August 2020

The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure

Jason Blessing
Syracuse University

Abstract

What explains the variation in implementation dynamics for cyber forces across militaries? In other words, as cyber forces emerge in states across the international system, why do some militaries undertake wide-ranging implementation efforts with few alterations to cyber force structure, while implementation in other militaries is characterized by a drawn-out, incremental process entailing several changes in cyber force structure?

Militaries have been building cyber capabilities since the late 1980s; however, formalized military cyber organizations for these capabilities have only recently emerged. These cyber forces—active-duty military organizations that possess the capability and authority to direct and control computer network operations (CNOs) for strategic ends—have received little attention from scholars. Despite the potential impacts cyber forces might hold for international security dynamics, there exists no comprehensive overview of cyber forces and no analysis on the various ways they have been implemented across militaries. Moreover, current explanations drawn from the diffusion of military innovations remain incomplete in explaining the ways in which cyber force structure change over the course of the implementation process.

In this dissertation, I examine the diffusion and implementation of cyber forces and advance a theory of organizational size to account for the varying implementation dynamics across militaries. My dissertation makes two important contributions to the growing literature on cyber conflict. First, I offer a novel typology for categorizing cyber forces and the respective force structures. By classifying cyber forces according to organizational model and scale of command, I identify nine distinct cyber force structures: Subordinated Branch, Subordinated Service, Subordinated Joint, Sub-Unified Branch, Sub-Unified Service, Sub-Unified Joint, Unified Branch, Unified Service, and Unified Joint. The second contribution is empirical: I

create the first comprehensive database to catalogue the diffusion of cyber forces and evolution of cyber force structures across state—the Dataset on Cyber Force Structures.

This dissertation also makes three broader contributions to the study of the diffusion of military innovations. First, I show how organizational characteristics mitigate diffusion pressures by constraining or enabling innovation and implementation. This dissertation moves past debates that portray militaries as either change-resistant or innovation-seeking organizations by providing a more nuanced claim: organizational characteristics—such as size—can predispose militaries to pursue certain types of changes while creating resistance to others. As such, this dissertation sheds important light on the ways in which the military organizational factors can shape the agency and decisions of those implementing an innovation principle.

Second, I advance a stage-based conception of implementation for diffusion frameworks comprised of five stages: pre-adoption, introduction, modification, expansion, and full implementation. This framework can account for both partial and full adoption and provides a way to assess intermediate changes to an innovation prior to its full institutionalization. As a result, I use this framework to showcase the value of stage-based theorizing.

Third, this dissertation introduces new methodological tools for testing stage-based hypotheses about adoption and implementation. In conjunction with qualitative analysis, this dissertation utilizes multistate survival modeling to assess variable effects at each stage of the implementation process. Traditional modeling techniques in the military diffusion literature—such as logistic regressions and basic survival modeling—prove both cumbersome and inadequate for assessing stage-based processes. In using multistate survival modeling, I emphasize the importance of matching methods to conceptual and theoretical assumptions.

THE DIFFUSION OF CYBER FORCES:
MILITARY INNOVATION AND THE DYNAMIC IMPLEMENTATION OF CYBER FORCE STRUCTURE

by

Jason Alexander Blessing

M.A., Virginia Polytechnic Institute and State University, 2013
B.A., The College of William and Mary, 2011

Dissertation
Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Political Science.

Syracuse University
August 2020

Acknowledgements

This dissertation could not have been completed without the support from several individuals and institutions. I am extremely grateful for the support and advice of my committee members at Syracuse University: Colin Elman, Brian Taylor, Dan McDowell, Jim Steinberg, and Sean O'Keefe. As my advisor, Colin Elman was particularly instrumental in guiding me through the graduate program and bringing this project to fruition. I owe thanks to several other faculty members at Syracuse University for their support related to the various incarnations of this project, including but not limited to: Matt Cleary, Renée de Nevers, Dimitar Gueorguiev, Peg Hermann, Seth Jolly, Pat Longstaff, Bob Murrett, and David Popp. I am also grateful for the insight and support from numerous colleagues over the last five years at Syracuse University, including André Anselmo, David Arceneaux, Robert Demgenski, Angely Martinez, Aykut Ozturk, and Elise Roberts. Additionally, I would like to thank the office staff at the Syracuse University Department of Political Science—Candy Brooks, Sally Greenfield, and Jacquie Meyer—for all their assistance since my arrival at Syracuse.

