, less attention has been paid to the operational realities of national cyber-defense. This dissertation rests soundly within that operational level of conflict. As a result, my research explicitly differentiates between technical expertise and the operational and strategic components of national cybersecurity efforts. Notably, the operationalization of strategy - spreading and applying technological expertise to broad swathes of industry, civil society, and government; information sharing and coordination in response to threats and in determining responsibilities between public and private actors; pooling of resources to stay ahead of the evolving threat landscape, maintaining critical infrastructure and services, etc. – represents one of the greatest challenges for effective policy in this space.

Empirically, through extensive within country and across country case study research, this research offers an unusual contribution by collecting frank, rich commentary directly from cybersecurity practitioners across five distinct countries. These empirics take on greater value when the contours of the nascent cybersecurity field within political science is considered. The threat of cyberattacks are one of the central national security challenges currently facing advanced industrial economies. It is altering the nature of warfare and conflict itself, and along with them, the character of security policy and the diversity of states prominently pursuing those policies. Notably, however, explaining these national defense outcomes has only recently become a focus of political scientists and security scholars.[465] The overwhelming focus of this nascent literature has been on large states, such as the U.S., U.K., China, and Russia. This leaves the question of how smaller states have pursued their national defense in cyberspace systematically unanswered.

3.2. Contributions to International Relations and Security Studies

In addition to contributing to cyber conflict scholarship, this research contributes directly to theory development within international relations and security studies more broadly. As previously mentioned, the largest, most powerful military actors are frequently assumed to also be the best positioned to provide national defense for their populations. Size and power are frequently conflated. Yet, resources are only part of the story. How those resources are organized and developed for specific strategic purposes are of equal importance, and often overlooked or underexamined in mainstream scholarship. In short, this research on the cyber-defense postures of smaller states further points to the limitations of a largely resource-based approach to power and national security capabilities within cyber conflict studies but also power and national security capabilities more broadly.

3.3. Implications for Policy

Finally, what can the Mice that Roar teach great powers about national cyber-defense? A primary motivation for this project was the pressing policy challenges facing states seeking to provide national cyber-defense for their populations. With this in mind, the broader policy implications of my doctoral work are three-fold.

First, my work takes an important step in the ongoing process of delineating systemic dynamics from situational dynamics in cyberspace: i.e. dynamics all states face due to the threat space versus dynamics that are significantly mediated through national contexts and circumstances. This draws attention not only to the systemic reality of critical interconnectedness but also to how the national contexts and circumstances of larger powers like the U.S. amplify this challenge in unique ways.

This feeds directly into the second policy contribution. In our efforts to understand cybersecurity in the context of national security, previously overlooked policy insights for the organization and efficacy of national cyber-defense efforts lay outside more heavily studied states such as the U.S. Notably, we observe a subset of small states crucially deploying societal defense architectures to support national cyber-defense efforts while great powers such as the U.S. struggle to do the same.

[465] Efforts to map out the nascent field have been undertaken by the Cyber Conflict Studies Association (CCSA). For further information, reference their 2016 State of the Field report, their 2017 and 2019 State of the Field series of White Papers, and their 2018 op-eds published by the Council on Foreign Relations. "Cyber Conflict Studies Association (CCSA)," accessed July 27, 2020, http://www.cyberconflict.org/.

These states provide potential models both for how to conceive of and operationalize a societal defense approach to national cyber-defense.

Third, and finally, by comparing Estonian, Finnish, Israeli, and Singaporean kinetic societal defense problems stemming from their geostrategic position to the societal defense problem emerging critical interconnectedness in the cyber era, this dissertation highlights areas where even the Mice that Roar must pivot away from historical foundations to address criterial interconnectedness more effectively. Notably, while cyber-defense is a kind of societal defense problem, it diverges from the kinetic iteration these states faced in several key areas: (i) much of the conflict space falls below the threshold of war or armed conflict and (ii) conflict in the cyber era is comprised not just of discrete crises or events, but constant contact between adversaries.

In conclusion, taken together these three contributions provide the beginnings of a blueprint for states seeking to pivot to or extend an existing societal defense posture. By scrutinizing tangible, policy-oriented solutions to the problems associated with the pursuit of national cyber-defense, this project directly advances policy-relevant research aimed at this complex and pressing global challenge.

4. Lingering Questions and Future Research

In addition to the contributions outlined above, a series of questions of import to both scholarship and policy emerge from this project. Five lingering questions and opportunities for future research are explored in this section. Each represents a gap in our academic understanding of cyber conflict while also speaking directly to a pressing policy challenge facing states in this domain. By laying them out explicitly in this concluding chapter, I hope they will motivate and inform future research on national cyber-defense.

4.1. What Factors Shape How Efficiently and Effectively a State Can Pivot?

Many states do not have the historical foundations found in states like Estonia, Finland, Israel, and Singapore at their disposal. Yet, they have widely recognized the importance of a coordinated, society-wide effort to address national cybersecurity concerns. Therefore, what factors determine how quickly and effectively a state can pivot to a societal defense posture? Future research could focus on variation between states pivoting to a societal defense posture without the foundations found in the Mice that Roar – such as Australia, the U.K., and the U.S. – to evaluate which factors shape the form, speed, and efficacy of this process.

Larger states may be at a disadvantage when attempting to shift to a societal defense architecture. The core of this concern hinges on size as a mechanism for trust but also as a condition for easier reorganization of existing bureaucracies and resources. First, fewer degrees of separation between citizens creates an environment where greater personal ties, familiarity, and regular face to face contact directly enable the breadth and depth of coordination required for adopting a societal defense architecture (or the whole-of-society/whole-of-nation defense posture) in cyber-defense. Yet, we know that larger states, such as the U.S. and U.K. during WWII, have adopted societal defense architectures in response to an existential threat. Although, for a limited duration of time.

Second, smaller structures can be more agile than their far larger, institutionally dispersed and bureaucratically dense counterparts. Agility takes on greater strategic importance in a threat space that is rapidly evolving. A commonly reoccurring analogy in interviews conducted for this project referred to smaller states as speedboats while the U.S. was an aircraft carrier. Speedboats have less

resources to bring to bear, but can maneuver quickly to bring those resources to bear. An aircraft carrier, in contrast, has a large turn radius and will struggle to bring its resources to bear in a quickly evolving competition space.

In conclusion, future research should explore which factors shape and/or constrain how states defense policies evolve beyond historical overlap such as population size, the structural realities of the domain itself (rapidly evolving in a manner that requires significant defense posture agility or not), or a series of domestic political factors unique to certain subsets of states (e.g. the degree to which there is foreign and security policy consensus domestically).

4,2, Are Great Powers at a Disadvantage in Cyber conflict?
Can great powers like the U.S. sustain a societal defense posture in cyberspace?

There are three central challenges of particular note to states like the U.S. attempting to pivot to a societal defense architecture.

First, these states do not face an existential threat, the type of threat that historically served as the justification for the costs associated with building and maintaining a societal defense architecture for the Mice that Roar. Put another way, while cyber-defense requires a coordinated effort across society, that coordination is not costless. Resources spent on security cannot also then be spent again on other domestic and foreign policy imperatives. Prioritizing security also frequently require deliberate tradeoffs between other core goals within a society such as economic growth, business competitiveness, efficiency, and privacy. As a consequence, national defense postures are not merely the result of the threats a state faces but the result of a series of domestic choices and tradeoffs. The question then becomes, for a state that is not facing an existential threat, which choices and tradeoffs are likely to be seen as too costly? Is the cost of a societal defense architecture likely to be domestically justifiable only in a limited set of security circumstances, and if so what factors determine those boundaries?

Second, states without a historical operational foundation are not merely pivoting to a societal defense posture. These states now face two different sets of defense problems - great power competition and a societal defense problem - with less strategic and operational overlap between their potential solution sets/defense postures. The U.S., for example, is now faced with the unique challenge of having to maintain two largely distinct, defense postures: one focused on deterrence through MAD, balancing peer competitors/rising powers, and targeted interventions (e.g. special forces) on the one hand and then a societal defense architecture in the other. This is not to say that these relatively small states are not also having to juggle a kinetic and cyber-defense posture. Just that in their case, their kinetic and cyber-defense postures represent a difference in kind rather than a difference in type.

Significantly, if great powers cannot sustain a robust societal defense posture in cyberspace (whether due to a lack of existential threat or the burden of simultaneously maintaining two largely distinct postures), the decision space available to these states may be far more limited than those of their smaller counterparts and, worryingly, may be heavily weighted toward more preemptive and offensive activity. Such a constrained decision space for some of the most well resources and traditionally powerful states in the global system would concerningly have downstream impacts on the stability of and escalatory dynamics in this emergent domain of conflict more broadly.

4.3. To What Extent are Solution Sets Transferrable between National Contexts?

Notably, a significant driver of these relatively small states' stories is how historical institutions provided an institutional foundation that was well suited to the realities of addressing cybersecurity at the national level. To what extent, then, are their models exportable? What outcomes, such as high levels of trust and cooperation between public and private actors, can be replicated by other countries?

Many states will not have strong pre-existing societal defense foundations, yet these four cases point to both conceptual and operational lessons of note. Cybersecurity at the national level requires the defense of a complex, interdependent system that is society-wide and can transcend national borders. In their strategic inception, these states' defense postures sought to alter the behavior of both private and public actors through an array of statutory requirements, government resolutions, and voluntary participation in established frameworks to address this core concern. As such, Estonia, Finnish, Israeli, and Singaporean approaches can provide useful goalposts for understanding and addressing vulnerability and risk in cybersecurity strategies more broadly.