I was fortunate enough to receive support from several institutions for this project. I spent the 2019-2020 academic year as a USIP-Minerva Peace and Security Scholar with the United States Institute of Peace (USIP) in Washington D.C. Without the funding provided jointly by USIP and the United States Department of Defense-sponsored Minerva Research Initiative, I would not have had the ability to finish this dissertation in 2020. I am particularly thankful for the efforts of Kathleen Kuehnast, Tina Hegadorn, and Jordon Mpingo in coordinating the Peace Scholars program and for the feedback provided by the other members of the 2019-2020 cohort. I have also received extensive support from the Syracuse University Institute for Security Policy and Law, and am grateful for the efforts of Keli Perrin, Tom Odell, and Roxanne Tupper in

coordinating funding and workshops. Thanks are also due to the Moynihan Institute of Global Affairs and the Department of Political Science at Syracuse University for their sustained support.

Parts of this dissertation were presented at the 2019 American Political Science Association Conference and benefited greatly from the questions and advice from Elsa Kania and Travis Sharp. An earlier incarnation of this research was workshopped with the Carnegie International Politics Scholars Consortium and Network through the Henry A. Kissinger Center for Global Affairs at the Johns Hopkins University School of Advanced International Studies; I would like to thank Frank Gavin and Kath Hicks for their insights that helped shape the project.

Several other individuals were instrumental to this project. Syracuse alumni were crucial for networking and gaining interview contacts. In the United States, I owe particular thanks to Megan Doscher, David Sulek, and Rich Wilhelm. In Estonia, I would like to thank Siim Alatalu and Alex Filippov, who, in addition to providing connections, showed great hospitality and introduced me to Hell Hunt in Tallinn. I also owe a debt of gratitude to Jim Lewis at the Center for Strategic and International Studies in Washington, D.C., who acted as a mentor, advocate, and sounding board for my research.

My greatest debts are owed to Beatriz Rey and to my family. This dissertation would not have been completed—much less during a global pandemic—without the help and support of Beatriz Rey the last three years; I will always be grateful. My endeavors in graduate school would not have been possible without the unwavering support of my parents, Mary Beth and Roy Echeverria and Don and Susan Blessing, my brother, Nick Blessing, and a list of extended family members too long to list. It truly does take a village. I dedicate this dissertation to my grandparents, Jean and Dan Phillips and Rosie and Carl Blessing.

Table of Contents

List of Figures

List of Tables

Abbreviations

4/PLA	General Staff Fourth Department of the People’s Liberation Army
AFCYBER	Air Forces Cyber
AFCYBER(P)	Air Force Cyber Command (Provisional)
APT	Advanced Persistent Threat
ARCYBER	Army Cyber Command
C4I	Command, Control, Communications, Computers, and Intelligence
CCDCOE	Cooperative Cyber Defense Center of Excellence
CERT	Computer Emergency Response Team
CERT-EE	Estonian Computer Emergency Response Team
CHOD	Chief of Defense
CIA	Central Intelligence Agency
CIDS	Cyber and Information Domain Service
CJTF-OIR	Combined Joint Task Force – Operation Inherent Resolve
CMF	Cyber Mission Force
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COCOM	Unified Combatant Command
CYBERCOM	Estonian Cyber Command
DCFS	Dataset on Cyber Force Structures

DDOS	Distributed Denial of Service
DIRNSA	Director of the National Security Agency
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DOD	Department of Defense
EDF	Estonian Defense Forces
EDL	Estonian Defense League
ENISA	European Union Agency for Cybersecurity
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FLTCYBER	Fleet Cyber Command
FOC	Full Operating Capability
FSB	Russian Federal Security Service
FSK	Norwegian Armed Forces Special Command
GRU	Main Intelligence Directorate of the Russian Military
HRO	High-Reliability Organization
ICBM	Intercontinental Ballistic Missile
ICT	Information and Communication Technology
IOC	Initial Operating Capability
IP	Internet Protocol
ISIL	Islamic State in Iraq and the Levant
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology

IT-RMA	Information Technology Revolution in Military Affairs
ITU	International Telecommunication Union
JFCC-NW	Joint Functional Component Command – Network Warfare
JTF-ARES	Joint Task Force – Ares
JTF-CND	Joint Task Force – Computer Network Defense
JTF-CNO	Joint Task Force – Computer Network Operations
JTF-GNO	Joint Task Force – Global Network Operations
MARFORCYBER	Marine Corps Forces Cyberspace Command
MENA	Middle East and North Africa
MilCERT	Military Computer Emergency Readiness Teams
MilCIRC	Military Computer Incident Response Centers
MJK	Norwegian Navy Special Operations Command
MOD	Ministry of Defense
NATO	North Atlantic Treaty Organization
NETCOM	Network Enterprise Technology Command
NETWARCOM	Network Warfare Command
NMCC	National Military Command Center
NORSOF	Norwegian Special Operations Forces Command
NSA	National Security Agency (United States)
NSPD	National Security Presidential Directive
PLA	People’s Liberation Army
PPD	Presidential Policy Directive
QDR	Quadrennial Defense Review

RMA	Revolution in Military Affairs
SECAF	Secretary of the Air Force
SECDEF	Secretary of Defense
SIPRNet	Secret Internet Protocol Router Network
TTP	Tactics, Techniques, and Procedures
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
USAF	United States Air Force
USAFRICOM	United States Africa Command
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USD	U.S. dollars
USDOD	United States Department of Defense
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
USSOUTHCOM	United States Southern Command
USSPACECOM	United States Space Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command
V-Dem	Varieties of Democracy Project

CHAPTER 1

Introduction

The Research Question

What explains the variation in implementation dynamics for cyber forces across militaries? In other words, as cyber forces emerge in states across the international system, why do some militaries undertake wide-ranging implementation efforts with few alterations to cyber force structure, while implementation in other militaries is characterized by a drawn-out, incremental process entailing several changes in cyber force structure?

The Need for an Organizational Focus in the Cyber Conflict Literature

Cyber forces[1] are active-duty military organizations that possess the capability and authority to direct and control strategic computer network operations (CNOs)[2] in the cyber domain[3] to

[1] Several scholars have used the terms "military cyber organizations" or “cyber commands.” However, as is explained in Chapter 2, I use "cyber forces" to facilitate a discussion of force structures, i.e., "cyber force structure" is more concise than "military cyber organization force structure” and more precise than “cyber command structure.” Thus, cyber forces, military cyber organizations, and cyber commands may be used interchangeably.

[2] Computer network operations encompass three types of operations in the cyber domain. The first is computer network defense (CND), which includes operations intended to the prevent compromises to the integrity, confidentiality, or availability—through theft, infiltration, disruption, denial, degradation, or destruction—of information on computers or the computers or networks themselves. The second type of operation is computer network exploitation (CNE), which encompasses intelligence, surveillance, or reconnaissance (ISR) operations to collect information from an adversary’s computers and networks that fall short of disrupting or destroying information. Finally, computer network attacks (CNA) are actions taken through a network of computers to disrupt, deny, degrade, or destroy another computer’s information or the computers or networks themselves. Espionage and theft only constitute CNAs when information or systems are destroyed in the process.
Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Arlington, VA: Cyber Conflict Studies Association, 2013), 279–80; Piret Pernik, “Preparing for Cyber Conflict: Case Studies of Cyber Command” (Tallinn, Estonia: International Centre for Defence and Security (RKK/ICDS), December 2018), 4.

[3] The cyber domain is a hierarchical contingent system with four layers: (1) the physical layer of infrastructures that enable the domain; (2) the syntactic layer of logical building blocks that support physical platforms and enable services; (3) the semantic layer containing information content; and (4) the user layer of humans who interact with the other three layers; see: Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge and London: The Massachusettes Institute of Technology Press, 2012), 8.

impact, change, or modify strategic diplomatic and military interactions between entities.[4] Militaries have been building cyber capabilities since the late 1980s;[5] however, formalized military cyber organizations for these capabilities have only recently emerged.[6] The creation of United States Cyber Command in 2010 and its subsequent elevation to an independent unified combatant command in 2017 stand as obvious examples of institutional innovation.[7] A variety of states have also established their own "cyber commands." Examples include: South Korea in 2010;[8] Colombia in 2011;[9] the United Kingdom, Turkey, and Spain in 2013;[10] and the

[4] On the impact of computer network operations (i.e. cyber-attacks) on strategic interactions, see: Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford and New York: Oxford University Press, 2015).

[5] For a detailed account of the development of cyber capabilities in the United States, see: Craig J. Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (Doctoral Dissertation, Fairfax, VA, George Mason University, 2016).

[6] Chris C. Demchak and Peter Dombroski, "Rise of a Cybered Westphalian Age 2.0," in *Understanding Cyber Security: Emerging Governance & Strategy*, ed. Gary Schaub, Jr. (London and New York: Rowman and Littlefield Publishers, Inc., 2018), 77–101; Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*.

[7] Robert Knake, "Obama's Cyberdoctrine," *Foreign Affairs*, May 6, 2016, https://www.foreignaffairs.com/articles/united-states/2016-05-06/obamas-cyberdoctrine; Elias Groll, "Trump Elevates Cyber Command," *Foreign Policy*, August 2017, https://foreignpolicy.com/2017/08/18/trump-elevates-cyber-command/.

[8] Zachary Keck, "South Korea Seeks Offensive Cyber Capabilities," *The Diplomat*, October 11, 2014, https://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/.

[9] "Colombia Rises to the Cyber Challenge," *Dialogo,* April 1, 2013, https://dialogo-americas.com/en/articles/colombia-rises-cyber-challenge.

[10] Osula, Anna-Maria, "National Cyber Security Organisation: United Kingdom," National Cyber Security Organisation (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/library/publications/national-cyber-security-organisation-united-kingdom/; Esnar Seker and Ihsan Burak Tolga, "National Cyber Security Organisation: Turkey," National Cyber Security Organisation (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2018), https://ccdcoe.org/library/publications/national-cyber-security-organisation-turkey/; Alexander Cendoya, "National Cyber Security Organisation: Spain," National Cyber Security Organisation (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016), https://ccdcoe.org/library/publications/national-cyber-security-organisation-spain/.

Netherlands and Ecuador both in 2014.[11] The North Atlantic Treaty Organization (NATO) has also announced its own plans to stand up a cyber command by 2023.[12]

Despite these developments, cyber forces have received little explicit attention from international security scholars. Instead, researchers have placed an overwhelming focus on coercive logics of cyber-attacks,[13] escalatory dynamics,[14] debates over offense-dominance,[15] and the transformation of warfare.[16] Other works have centered on military organizations as stakeholders in national cyber-ecosystems[17] and in emerging civil-military issues related to

[11] Kadri Kaska, "National Cyber Security Organisation: The Netherlands," National Cyber Security Organisation (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/library/publications/national-cyber-security-organisation-the-netherlandskadri-kaskaactive-passive-cyber-defence-law-national-frameworks-policy-strategy-the-netherlands/; Directorate of Social Communication of the Joint Command of the Armed Forces of Ecuador, "Fuerzas Armadas realiza taller para defini Infraestructura critica [Armed Forces conducts workshop to define Critical Infrastructure]," *Nota Periodistica No. 2015-04-20-01-DIR-C.S.*, April 20, 2015, https://www.ccffaa.mil.ec/2015/04/20/fuerzas-armadas-realiza-taller-para-definir-infraestructura-critica/.

[12] Robin Emmott, "NATO Cyber Command to Be Fully Operational in 2023," *Reuters*, October 16, 2018, https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9.