Large states, however, face a very different institutional landscape than Estonia, Finland, Israel, and Singapore simply as a product of their size. The bigger you are, the more bureaucratic. This density of institutions is readily observable in the U.S. spanning national, state, and sub-state jurisdictions. This increases the number of potential silos and opportunities for duplication and decreases the state's ability to effectively coordinate a cohesive, national response. The larger an organization – or in this case a state – becomes the more interactions need to be formal rather than informal in nature. For the mice that roar, their population size and subsequent bureaucratic density allows for more agile, less formalized mechanisms for cooperation and coordination. As the joke goes, in small countries everyone knows everyone. And that is even more true when talking about a subset of the populations such as cybersecurity experts in government, industry, and academia. The question then becomes, how can great powers, which like the U.S. tend to boast large populations or territories, formalize mechanisms for a societal defense posture that can capture some of the positive outcomes these smaller countries have achieved through less formally and bureaucratically dense processes? And which outcomes, say a robust innovation ecosystem with a tight feedback loop between security apparatus and industry, will a larger country simply not be able to replicate in any depth.

Yet, lessons from these states can still travel in two ways – conceptually and operational. The question isn't whether or not he U.S. should set up reserve forces in cyberspace (a cyber national guard) but rather how can the U.S. create a formal network of citizens dispersed across the country who can come together in real time for a coordinated response? In reality, this operational need lays at the crux of Estonia's Cyber Defense League. These aren't soldiers that are deployed to some metaphorical 'cyber front' but rather the formalization of an informal network to bolster capacity outside of government networks at the national level in times of crisis.

Take for example, the institution of conscription which is a shared foundation across all four of the smaller states presented in this dissertation. Conscripts serve a four-fold function beyond their role within the military operations across these states in terms of cyber-defense. First, as a mechanism for education – best practices – for a large portion of the population. Second, in creating a shared network – ties that then span across industry and elsewhere. Third, helping shape narratives around national security and instilling national security responsibility ethos across the population. Four, as a model that can be mirrored (though really only in name only) to organize a response to a cyber incident in breadth and depth across a state by creating a formal network. The focus then for great

powers is not how to replicated the exact architecture in place in the Mice that Roar, but rather how to achieve similar objectives using existing infrastructure or through the creation of new infrastructure. The question then is not 'should the U.S. build out a cyber-national guard' but rather what gaps currently exist in our defense posture (education, shared networks, visibility into networks outside of government, the ability to leverage that broader visibility in real time). And then, what resources need to mobilized in order to achieve that goal and what institutional constraints (legal for example) need to be addressed to make that process possible. Conscription and reserves may be the mechanism the mice that roar have used, but that does not mean they would be the best mechanism for the U.S. to use when pursuing similar goals.

Ultimately, while cybersecurity concerns are global and many solutions are local, it would be a lost opportunity not to consider which domestic solutions, in some form or another, can travel. Identifying types of domestic approaches and the core drivers and providing a structure through which to compare the American, Estonian, Finnish, Israeli, and Singaporean defense postures to other cases is only the first step in this process. The question for future research, therefore, is to identify which components of these Mice that Roar's successes are dependent upon the broader domestic environment in which they are embedded and which can be adapted to countries that do not match these states in terms of their geostrategic threat environments, technological ecosystems, or relative size.

4.4. What are the Limits of Nationally Bounded Approaches?

While several areas of persisting concern remain for each of the five countries examined in this dissertation, the Mice that Roar face a unique set of national cybersecurity concerns related specifically to their size; most notably, the limitations of internal balancing for national defense purposes and the question of securing the product lifecycle. Importantly, however, these two areas of inquiry are also relevant to great powers' and larger state approaches to national defense in the cyber era.

4.4.1. Collaborative Approaches to National Cyber-Defense

In additional to compete or contest models undertaken by bolstering one's own domestic capability (what neo-realists refer to as internal balancing), states also have at their disposal collaborative defense options such as military and intelligence alliances. While, this dissertation has focused heavily on the internal balancing components of national defense, the dynamics of cooperation[466] remain largely underexamined in the field more broadly yet relevant both for the national security of small and large states alike.

Smaller states, given limited domestic resources, are assumed to need to rely more heavily on these collaborative options for their own national security than great powers. In theory, for a neo-realist, these collaborative approaches can take two forms: in addition to internally balancing, a state can either (i) ally with other similarly positioned states against more powerful states (externally balance)

[466] International Relations theory has identified four broad categories of security cooperation between states. Coalitions are created within the immediate confines of a war or conflict. They do not include additional functions such as deterrence since the conflict has already occurred. Outside of formation during conflict, three categories of cooperation remain: alignment, alliance, and federation. Alignments occur between states with shared interests, but often lack formal written commitments. On the other extreme from alignment lies Federations, which require states to cede control directly to a higher body. They are also far rarer than alignments or alliances, historically. Alliances, in contrast, seek to combine states' capacities in a manner that furthers their own individual interests beyond simple coordination during a conflict. Unlike alignments between states with shared interest, alliances contain formal written commitments. Alliances may be defensive (reactive alliances) and/or offensive in nature (active alliances).

or (ii) ally with a far more powerful state (bandwagon).[467] In practice, these collaborative efforts have taken a myriad of institutional forms and span intelligence and military activity. Notably, cooperation is both costly and beneficial to participating states. As such, new threats can shape countries' preferences for collaboration by altering these costs and benefits.

Historically, alliances have served as a key feature of security cooperation in world politics and have led to important downstream outcomes such as the occurrence of war, conflict escalation, conflict prevention, and conflict cessation.[468] Given that military and intelligence alliances have been a core means through which small states have sought to improve their security[469] (as well as how great powers like the U.S. have projected power abroad),[470] how have they been leveraged by member states in response to the emerging cybersecurity threat environment? How have these institutions and member states' preferences for cooperation evolved? What are the range of opportunities and challenges facing states seeking to integrate cybersecurity into historical intelligence (e.g. Five Eyes[471] and Meximator[472]) military (e.g. the North Atlantic Treaty Organization (NATO)), and broader security (e.g. the European Union (EU)) venues? Are states predominantly leveraging existing institutions or are they creating new venues for cooperation?

When considering the challenges and opportunities for military and intelligence cooperation in cyberspace, it is useful to consider the question at two levels. The first level focuses on the challenges and opportunities for integrating cybersecurity into the current operations or functions of existing alliances or institutions. Here there are operational, tactical, and structural challenges and opportunities for folding cybersecurity into existing architectures. There is another level to consider, however, which resides at the strategic level. Here the relevant question is how can a military or intelligence alliances or cooperation more broadly provide strategic benefits to member states in cyberspace and does that differ from how they provided strategic benefits to member states in the historical domains of air, land, and sea.

4.4.2. Securing the Supply Chain and Product Lifecycle

Given relatively small domestic markets and limited resources, it is not possible for these smaller states to contain the entire security lifecycle of products within their domestic market. This means that domestic industry will continue to specialize and that the market will be augmented by products emanating from abroad. Many of the dominant players in ICT are currently American, and increasingly Chinese. The question for these states then becomes, what aspects of the product

467 Kenneth N. Waltz, *Theory of International Politics*, *McGraw-Hill*, 1979; Robert Keohane, *Neorealism and Its Critics* (Columbia University Press, 1986); and Colin Elman, "Horses for Courses: Why Not Neorealist Theories of Foreign Policy?," *Security Studies* 6, no. 1 (1996): 7–53.

468 Bruce Buemo De Mesquita, *The War Trap* (Yale University Press, 1981); Glenn Harold Snyder, *Alliance Politics*, First Edition (Cornell University Press, 1997); Zeev Maoz, "Alliances: The Street Gangs of World Politics," in *What Do We Know About War?*, ed. J. Vasquez (Rowman and Littlefield, 2000); John J. Mearsheimer, "The Future of the American Pacifier," *Foreign Affairs* 80, no. 5 (2001): 46–61; and Patricia A. Weitsman, *Waging War: Alliances, Coalitions, and Institutions of Interstate Violence*, Kindle Edition (Stanford University Press, 2014).

469 Brett Ashley Leeds, "Alliance Treaty Obligations and Provisions (ATOP) Codebook," 2005. p 4.

470 G. John Ikenberry, *America Unrivaled: The Future of the Balance of Power*, Kindle Edi (Princeton University Press, 2002) and Weitsman, *Waging War: Alliances, Coalitions, and Institutions of Interstate Violence*.

471 Five Eyes, a signals intelligence (SIGINT) alliance that emerged from foundatiosn laid in WWII, fasciliates intelligence collaboration between the U.S., the U.K., Australia, Canada and New Zealand. For more information on the Five Eyes alliance, refer to Scarlet Kim and Pauline Perlin, "Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance," *Lawfare*, March 25, 2019.

472 Maximator was a secret, until very recently, European signals intelligence alliance between Denmark Sweden, Germany, the Netherlands, and France. For more information on Maximator, refer to Bart Jacobs, "Maximator: European Signals Intelligence Cooperation, from a Dutch Perspective," *Intelligence and National Security* 35, no. 5 (July 28, 2020): 659–68.

lifestyle can be sourced from domestic companies? From what is leftover, what needs to be secured from abroad and what portion of those products can already be secured from other partner states or developed cooperatively. Following this question of broader collaborative alternatives, the question for these relatively small states then becomes how to import technology and rely on non-domestic providers of technology in the most secure manner possible. The reliance on global supply chains coupled with the specialization required of small, agile economies remain two economic realities that bring with them deep national security concerns for these countries going forward.

Notably, however, this national security concerns is not unique to relatively small countries, though it is heightened. Take for example, the national security debate surrounding 5G, the fifth generation of telecommunications networks, in the U.S.[473] The U.S., like all other states adopting this technology, is facing a domestic environment defined by critical interdependence on an ecosystem in which large portions of the supply chain may not be dominated by U.S. or allied country industry.[474] Notably, 5G is the very definition of critical infrastructure and a single point of failure. As a consequence, it is also an area where two core policy questions take center stage:

1. How can the U.S. not only increase the underlying security of the 5G ecosystem but also operate securely and reliably on inherently insecure networks?
2. How can the U.S. limit the dominance and influence of a rising geopolitical competitor in domestic and global critical infrastructure?

The latter question has animated much of the public discussion on 5G to date within the U.S. But the former is equally as important, and remains essential to American national security regardless of how successful the U.S. is at the latter. Notably, however, both of these policy imperatives rely on a combination of internal balancing and collaboration, even from a so-called great power like the U.S. For example, the former centers the concern of how to import technology and rely on non-domestic providers of technology in the most secure manner possible while the latter centers efforts to bolster U.S. and allied country industry alternatives to Chinese companies across the 5G ecosystem and supply chain.[475]

4.5. What is the Utility of Resilience as a National Cyber-Defense Strategy

Given the limitations of deterrence and denial-based defense strategies, what lessons can we learn from resilience-based strategies as seen in Finland.

Given ongoing research on and debate over the limitations of deterrence and denial models for national cyber-defense, strategies addressing malicious activity that falls below the level of credible threats of retaliation (deterrence) and yet is too sophisticated to secure against (deny) are growing in importance. Future research should analyze key differences between kinetic concepts of society-wide resilience and the requirements of cyber-resilience given the deeply interconnected nature of cyberspace.

The Finnish case study presented in this dissertation (a country whose kinetic defense posture centered around resilience of critical systems) presents us with several lessons of note. First, despite how it is often talked about in many policy circles, resilience is not a silver bullet. States cannot be resilient against all threats at all times at an achievable cost. This reality is born out in the experience

473 For a detailed examination of U.S. national security concerns related to 5G, refer to Griffith, "5G and Security: There Is More to Worry About than Huawei."

474 While the national security concerns related to 5G are not solely the product of Chinese presence in the market as a peer competitor, it does play a large role in amplifying those concerns.

475 Erik Brattberg and Ben Judah, "Britain's D-10 Summit of Democracies Beats a Moribund G-7," *Foreign Policy*, June 10, 2020.

of states who centered resilience-based national security strategies prior to the emergence of this 5th domain of conflict. States like Finland, but also Norway and Sweden, tailored their resilience-based strategies against specific types of threats. In the case of Finland, an invasion from the east and but later broadened to include concerns over natural disasters, such as winter storms. These strategies were not seeking to address all potential threats to the state but rather a subset of specific national security concerns. As other states seek to adopt this type of defense strategy more broadly, they must begin by asking themselves three core questions: (i) resilience against which types of threats, (ii) under what circumstances, and (iii) at what cost?

Second, resilience-based national defense strategies require an incredibly nuanced understanding of your own terrain: what constitutes critical functions as well as potential single points of failure, upstream and downstream dependencies, and opportunities for cascading effects that could compromise those identified critical functions. It is not enough to identify critical sectors and then distribute best practices to those sectors. This effort must assess what types of functions are critical for national security and which, though deeply important and impactful, are not critical. Resilience does not mean a state never suffers negative security outcomes. It refers to the ability if a state to carry on critical functioning for as long as possible despite disruption and/or destruction. As one Finnish government official clarified, pursuing resilience is about "buying time" so that states are afforded a wider decision space than they might otherwise face.[476]

Moreover, there are also two areas in which cyber-resilience diverges from historical resilience-based national defense strategies born from the domains of air, land, and sea that are worthy of future research efforts. First, what does it mean to have a resilience-based national security strategy when the conflict space is not discrete but instead defined largely by constant contact? Second, how can states structure national approaches to resilience when their critical infrastructure might be not be domestically located and their critical functions are largely dependent on or can be compromised through global networks?

4.6. A Beginning to a Broader Research Agenda

In conclusion, while this project lays an important foundation for thinking about the cyber-defense problem facing states, it also raises a series of subsequent inquiries relevant for both academic and policy audiences. These questions are far too expansive to address in their entirety in this dissertation, but remain important opportunities for future research on the dynamics of national defense in an era of cyber conflict.

5. Final Thoughts and a Note of Caution

The Mice that Roar, notwithstanding the limitations of their size, have set themselves apart as emerging global leaders in cyber-defense capabilities. As states seek to provide security for their populations in the cyber era, they should look to the lessons the Mice that Roar can teach them about the operational realities of national defense when a state is faced with a societal defense problem.

However, and as an important note of caution to keep at the forefront of your minds, despite the relative strengths of their historical defense posture legacies conceptually and operationally, leadership in this space should not be mistaken for excellence. Perhaps Jarno Limnéll, Professor of Cybersecurity at Aalto University and former Director of Cybersecurity at both McAfee and

[476] Author's Interview, 2018

Stonesoft, put it best when he explained that just because Finland appears to being doing well in comparison to other countries "does not mean there isn't a lot more to do. We're the valedictorian in a class full of dummies".[477] The same holds true for all the states examined in this dissertation and leaders in this space more broadly. Even leaders in this space continue to fall victim to malicious cyber or cyber-enabled activity and the challenges of cyber-defense continue to keep policy makers and industry leaders alike up at night. Melissa Hathaway, who led the Comprehensive National Cybersecurity Initiative for President George W. Bush and spearheaded the Cyberspace Policy Review for President Barack Obama, echoed this sentiment, arguing that "no country is cyber ready".[478] Yet, as this domain and our academic understanding and policy/industry approaches evolve, the stakes remain incredibly high. Why? When it comes to national cyber-defense efforts in an era of cyber conflict former U.S. Secretary of Defense General Mattis' dictum holds true: "[w]hen good people meet bad process, bad process wins."[479]

[477] "Finland a 'Valedictorian in a Class of Dummies' in Cyber Security ," *YLE Uutiset*, April 2, 2017.
[478] Melissa Hathaway et al., "Cyber Readiness Index 2.0" (Potomac Institute for Policy Studies, 2015).
[479] At the 10th annual Billington Cyber Security Summit held in Washington D.C. in 2019, U.S. Major General Crall, Deputy Principal Cyber Advisor and Senior Military Advisor for Cyber Policy in the Department of Defense, quoted fellow Marine and former Secretary of Defense General Mattis. The CyberWire, "Transcript: The CyberWire Daily Podcast Ep 922," September 6, 2019, https://thecyberwire.com/podcasts/daily-podcast/922/transcript.

References

(ITU), International Telecommunication Union. "Global Cybersecurity Index," 2017.

"500 Most Innovative Cybersecurity Firms in 2018." Cybersecurity Ventures, 2018. https://cybersecurityventures.com/.

Adamowski, Jaroslaw. "Ukraine Conflict Puts Cyber-Security High on Agenda in Eastern Europe." *SC Magazine UK*, June 1, 2017.

Agency, Congressional Research. "Defense Primer: Department of Defense Contractors Contractors as Individuals," 2020.

Aggarwal, Vinod K., and Andrew W. Reddie. "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 291–305.

———. "Comparative Industrial Policy and Cybersecurity: The US Case." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 445–66.

Ali-Yrkkö, Jyrki, Marrku Lehmus, Petri Rouvinen, and Vesa Vihriälä. *Riding the Wave: Finland in the Changing Tides of Globalization*. Helsinki: Research Institute on the Finnish Economy (ETLA), 2017.

Ali, Idrees. "U.S. Military Puts 'great Power Competition' at Heart of Strategy: Mattis - Reuters." *Reuters*, January 19, 2018.

Amiran, David H. K. "Geographical Aspects of National Planning in Israel: The Management of Limited Resources." *Transactions of the Institute of British Geographers* 3, no. 1 (1978): 115.

Applegate, Scott. "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security and Privacy* 9, no. 5 (September 2011): 16–22.

Aravindan, Aradhana, and John Geddie. "Explainer: Why One Party Dominates Singapore Politics - Reuters." *Reuters*, July 5, 2020.

"ARPA Changes Names." DARPA. Accessed July 20, 2020. https://www.darpa.mil/about-us/timeline/arpa-name-change.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141–65.

Axelrod, Robert. " Beyond the Tragedy of the Commons: A Discussion of Governing the Commons: The Evolution of Institutions for Collective Action ." *Perspectives on Politics* 8, no. 2 (June 2010): 580–82.

Baldwin, David A. "The Concept of Security." *Review of International Studies* 23, no. 1 (1997): 5–26.

Bartlett, Benjamin. "Government as Facilitator: How Japan Is Building Its Cybersecurity Market." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 327–43.

Behar, Richard. "Inside Israel's Secret Startup Machine." *Forbes*, May 11, 2016.

Betts, Richard. *Military Readiness: Concepts, Choices, and Consequences*. Brookings Institution Press, 1995.

Betz, David. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies* 35, no. 5 (October 2012): 689–711.

Biddle, Stephen. *Military Power: Explaining Victory and Defeat in Modern Battle*. Kindle Edition. Princeton University Press, 2010.

Blank, Stephen. "Russian Information Warfare as Domestic Counterinsurgency." *American Foreign Policy Interests*. Taylor & Francis Group , January 2013.

Borghard, Erica D., and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* 26, no. 3 (July 3, 2017): 452–81.

Borghard, Erica, and Shawn Lonergan. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* Fall (2019): 122–45.

Brands, Hal. "One War Is Not Enough: Strategy and Force Planning for Great Power Competition

| American Enterprise Institute - AEI." *Texas National Security Review*, March 1, 2020.
Brant, Tom. "Singapore Tops U.S. for Best Cybersecurity." *Entrepreneur*, July 6, 2017.
Brattberg, Erik, and Ben Judah. "Britain's D-10 Summit of Democracies Beats a Moribund G-7." *Foreign Policy*, June 10, 2020.
Breznitz, Dan. *Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland*. Yale University Press, 2007.
Bryant, Martin. "20 Years Ago Today, the World Wide Web Was Born." The Next Web (TNW) Insider, August 6, 2011. https://thenextweb.com/insider/2011/08/06/20-years-ago-today-the-world-wide-web-opened-to-the-public/.
Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Kindle Edition. Oxford University Press, 2017.
———. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Kindle Edition. Harvard University Press, 2020.
Bujold, Lois McMaster. *CryoBurn (Vorkosigan Saga)*. Kindle Edition. Spectrum Literary Agency, Inc. , 2011.
Burton, Joe. "Small States and Cyber Security: The Case of New Zealand." *Political Science* 65, no. 2 (2013): 216–38.
Bussolati, Nicolò. "The Rise of Non-State Actors in Cyberwarfare." In *Cyber War: Law and Ethics for Virtual Conflicts*, edited by Jens David Ohlin, Kevin Govern, and Claire Finkelstein. Oxford Scholarship Online, 2015.
Carr, Jeffrey. *Inside Cyber Warfare: Mapping The Cyber Underworld*. Second Edi. O'Reilly Media, 2012.
Carr, Madeline. "Public–Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92, no. 1 (2016): 43–62.
Carr, Madeline, and Leonie Maria Tanczer. "UK Cybersecurity Industrial Policy: An Analysis of Drivers, Market Failures and Interventions." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 430–44.
Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*. Routledge, 2007.
Cavelty, Myriam Dunn, and Elgin M. Brunner. "Introduction: Information, Power, and Security—an Outline of Debates and Implications." In *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, edited by Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel. Aldershot: Ashgate, 2007.
Cavelty, Myriam Dunn, and Manuel Suter. "Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179–87.
CCD COE. "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Cyber Defence Hub." Accessed July 27, 2020. https://ccdcoe.org/.
Cheung, Tai Ming. "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 306–26.
Chieh, Lim Wei. "Policy Analysis: Singapore's Public-Private Partnerships for Cybersecurity in the Critical Infrastructure Sectors — Challenges and Opportunities." Lee Kuan Yew School of Public Policy (LKY School), National University of Singapore, 2017.
Choucri, Nazli. *Cyberpolitics in International Relations*. MIT Press, 2012.
Clark, David, Thomas Berson, and Herbert S. Lin. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. National Academies Press, 2014.
Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. Reprint Edition. HarperCollins e-books, 2010.

Cohen, Natasha, and Peter Warren Singer. "The Need for C3: A Proposal for a United States Cybersecurity Civilian Corps." *New America Report*, October 25, 2018.
Cohen, Raymond. "Threat Perception in International Crisis." *Political Science Quarterly* 93, no. 1 (1978): 93.
Cooper, Benjamin. "Changes in Estonian Defense Policy Following Episodes of Russian Aggression." *Inquiries* 10, no. 10 (2018).
Cooper, Jeffrey. "A New Framework for Cyber Deterrence." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek. S. Reveron, 105–120. Georgetown University Press, 2012.
"Cyber Conflict Studies Association (CCSA)." Accessed July 27, 2020. http://www.cyberconflict.org/.
"Cyber Security Agency of Singapore." Accessed July 26, 2020. https://www.csa.gov.sg/.
Cyber Security Agency of Singapore (CSA). "CSA Leads Whole-of-Government Exercise to Respond to Cyber Attacks." Press Release, July 18, 2017. https://www.csa.gov.sg/news/press-releases/csa-leads-wog-exercise-to-respond-to-cyber-attacks.
"Cyber Vault." National Security Archive, https://nsarchive.gwu.edu/project/cyber-vault-project.
"Cybersecurity Market Report." Cybersecurity Ventures, 2016. https://cybersecurityventures.com/cybersecurity-market-report-test/.
D'Elia, Danilo. "Industrial Policy: The Holy Grail of French Cybersecurity Strategy?" *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 385–406.
Darknet Diaries. "Unit 8200." Podcast Episode Transcript, December 15, 2018. https://darknetdiaries.com/transcript/28/.
Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *WIRED*, August 21, 2007.
Davis, Norman C. "An Information-Based Revolution in Military Affairs." *Strategic Review* 24, no. 1 (1996): 43–53.
Defence, Republic of Estonia Ministry of. "Cyber Security Strategy," 2008.
Defense, Singaporean Ministry of. "MINDEF Singapore." Accessed July 20, 2020. https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/total-defence.
Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. University of Georgia Press, 2011.
DeNardis, Laura. *The Global War for Internet Governance*. Yale University Press, 2014.
Deppisch, Breanne. "DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump." *Politico*, December 18, 2019.
Dicter, Avi, and Daniel L Byman. "Israel's Lessons for Fighting Terrorists and Their Implications for the United States," March 2006.
Dipert, Randall R. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9, no. 4 (December 2010): 384–410.
Doz, Yvos, and Keeley Wilson. *Ringtone: Exploring the Rise and Fall of Nokia in Mobile Phones*. Oxford: Oxford University Press, 2018.
Dyson, Tom. "Convergence and Divergence in Post-Cold War British, French, and German Military Reforms: Between International Structure and Executive Autonomy." *Security Studies* 17, no. 4 (2008): 725–74.
"East Asia/Southeast Asia :: Singapore." Accessed July 26, 2020. https://www.cia.gov/library/publications/the-world-factbook/geos/sn.html.
Ebert, Hannes, and Tim Maurer. "Contested Cyberspace and Rising Powers." *Third World Quarterly*

34, no. 6 (July 2013): 1054–74.
Elman, Colin. "Horses for Courses: Why Not Neorealist Theories of Foreign Policy?" *Security Studies* 6, no. 1 (1996): 7–53.
Elman, Colin, and Miriam Fendius Elman, eds. *Bridges and Boundaries: Historians, Political Scientists, and the Study of International Relations*. MIT Press, 2001.
Engel, Jerome S., and Itxaso del-Palacio. "Global Clusters of Innovation: The Case of Israel and Silicon Valley." *California Management Review* 53, no. 2 (2011): 27–49.
Erskine, Toni, and Madeline Carr. "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace." In *International Cyber Norms: Legal, Policy & Industry Perspectives*. NATO Cooperative Cyber Defence Centre of Excellence, 2016.
"Europe :: Estonia — The World Factbook - Central Intelligence Agency." Accessed July 15, 2020. https://www.cia.gov/library/publications/the-world-factbook/geos/en.html.
European Commision. "Commission Launches a Call for Proposals for a €50 Million Pilot to Support the Creation of a Network of Cybersecurity Competence Centres across the EU," 2018. https://ec.europa.eu/programmes/horizon2020/en/news/%0Dcommission-launches-call-proposals-€50-million-pilot-support-creation-networkcybersecurity.
European Commission. "Galileo," 2018 https://ec.europa.eu/growth/sectors/space/galileo_en.
European Union Agency for Cybersecurity (ENISA). "National Cyber Security Strategies - Interactive Map." Accessed July 24, 2020. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
F.C. "Hacking in Singapore - Messiah Complicated | Banyan." *The Economist*, December 7, 2013.
Farrell, Harry. "Promoting Norms for Cyberspace," Council on Foreign Relations (CFR). 2015.
Farrell, Henry, and Charles L Glaser. "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine." *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 7–17.
Fielder, James D. "Bandwidth Cascades: Escalation and Pathogen Models for Cyber Conflict Diffusion." *Small Wars Journal* 9, no. 3 (2013).
"Finland's Cyber Security Strategy," 2013.
"Finland a 'Valedictorian in a Class of Dummies' in Cyber Security ." *YLE Uutiset*, April 2, 2017.
Finnemore, Martha. "Cultivating International Cyber Norms." In *America's Cyber Future: Security and Prosperity in the Information Age*, edited by Kristin M. Lord and Travis Sharp. The Center for a New American Security (CNAS), 2011.
Finnish Defense Forces. "Finnish Conscription System - Puolustusvoimat The Finnish Defence Forces." Accessed July 20, 2020. https://puolustusvoimat.fi/en/finnish-conscription-system.
Finnish Information Security Cluster (FISC). "Mission," 2018. https://www.fisc.fi/.
Fischerkeller, Michael P., and Richard J. Harknett. "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation," Institute of Defense Analyses. 2018.
———. "What Is Agreed Competition in Cyberspace?" *Lawfare*, February 19, 2019.
Forces, Finnish Defense. "NATO's Partnership for Peace Programme - Puolustusvoimat The Finnish Defence Forces." Accessed July 20, 2020. https://puolustusvoimat.fi/en/international-activities/natos-partnership-for-peace-programme.
Forsell, Tuomas, and Jussi Rosendahl. "Finland Government Strikes Deal with Unions to Boost Stagnant Economy." *Reuters*, 2016.
Forsyth, James W. "What Great Powers Make of It: International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly* 7, no. 1 (2013).
Freedman, Lawrence. *Strategy: A History*. Kindle Edition. Oxford University Press, 2013.
Friedler, Eran. "Water Reuse - An Integral Part of Water Resources Management: Israel as a Case Study." *Water Policy* 3, no. 1 (January 1, 2001): 29–39.

Ganesan, Narayanan. *Realism and Interdependence in Singapore's Foreign Policy*. *Realism and Interdependence in Singapore's Foreign Policy*. Routledge Taylor & Francis Group, 2005.
Garcia, Ahiza. "Who's Winning the 5G Race?" *CNN*, April 2, 2019.
Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth." *International Security* 38, no. 2 (2013): 41–73.
Gartzke, Erik, and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2 (April 3, 2015): 316–48.
Gartzke, Erik, and Jon R Lindsay. "Thermonuclear Cyberwar." *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 37–48.
Geers, Kenneth. "Cyber Weapons Convention." *Computer Law and Security Review* 26, no. 5 (September 1, 2010): 547–51.
Gerring, John. *Case Study Research: Principles and Practices*. Second Edition. Kindle Edition. Cambridge University Press, 2006.
"Global Firepower - 2020 World Military Strength Rankings." Accessed July 18, 2020. https://www.globalfirepower.com/.
Golden, Chris. "Creating New Private-Public Partnerships in Cybersecurity." *National Cybersecurity Institute Journal* 2, no. 3 (2015).
Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (September 22, 2010): 102–36.
———. "Cyber Deterrence: Tougher in Theory than in Practice?" *U.S. Senate Washington, DC Committee on Armed Services* 4, no. 3 (2010).
Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Kindle Edition. Doubleday, 2019.
———. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018.
Griffith, Melissa K. "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 407–29.
———. "Is the Strategic Corporal on Your Twitter Feed?" *Net Politics and Digital and Cyberspace Policy Program from the Council on Foreign Relations*, July 12, 2017.
———. "Why Cyber Conflict as an Academic Discipline Struggles to Make Its Mark in Political Science." *Council for Foreign Relations' Net Politics and Digital and Cyberspace Policy Program*, September 6, 2018.
Griffith, Melissa K., and Adam Segal. "International Security and the Strategic Dynamics of Cyber Conflict," Columbia University SIPA and the Cyber Conflict Studies Association (CCSA). 2018.
Griffith, Melissa K. "5G and Security : There Is More to Worry About than Huawei." *Wilson Center Policy Brief*, 2019.
Guitton, Clement. "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?" *European Security* 22, no. 1 (March 2013): 21–35.
Gvosdev, Nikolas K. "The Bear Goes Digital: Russia and Its Cyber Capabilities." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek Reveron. Georgetown University Press, 2012.
Hall, Peter A. "Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain." *Comparative Politics* 25, no. 3 (April 1993): 275.
Hall, Peter A., and Rosemary C. R. Taylor. "Political Science and the Three New Institutionalisms." *Political Studies* 44, no. 5 (December 1, 1996): 936–57.
Hammersley, Ben. "Become an E-Resident of Estonia." WIRED UK, March 27, 2017.

Harel, Amos. "Israel's Walls." *Foreign Affairs*, February 17, 2017.
Harknett, Richard. "Information Warfare and Deterrence." *Parameters*, 1996, 93–107.
Hathaway, Melissa. "Cyber Readiness Index 1.0," Report Presentation at the Belfer Center. Hathaway Global Strategies. 2013.
Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer F McArdle, and Rancesca Spidalieri. "Cyber Readiness Index 2.0." Potomac Institute for Policy Studies, 2015.
Hathaway, Melissa E. "Toward a Closer Digital Alliance." *SAIS Review of International Affairs* 30, no. 2 (2010).
Healey, Jason. *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. Kindle Edition. Cyber Conflict Studies Association (CCSA), 2013.
———. "Beyond Attribution: Seeking National Responsibility in Cyberspace," Atlantic Council. 2016.
———. "The Spectrum of National Responsibility for Cyberattacks." *Brown Journal of World Affairs* 18, no. 1 (2011): 57–69.
Healey, Jason, and Leendert van Bochoven. "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Issue Brief for The Atlantic Council. 2011.
Heath, Nick. "How Estonia Became an E-Government Powerhouse." *TechRepublic*, February 19, 2019.
Heckman, Jory. "CISA Focuses on Building Agency Trust in Data as Part of Upcoming CDM Dashboard | Federal News Network." *Federal News Network*, June 9, 2020.
Henry, Basil, and Liddell Hart. *The Defence of Britain*. Praeger, 1980.
Hermunen, Tommi. "Finnish Defence Forces Starts Engaging Conscripts in Cyber Defense." English Translation of Hermunen's Original Article in Finnish, 2015.
Hio, Lester. "S'pore Takes Top Spot in UN Cyber Security Index." *Straits Times*, July 7, 2017.
Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (June 2011): 1–24.
Hodgson, Quentin E., Logan Ma, Krystyna Marcinek, and Karen Schwindt. "Fighting Shadows in the Dark Understanding and Countering Coercion in Cyberspace," 2019.
House, U.S. White. "National Cyber Strategy of the United States of America," 2018.
"How Estonia Became a Global Heavyweight in Cyber Security." E-Estonia. Accessed June 27, 2020. https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.
Huang, Hsini, and Tien-Shen Li. "A Centralised Cybersecurity Strategy for Taiwan." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 344–62.
Hurwitz, Roger. "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly* 6, no. 3 (September 22, 2012): 20–46.
———. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 322–31.
Iasiello, Emilio. "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2014): 54–67.
Ikenberry, G. John. *America Unrivaled: The Future of the Balance of Power*. Kindle Edition. Princeton University Press, 2002.
———. "The Irony of State Strength: Comparative Responses to the Oil Shocks in the 1970s." *International Organization* 40, no. 1 (1986): 105–37.
Inboden, Will. "Is Finland Rejecting 'Finlandization'?"." *Foreign Policy*, December 1, 2014.
Inkster, Nigel. "China in Cyberspace." *Survival* 52, no. 4 (September 21, 2010): 55–66.
International Telecommunication Union (ITU). "Global Cybersecurity Index," 2018.
———. "Index of Cybersecurity Indices," 2017.
Ioanes, Ellen. "The US Military Is Buying Israel's Battle-Proven Iron Dome That Destroys Rockets.

Here's How It Works." *Business Insider*, August 15, 2019.
"Israel: Military Draft Law and Enforcement." Library of Congress - LAW. Accessed July 26, 2020. https://www.loc.gov/law/help/military-draft/israel.php.
Israeli Defense Forces (IDF) - Mahal. "IDF Background Information." Accessed July 26, 2020. https://www.mahal-idf-volunteers.org/information/background/content.htm#reserve.
Israeli Ministry of Foreign Affairs. "Israel's Wars." Accessed July 24, 2020. https://mfa.gov.il/MFA/AboutIsrael/History/Pages/Israel-Wars.aspx.
Jacobs, Bart. "Maximator: European Signals Intelligence Cooperation, from a Dutch Perspective." *Intelligence and National Security* 35, no. 5 (July 28, 2020): 659–68.
Jakobsen, Peter Viggo. "Small States, Big Influence: The Overlooked Nordic Influence on the Civilian ESDP*." *JCMS: Journal of Common Market Studies* 47, no. 1 (January 1, 2009): 81–102.
Jensen, Benjamin M., Brandon Valeriano, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press, 2018.
Jermalavičius, Tomas, Piret Pernik, Martin Hurt, Henrik Breitenbauch, and Pauli Järvenpää. "Comprehensive Security and Integrated Defence: Challenges of Implementing Whole-of-Government and Whole-of-Society Approaches," RKK ICDS. 2014.
Jervis, Robert. "The Dustbin of History: Mutual Assured Destruction." *Foreign Policy*, November 9, 2009.
Jha, Abhas. "'But What about Singapore?' Lessons from the Best Public Housing Program in the World." World Bank Blog, January 31, 2018.
Joenniem, Pertti. "Neutrality beyond the Cold War." *Review of International Studies* 19, no. 3 (1993):
Junio, Timothy. *A Theory of Information Warfare*. University of Pennsylvania dissertation, 2013.
Kapusta, Philip. "The Gray Zone," Special Warfare. 2015.
Katzenstein, Peter J. "Same War - Different Views: Germany, Japan, and Counterterrorism." *International Organization*. Cambridge University Press, 2003.
Kauppinen, Tero. "Cybersecurity of Supply." National Emergency Supply Agency presentation at the FIIF JAM SESSION., 2015.
Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (October 28, 2013): 7–40.
———. "The Security Dilemma of Cyberspace: Ancient Logic, New Problems - Lawfare." *Lawfare*, August 28, 2017.
———. *The Virtual Weapon and International Order*. Kindle Edition. Yale University Press, 2017.
Keohane, Robert. *Neorealism and Its Critics*. Columbia University Press, 1986.
Khoo, Louisa-May. "Living with Diversity the Singapore Way Inclusion through Intervention." *Urban Solutions*, no. 10 (January 2017).
Kim, Scarlet, and Pauline Perlin. "Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance." *Lawfare*, March 25, 2019.
Kissinger, Henry. *World Order: Reflections on the Character of Nations and the Course of History*. Kindle Edition. Penguin, 2014.
Klimburg, Alexander. "Mobilizing Cyber Power." *Survival* 53, no. 1 (2011): 41–60.
Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. National Defense University Press and Potomac Books, 2010.
Krasner, Steven D. "Approaches to the State: Alternative Conceptions and Historical Dynamics." *Comparative Politics*, no. 16 (1984): 223–246.
Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*. National Defense University Press, 2009.
Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security.*, edited by Franklin Kramer, Stuart H. Starr, and Larry K. Wentz, First Edition., 309–342. Potomac

Books, 2009.
Kuper, Stephen. "Taking a Closer Look at Singapore's 'Poison Shrimp' Defence Doctrine." *Defence Connect*, February 11, 2020.
Lanchester, F.W. *Aircraft in Warfare: The Dawn of the Fourth Arm*. Kindle Edition, 2011.
Laslo, Matt. "Russia Is Going to Up Its Game for the 2020 Elections." *Wired*, July 31, 2019.
Lawson, Sean. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology and Politics* 10, no. 1 (January 2013): 86–103.
Leeds, Brett Ashley. "Alliance Treaty Obligations and Provisions (ATOP) Codebook," 2005.
Lehto, Martti, Limnéll Jarno, Eeva Innola, Jouni Pöyhönen, Arja Rusi, and Mirva Salminen. "Finland's Cyber Security: The Present State, Vision and the Actions Needed to Achieve the Vision." For the Prime Minister's Office, 2017.
Lehto, Martti, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhöne, and Mirva Salminen. "Strategic Management of Cyber Security in Finland," For the Prime Minister's Office. 2018.
Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "Brief History of the Internet | Internet Society." The Internet Society, 1997. https://www.internetsociety.org/internet/history-internet/brief-history-internet/.
Lemos, Robert. "Bush Unveils Final Cybersecurity Plan." *CNET*, November 13, 2003.
Libicki, Martin. "Would Deterrence in Cyberspace Work Even with Attribution?" *Georgetown Journal of International Affairs*, 2016.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007.
———. "Cyberdeterrence and Cyberwar," RAND, 2010.
Lieber, Keir. "The Offense-Defense Balance and Cyber Warfare." In *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla. Naval Postgraduate School, 2013.
Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (June 2012): 401–28.
Lim, Linda Y C. *Singapore's Economic Development: Retrospection And Reflections (World Scientific Series On Singapore's 50 Years Of Nation-Building)* . Kindle Edition. World Scientific, 2015.
Lin, Herbert. "Arms Control in Cyberspace: Challenges and Opportunities." *World Politics Review* March (2012).
———. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (September 22, 2012): 46–71.
Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (July 2013): 365–
———. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39, no. 3 (January 27, 2015): 7–47.
Lindsay, Jon R., and Lucas Kello. "Correspondence: A Cyber Disagreement." *International Security* 39, no. 2 (2014): 181–192.
Lindsay, Jon R. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack." *Journal of Cybersecurity* 1, no. 1 (September 1, 2015): 53–67.
Lindsay, Jon R, and Tai Ming Cheun. "From Exploitation to Innovation: Acquisition, Absorption, and Application." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek Reveron. Oxford University Press, 2015.
Lindsay, Jon Randall. "Restrained by Design: The Political Economy of Cybersecurity." *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 493–514.
Lis, Jonathan, and Yaniv Kubovich. "Defense Ministry: Israel Has Destroyed 45 Homes of

Terrorists' Families in Last 3 Years." *Haaretz*, January 11, 2018.
Lupovici, Amir. "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives* 17, no. 3 (August 1, 2014).
Lyngaas, Sean. "Lawmakers Introduce Bill to Save Top White House Cyber Job after Bolton Eliminated It." *Cyber Scoop*, May 15, 2018.
Makridis, Christos Andreas, and Max Smeets. "Determinants of Cyber Readiness." *Journal of Cyber Policy* 4, no. 1 (January 2, 2019): 72–89.
Maoz, Zeev. "Alliances: The Street Gangs of World Politics." In *What Do We Know About War?*, edited by J. Vasquez. Rowman and Littlefield, 2000.
Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2017.
Mearsheimer, John J. "Assessing the Conventional Balance: The 3:1 Rule and Its Critics." *International Security* 13, no. 4 (1989): 54–89.
———. "The Future of the American Pacifier." *Foreign Affairs* 80, no. 5 (2001): 46–61.
Mesquita, Bruce Buemo De. *The War Trap*. Yale University Press, 1981.
Miler, Tom. "U.N. Survey Finds Cybersecurity Gaps Everywhere except Singapore." *Reuters*, July 5, 2017.
Miller Jr., James N., and Richard Fontaine. "A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict," Center for a New American Security (CNAS), 2017.
Ministry of Foreign Affairs Singapore. "National Service Obligation." Accessed July 26, 2020. https://www.mfa.gov.sg/Overseas-Mission/Chennai/Consular-Services/National-Service-Obligation.
Mitchell, Charlie. *Hacked: The Inside Story of America's Struggle to Secure Cyberspace . Rowman & Littlefield Publishers*. Kindle Edition., 2016.
Mittelman, Sharyn. "Israel and Singapore – out of the Shadows." *The Jerusalem Post*, June 6, 2016.
National Cyber Directorate. "Israel National Cyber Security Strategy in Brief." *State of Israel's Prime Minister's Office*, September 2017.
"National Security Concept of the Republic of Estonia ," 2004.
Nenye, Vesa, Peter Munter, Toni Wirtanen, and Chris Birks. *Finland at War: The Continuation and Lapland Wars 1941–45*. Kindle Edition. Osprey Publishing, 2016.
Ng, Pak Shun. "From 'Poisonous Shrimp' to 'Porcupine': An Analysis of Singapore's Defence Posture Change in the Early 1980s," Strategic & Defence Studies Centre. 2005.
Notes, EPSC Strategic. "No TitleBuilding an Effective European Cyber Shield: Taking EU Cooperation to the Next Level." *European Political Strategy Centre*, no. 24 (2017).
Nye, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, 2011.
Nye Jr, Joseph S. "Cyber Power," 2010.
———. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (n.d.): 44–71.
———. *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone*. Kindle Edition. Oxford University Press, 2003.
O'Hanion, Michael E. "Beware the RMA'nia!"".". *Brookings Report*, September 9, 1998.
Office of Management and Budget. "21. Cyber Security Funding." In *An American Budget: Analytical Perspectives*, 273–287. U.S. Government Publishing Office, 2017.
Ohio National Guard Adjutant General's Department. "Ohio Cyber Reserve." Accessed July 28, 2020. https://www.ong.ohio.gov/special-units/cyber/ohcr/index.html.
Ohio National Guard Public Affairs. "Ohio Gov. Mike DeWine Signs Cyber Reserve Legislation." *Ohio National Guard/ Adjutant General's Department* , October 25, 2019.
Osula, Anna-Maria, and Henry Rõigas, eds. *International Cyber Norms: Legal, Policy & Industry Perspectives*. NATO Cooperative Cyber Defence Centre of Excellence, 2016.

Peck, Michael. "How Finland Lost World War II to the Soviets, But Won Peace." *National Interest*, August 19, 2016.
Pellerin, Cheryl. "DOD Releases First Strategy for Operating in Cyberspace." *American Forces Press Service*, July 14, 2011.
Perkovich, George, and Ariel E. Levite, eds. *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press, 2017.
Perlroth, Nicole, and David E. Sanger. "White House Eliminates Cybersecurity Coordinator Role." *New York Times*, May 15, 2018.
Pernik, Piret. "Estonian Cyber Command: What Is It For? ." RKK ICDS Blog, November 26, 2018.
———. "Report Preparing for Cyber Conflict Case Studies of Cyber Command," RKK ICDS. December 2018.
Pernik, Piret, Jesse Wojtkowiak, and Alexander Verschoor-Kirss. "National Cyber Security Organisation: United States." CCD COE, Tallinn, 2016.
Peters, B. Guy. *Institutional Theory in Political Science*. London: Continuum, 2001.
Pierson, Paul. "Increasing Returns, Path Dependence, and the Study of Politics." *American Political Science Review* 94, no. 2 (June 2000): 251–67.
———. "The Limits of Design: Explaining Institutional Origins and Change." *Governance* 13, no. 4 (October 1, 2000): 475–99.
———. "When Effect Becomes Cause: Policy Feedback and Political Change." *World Politics* 45, no. 4 (July 1993): 595–628.
Polkinghonre, Donald. *Methodology for the Human Sciences*. State University of New York Press, 1983.
Press, Gil. "How Startup Nation's Innovation Catalyst Masters The Art Of Public-Private Partnership." *Forbes*, July 20, 2015.
———. "Israeli Startups Shine In The $92 Billion Cybersecurity Market." *Forbes*, February 26, 2019.
Pritzker, Penny. "U.S. Secretary of Commerce Penny Pritzker Details Cybersecurity Challenges Faced by Cabinet Secretaries in Speech to Commission on Enhancing National Cybersecurity." U.S. Department of Commerce.
Renaud, Michael T., Marguerite McConihe, and Derek E. Constantine. "Will Israel Become a Leader in AI Protections?" *The National Law Review*, June 10, 2019.
Republic of Estonia Defence Forces. "History – Estonian Defence Forces." Accessed July 27, 2020. https://mil.ee/en/defence-forces/history-of-the-defence-forces/.
Republic of Estonia Government Office. "The Coordination of National Security and Defence Management | Government Office of Estonia." Accessed July 27, 2020. https://www.riigikantselei.ee/en/supporting-government/coordination-national-security-and-defence-management.
Republic of Estonia Information System Authority. "CERT-EE." Accessed July 27, 2020. https://www.ria.ee/en/cyber-security/cert-ee.html.
———. "Crisis Management." Accessed July 27, 2020. https://www.ria.ee/en/cyber-security/crisis-management.html.
———. "Critical Information Infrastructure Protection CIIP." Accessed July 27, 2020. https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html.
———. "Introduction and Structure." Accessed July 27, 2020. https://www.ria.ee/en/information-system-authority/introduction-and-structure.html.
———. "Supervision." Accessed July 27, 2020. https://www.ria.ee/en/cyber-security/supervision.html.
Republic of Estonia Ministry of Defence. "National Security Concept," 2017.
Republic of Estonia Ministry of Economic Affairs and Communication. "Cyber Security Strategy

2014-2017," 2014.
Republic of Estonia Ministry of Economic Affairs and Communications. "Cybersecurity Strategy 2019-2022," 2019.
Republic of Estonia Riigi Teataja. "Cybersecurity Act," 2018.
Reuters Staff. "Finnish Government Calls for Urgent Approval of Intelligence Bill." *Reuters*, January 25, 2018.
Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.
Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (January 2, 2015): 4–37.
Riley, Walters. "Russian Hackers Shut Down Ukraine's Power Grid." *Newsweek*, January 14, 2016.
Rovner, Joshua, and Tyler Moore. "Does the Internet Need a Hegemon?" *Journal of Global Security Studies* 2, no. 3 (July 1, 2017): 184–203.
Roy, Kaushik. *Sepoys Against the Rising Sun: The Indian Army in Far East and South-East Asia, 1941-45 (History of Warfare)*. Lam Edition. Brill Academic Pub, 2016.
Saltzman, Ilai. "Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy* 34, no. 1 (2013): 40–63.
Sanchez, Ray. "Israel and Its Neighbors: Decades of War." *CNN*, August 13, 2014.
Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013.
Schmitt, Michael N., and Liis Vihul. "Proxy Wars in Cyberspace: The Evolving International Law of Attribution." *Fletcher Security Review* 1, no. 2 (2014): 54–73.
Schneider, Jacquelyn G. "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy - Lawfare." *Lawfare*, May 10, 2019.
Security and Defense Agenda. "Cyber-Security: The Vexed Question of Global Rules," 2012.
"Security Strategy for Society" English Translation, (2017).
Segal, Adam. *Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Public Affairs, Kindle Edition, 2016.
———. "The Code Not Taken: China, the United States, and the Future of Cyber Espionage." *Bulletin of the Atomic Scientists* 69, no. 5 (September 27, 2013): 38–45.
———. "The Rise of Asia's Cyber Militias," The Atlantic. 2012.
Senor, Dan, and Saul Singer. *Start-up Nation: The Story of Israel's Economic Miracle*. Kindle Edition. Twelve, 2011.
Sharkansky, Ira. *The Political Economy of Israe*. First Edition. Routledge, 2017.
Sharp, Travis. "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony." *Journal of Strategic Studies* 40, no. 7 (November 10, 2017): 898–926.
Sheldon, John B. "Geopolitics and Cyber Power: Why Geography Still Matters." *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 286–93.
———. "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.*, edited by Derek Reveron. Georgetown University Press, 2012.
Singapore Civil Defence Force. "Total Defence | SCDF." Accessed July 26, 2020. https://www.scdf.gov.sg/home/community-volunteers/community-preparedness/total-defence.
"Singapore Opposition Make 'landmark' Election Gains - BBC News." *BBC*, May 9, 2011.
Singer, Peter W., and Allan Friedman. *Cybersecurity: What Everyone Needs to Know. Oxford University Press.* Kindle Edition, 2014.
Smeets, Max. "A Matter of Time: On the Transitory Nature of Cyberweapons." *Journal of Strategic Studies* 41, no. 1–2 (February 23, 2018): 6–32.

———. "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment." *Defence Studies* 18, no. 4 (October 2, 2018): 395–410.
Snyder, Glenn Harold. *Alliance Politics*. First Edition. Cornell University Press, 1997.
Standish, Reid. "How Finland Became Europe's Bear Whisperer." *Foreign Policy*, March 7, 2016.
Sterling, Bruce. "Estonian Cyber Security." *WIRED*, January 9, 2018.
Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (April 2012): 148–70.
Stiglitz, Joseph E., and Scott J. Wallsten. "Public-Private Technology Partnerships." *American Behavioral Scientist* 43, no. 1 (September 27, 1999): 52–73.
"Strategic Doctrine - Israel." Federation of American Scientists, 2000.
Subramanian, Arvind. "Preserving the Open Global Economic System: A Strategic Blueprint for China and the United States," Peterson Institute for International Economics. Policy Brief 13-16. 2013.
Sucio, Peter. "Why Israel Dominates in Cyber Security." *Fortune*, September 1, 2015.
Tabansky, Lior, and Isaac Ben-Israel. *Cybersecurity in Israel (SpringerBriefs in Cybersecurity)*. Kindle Edition. Springer, 2015.
———. "The National Innovation Ecosystem of Israel." In *The National Innovation Ecosystem of Israel. In: Cybersecurity in Israel. SpringerBriefs in Cybersecurity*, 15–30. Springer, Cham, 2015.
Taliaferro, Jeffrey W. "State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State." *Security Studies* 15, no. 3 (July 2006): 464–95.
Tapon, Francis. "The Bronze Soldier Explains Why Estonia Prepares For A Russian Cyberattack." *Forbes*, July 7, 2018.
Tarnoff, Ben. "How the Internet Was Invented | Internet." *The Guardian*, July 15, 2016.
Taylor, Guy. "James Clapper, Intel Chief: Cyber Ranks Highest on Worldwide Threats to U.S." *The Washington Times*, February 26, 2015.
"Text: Obama's Remarks on Cyber-Security." *New York Times*, May 29, 2009.
"The Comprehensive National Cybersecurity Initiative." The Obama White House Archives, 2008. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.
The Cyber Security Agency of Singapore (CSA). "Singapore's Cybersecurity Strategy," 2016.
The CyberWire. "Transcript: The CyberWire Daily Podcast Ep 922," September 6, 2019. https://thecyberwire.com/podcasts/daily-podcast/922/transcript.
"THE LAND: Geography and Climate." Israel Ministry of Foreign Affairs. Accessed July 18, 2020. https://mfa.gov.il/mfa/aboutisrael/land/pages/the land- geography and climate.aspx.
The National Defence University (NDU). "National Defence Courses," 2018. http://maanpuolustuskorkeakoulu.fi/en/national-defence-courses.
The National Emergency Supply Agency (NESA). "Security of Supply in Finland," 2018. https://www.nesa.fi/security-of-supply/.
Thelen, Kathleen. "HISTORICAL INSTITUTIONALISM IN COMPARATIVE POLITICS." *Annual Review of Political Science* 2, no. 1 (June 1999): 369–404.
Tikk, Eneken. "Global Cybersecurity–Thinking About the Niche for NATO." *SAIS Review of International Affairs* 30, no. 2 (2010).
———. "Ten Rules for Cyber Security." *Survival* 53, no. 3 (June 2011): 119–32.
Timmers, Paul. "The European Union's Cybersecurity Industrial Policy." *Journal of Cyber Policy* 3, no. 3 (September 2, 2018): 363–84.
Tkacik, John. "Trojan Dragon: China's Cyber Threat," Heritage Foundation. 2008.
Tomba, Mattia. *Beating the Odds Together. Beating the Odds Together: 50 Years of Singapore–Israel Ties*. World Scientific, 2019.
Trajtenberg, Manuel. "R&D Policy in Israel." In *Economics of Science, Technology and Innovation Book*

Series (ESTI, Volume 23), edited by M. P. Feldman et al., 409–54. Springer, Boston, MA, 2001.
Trejos, Amanda. "Why Getting Rid of Costa Rica's Army 70 Years Ago Has Been Such a Success." *USA Today*, 2018.
Tropina, Tatiana, and Callanan Cormac. *Self- and Co-Regulation in Cybercrime, Cybersecurity and National Securit*. SpringerBriefs in Cybersecurity, 2015.
Trujillo, Clorinda. "The Limits of Cyberspace Deterrence." *Joint Force Quarterly*, no. 75 (2014).
Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution." *Journal of Conflict and Security Law* 17, no. 2 (July 1, 2012): 229–44.
U.S. Department of Defense. "Cyber Scholarship Program (CySP) ." Accessed July 28, 2020. https://public.cyber.mil/cysp/.
———. "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," 2018.
———. "The National Military Strategy of the United States of America," 2015.
"U.S. National Defense Strategy | Wilson Center." Woodrow Wilson Center, 2018. https://www.wilsoncenter.org/article/us-national-defense-strategy?gclid=CjwKCAjwltH3BRB6EiwAhj0IUPANMronOUeCHyVki1f1M8VAmOrroUO4Q498nFyhamCOHYMGyGmsuBoCEHwQAvD_BwE.
U.S. National Institute of Standards and Technology (NIST). "National Initiative for Cybersecurity Education (NICE)." Accessed July 28, 2020. https://www.nist.gov/itl/applied-cybersecurity/nice.
U.S. White House. "The National Strategy to Secure Cyberspace," 2003.
Valeriano, Brandon, and Ryan C Maness. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11." *Journal of Peace Research* 51, no. 3 (May 1, 2014): 347–60.
Veebel, Viljar, and Illimar Ploom. "Estonia's Comprehensive Approach to National Defence: Origins and Dilemmas." *Journal on Baltic Security* 4, no. 2 (February 7, 2019): 10–22.
Vogel, Steven K. *Marketcraft: How Governments Make Markets Work*. Kindle Edition. Oxford: Oxford University Press, 2018.
VTT Technical Research Centre of Finland. "Security Testing and Analysis," 2018. http://www.vttresearch.com/services/digital-society/data-driven-solutions/cyber-andinformation-%0Dsecurity/security-testing-and-analysis.
———. "Services: Cybersecurity," 2018. http://www.vttresearch.com/.
———. "What Is VTT." Accessed July 20, 2020. https://www.vttresearch.com/en/about-us/what-vtt.
Walt, Stephen M. *The Origins of Alliances*. Kindle Edition. Cornell University Press, 2013.
Waltz, Kenneth N. *Theory of International Politics*. McGraw-Hill, 1979.
Website Builder Expert. "Which EU Country Is Most Vulnerable To Cybercrime?"," 2017. https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.
Weir, Margaret, and Theda Skocpol. "State Structures and the Possibilities for 'Keynesian' Responses to the Great Depression in Sweden, Britain, and the United States." In *Bringing the State Back In*, edited by Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol. Cambridge University Press, 1985.
Weitsman, Patricia A. *Waging War: Alliances, Coalitions, and Institutions of Interstate Violence*. Kindle Edition. Stanford University Press, 2014.
Westerman, Ashley. "'Fake News' Law Goes Into Effect In Singapore, Worrying Free Speech Advocates : NPR." *NPR*, October 2, 2019.
Wu, Xu. *Chinese Cyber Nationalism: Evolution, Characteristics, and Implications*. Lexington Books, 2007.
Yaakov, Katz, and Amir Bohbot. *The Weapon Wizards: How Israel Became a High-Tech Military*

Superpower. First American Edition. St. Martin's Press, 2017.
Yannakogeorgos, Panayotis. "Cyberspace, the New Frontier – and the Same Old Multilateralism." In *Global Norms, American Sponsorship and the Emerging Patterns of World Politics*, edited by S. Reich. Palgrav, 2011.
Yin, David. "Secrets To Israel's Innovative Edge." *Forbes*, June 5, 2016.
———. "What Makes Israel's Innovation Ecosystem So Successful." *Forbes*, January 9, 2017.
Young, Ashton. "INFOGRAPHIC – The EU's Most Vulnerable Countries to Cybercrime." *Security Brief*, September 6, 2017.
Yu, Eileen. "Singapore Arms up on Cyberdefence Experts, Opens Cyberdefence School." *ZDNet*, February 20, 2019.
Zegart, Amy. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Kindle Edition. Princeton University Press, 2009.
Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*, November 3, 2014.

Appendix
An Overview of Cyber-Defense Indices referenced in Chapter One

1. Introduction

As discussed in the introductory chapter of this dissertation, several relatively small states have historically outpaced and/or continue to rival larger states in their cybersecurity readiness across a variety of indices. The purpose of this appendix is to offer an overview of these indices in more detail and to provide greater insight into the challenges of quantifying cyber-defense capabilities. Each of the indices referenced differ in terms of their source and the metrics used to provide a quantitative framing for assessing cyber-defense capabilities. Yet, all of these indices illustrate a general trend of particular note: leaders are comprised of a mix of larger and relatively small states. In short, a diversity of indices, including the most comprehensive index and my own interview subjects' responses, all demonstrate that in the emergent cyber-defense space, size is not a reliable predictor of capability. It is this observation, rather than any one specific index, metric, or quantitative measure, that underpins the first of the two motivating puzzles presented in the introduction to this dissertation.

Notably, while each of these indices focus on the defensive rather than offensive realities of cybersecurity operations, a high caliber defense relies on the existence of high caliber offensive capabilities. For example, it is not possible to have robust systems or network defense without having offensive expertise in the form of intelligence gathering and red/white teams that 'hack' your own systems to expose vulnerabilities, exercise crisis response frameworks, etc. As one senior American cyberthreat analyst indicated in relation to a question I lobbied to them regarding Finland, just because Finland does not publicly discuss offense or deploy it openly in conflict situations does not mean they do not have state of the art offensive expertise. In fact, their significant defensive expertise "is dependent" on that offensive expertise.[480] By observing the former, we can safely infer the presence of the latter, even when the latter may be under-deployed in non-domestic networks in practice and/or remains chiefly classified or not discussed publicly.

This section proceeds in five parts: four individual overviews covering the indices referenced in Chapter One and a then few concluding thoughts. For an overview of additional indices not directly referenced in the introductory chapter of this dissertation, refer to the "Index of Cybersecurity Indices" by the UN's ITU.[481]

2. Security and Defense Agenda's Index of State's Cybersecurity Preparedness Levels

In 2012, the Brussels-based thinktank Security and Defense Agenda (SDA) released an index of states' cybersecurity preparedness levels.[482] This report's results were supported by country-specific analysis using Robert Lentz's Cyber Security Maturity Model[483] and a global survey conducted by the SDA in late 2011. The survey comprised of 250 senior cybersecurity practitioners and experts ranging from Ministers of Defense to academics and industry practitioners. Respondents spanned 35 countries - from Albania and Mexico to the U.S. and U.K. - and included staff from within the E.U.,

480 Conversation at CyberCon in Tallinn, Estonia. 2018.
481 International Telecommunication Union (ITU), "Index of Cybersecurity Indices," 2017.
482 Security and Defense Agenda, "Cyber-Security: The Vexed Question of Global Rules."
483 President of Cyber Security Strategies and former Director of Cybersecurity for the U.S. Department of Defense.

Interpol,[484] Eurocontrol,[485] the UN, NATO, and the OSCE.[486] Participants were asked to rate 24 countries[487] and 2 international organizations[488] in terms of how well prepared they were against cyberattacks. These survey results helped inform and were coupled with an independent assessment of each countries' cyber readiness using Lentz's Cyber Security Maturity Model, which focuses on cybersecurity capability in the face of Advanced Persistent Threats (APTs). This model provides a five-tier roadmap for achieving security and resilience in the cyber era: (i) applying cyber-hygiene best practices; (ii) using computer network defense tools (e.g. anti-virus software, firewalls, intrusion detection and protection, etc.), (iii) standard setting and data exchange with a focus on creating a robust and interoperable cyber-ecosystem, (iv) implementing dynamic defense at the enterprise/organization level that is both predictive and agile, and (v) implementing dynamic defense of the ecosystem as a whole (e.g. supply chain security, protection of critical infrastructure, etc.) that is both predictive and agile.[489]

3. Cyber Readiness Index (CRI)

Led first Melissa Hathaway[490] but now alongside a team of cybersecurity experts[491] in cooperation with the Potomac Institute for Policy Studies, the Cyber Readiness Index[492] has been published twice: 1.0 in 2013 and 2.0 in 2015. CRI 1.0 examined 35 countries[493] cybersecurity capabilities using primary and secondary sources across five areas: (i) a robust National Cyber Security Strategy, (ii) an operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) to facilitate national incident response, (iii) robust international commitment to address cybercrime, (iv) robust and actionable information sharing mechanisms between government and industry, and (v) investment in R&D and cybersecurity initiatives more broadly. CRI 2.0 expanded its purview to examine 125 countries[494] across seven areas: (i) national strategy, (ii) incident response, (iii) crime and law enforcement, (iv) information sharing, (v) investment in R&D, (vi) diplomacy and trade, and (vii) defense and crisis response. Notably, the CRI does not offer any formal ranking of states despite its scoring mechanism and a series of specific companion case studies for the 2.0 version.

4. Website Expert Builder's Least and Most Vulnerable EU Countries to Cybercrime

While primarily an assessment of cybercrime vulnerability, many of the metrics used to assess that vulnerability in this index also mirror vulnerabilities and areas of preparedness for conflict and APIs more broadly. Moreover, when it comes to nation states or terrorist organizations, the line between crime and conflict below the threshold of war can rapidly become murky and outages, data loss, hacks, etc. stemming from crime can represent a national security threat. This ranking utilized

484 The International Criminal Police Organization.
485 The European Organisation for the Safety of Air Navigation.
486 Organization for Security and Co-operation in Europe.
487 Australia, Austria, Brazil, Canada, China, Denmark, Estonia, Finland, France, Germany, India, Israel, Italy, Japan, Mexico, the Netherlands, Poland, Romania, Russia, Spain, Sweden, the U.K., and the U.S.
488 The E.U., NATO, and the U.N.
489 Security and Defense Agenda, "Cyber-Security: The Vexed Question of Global Rules."
490 President of Hathaway Global Strategies LLC, a Senior Advisor at Harvard Kennedy School's Belfer Center, led the Comprehensive National Cybersecurity Initiative for President Bush, and spearheaded the Cyberspace Policy Review for President Obama.
491 Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri facilitated through the Potomac Institute.
492 Hathaway, "Cyber Readiness Index 1.0," Report Presentation at the Belfer Center. Hathaway Global Strategies.
493 Argentina, Australia, Austria, Brazil, Canada, China, Denmark, Finland, France, Germany, Hong Kong, Iceland, India, Indonesia, Israel, Italy, Japan, Luxembourg, Macau, Mexico, the Netherlands, New Zealand, Norway, Russia, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Switzerland, Sweden, Taiwan, Turkey, the U.K., and the U.S.
494 International Telecommunication Union (ITU), "Index of Cybersecurity Indices." p 5.

publicly available data from the E.U., the U.N.'s ITU GCI, Microsoft, and Rapid7 across four key variables: (i) the percentage of the population experiencing cybercrime, (ii) frequency of residents encountering malware and viruses, (iii) commitment to and robustness of cybersecurity initiatives, and (iv) how exposed internet connections were in each country. Notably, Finland topped the list because it had "the lowest cybercrime encounter rate in Europe" but also was "one of the most prepared nations too" when it came to addressing those vulnerabilities and mitigating their impact on the population and reducing their occurrence.[495]

5. The UN's ITU Global Cybersecurity Index (GCI)

The International Telecommunications Union (ITU), which is associated with the United Nations (UN), is a "a public-private partnership consisting of 193 member states and regulator bodies, 750 sector members (companies, business associations and NGOs) and academic partners."[496] The breadth of the ITU's assessment is quite unique – 194 countries across time – and it assesses each state based on five components of cybersecurity capability: (i) legal measures, (ii) technical measures, (iii) organizational measures, (iv) capacity building, and (v) cooperation. Within these five components, data is collected on twenty-five indicators. Data collection is both primary (survey) and secondary (publicly available data) in nature. As Makridis and Smeets argue, while there are concerns with any data collection method that leverages a survey of stakeholders and experts within the country in question, the ITU has taken specific steps to address and mitigate these concerns. They seek to corroborate survey data with publicly available data in an effort to address self-reporting bias. In addition, when they do not receive responses to their survey, they build out an assessment using public resources and send that profile back to the country in question for validation in an effort to address non-response bias.[497] There have been three editions of this index (2014, 2017, and 2018) so far, with another currently in process but delayed due to covid-19.

6. Concluding Thoughts

There are important limitations to quantifying national defense capabilities in general (such efforts often default to a numerical evaluation of resources or an oversimplification of defense posture due in large part to a range of persisting difficulties, as discussed in detail in Chapter Two). There are also important limitations to quantifying national cyber-defense capabilities in particular (such as classified information, non-publicly available information, and a lack of paper trail. All of which are discussed in greater detail in Chapter Three). These limitations should be taken seriously whenever we assess efforts to quantitively rank or assess cyber-defense capabilities across countries.

In this dissertation, however, one of the two puzzles motivating the project – why do mice roar – stems not from a single index but rather a general observation across indices and my own interviews. Although size has traditionally been understood as a core driving factor of defense capability, it is a poor predictor of nascent but rapidly developing cyber-defense capabilities across states. Moreover, I have chosen to present support for this observation from a series of indices rather than one specific index in order to mitigate some of the concerns that may arise over the source, methodology, and results of any one index or line of effort. The purpose of their use in this project is not to provide an absolute, quantitative ranking of countries but rather to demonstrate that across

[495] Website Builder Expert, "Which EU Country Is Most Vulnerable To Cybercrime?"," 2017, https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.
[496] Makridis and Smeets, "Determinants of Cyber Readiness." p 4.
[497] Makridis and Smeets.. p 5.

quantitative and qualitative assessments, relatively small states have found themselves in the company of far larger historical powers.

This appendix and detailed overview of these various indices also serves a second purpose. All of these indices recognize, through the types of indicators they identify and data they collect, that cyber-defense and cybersecurity capabilities are driven as much by the postures a state adopts (strategies and operationalization of those strategies through an eco-system of laws, institutions, funding initiatives, etc.) as they are by the preponderance and quality of resources at a state's disposal. Yet, questions of how states develop their defense postures, why their defense postures vary, and what factors drive that evolution remain systematically overlooked and underexamined in the cyber conflict and cybersecurity literature. This dissertation situates itself deliberately within that gap.