[13] Ryan C. Maness and Brandon Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces & Society* 42, no. 2 (2016): 301–23; Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*; E. D. Borghard and S. W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–81; Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter /2017 2016): 44–71; Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York, NY: Oxford University Press, 2018).

[14] D. Gompert and Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability," *Survival* 56, no. 4 (2014): 7–22; Sean T. Lawson et al., "The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate" (2016 8th International Conference on Cyber Conflict, Tallinn, 2016), 65–80; Mischa Hansel, "Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks," *Journal of International Relations and Development*, 2016, 1–29; Jacquelyn Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict" (Dissertation, Washington, D.C., George Washington University, 2017); Benjamin Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (Oxford: Oxford University Press, 2017).

[15] I. Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (2013): 40–63; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (Winter /2017 2016): 72–109.

[16] J. Arquilla and D. Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993): 141–65; Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security* (New York: Harper Collins, 2010); Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 7–40; Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (2013): 125–33; John Lindsay, "The Impact of China on Cyber Security: Fiction and Friction," *International Security* 39, no. 3 (2015): 7–47.

[17] For overviews, see: Eviatar Matania, Lior Yoffe, and Tal Goldstein, "Structuring the National Cyber Defence: In Evolution towards a Central Cyber Authority," *Journal of Cyber Policy* 2, no. 1 (2017): 16–25; Moritz Weiss and

cyberspace.[18] As one recent review of the literature has highlighted, the lack of analysis of cyber forces—and, in particular, *different organizational structures*—hinders a greater understanding of cyber conflict.[19] Given the implications that cyber forces might hold for security dynamics, this shortage of substantial analysis is problematic. The development and growth of cyber forces provide evidences of states' interest in conducting offensive cyber operations.[20] As a result, these organizations and their activities can potentially impact escalatory dynamics in cyberspace,[21] cyber-arms racing,[22] and the effectiveness of coercive campaigns in the cyber domain.[23] More broadly, understanding the diffusion and evolution of cyber forces is also a necessary step in

Vytautas Jankauskas, "Securing Cyberspace: How States Design Governance Arrangements," *Governance*, 2018, 1–17.

[18] Sergei Boeke, Matthijs A. Veenendaal, and Caitriona H. Heinl, "Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges and State Practices across Asia and Europe," in *7th International Conference on Cyber Conflict* (Architectures in Cyberspace, Tallinn, Estonia: NATO CCD COE Publications, 2015), 1–13; Sergei Boeke, "National Cyber Crisis Management: Different European Approaches," *Governance* 31 (2018): 449–64.

[19] Emphasis added. Robert Gorwa and Max Smeets, "Cyber Conflict in Political Science: A Review of Methods and Literature" (2019 International Studies Association Annual Convention, Toronto, Canada, 2019), 1–24.

[20] Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," in *11th International Conference on Cyber Conflict: Silent Battle*, ed. T. Minarik et al. (Tallinn, Estonia: NATO CCD COE Publications, 2019), 163–78. On the integrations of offensive cyber operations ito organizational missions, see: Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?," in *10th International Conference on Cyber Conflict* (CyCon X: Maximising Effects, Tallinn, Estonia: NATO CCD COE Publications, 2018), 55–72; Max Smeets, "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks," in *9th International Conference on Cyber Conflict* (Defending the Core, Tallinn, Estonia: NATO CCD COE Publications, 2017), 1–18.

[21] On cyber-escalation, see: Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict"; Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*.

[22] Anthony Craig and Brandon Valeriano, "Conceptualising Cyber Arms Races" (2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2016), 141–58; Anthony Craig and Brandon Valeriano, "Reacting to Cyber Threats: Protection and Security in the Digital Age," *Global Security and Intelligence Strudies* 1, no. 2 (2016): 21–41.

[23] These organizations can also provide insight into how states and conceptualize the co-deployment of computer network operations with kinetic force in battlefield settings to coerce adversaries; see: Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution*, 2017, 1–31, http://journals.sagepub.com/doi/pdf/10.1177/0022002717737138. For overviews of cyber coercion, see: Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter /2017 2016): 44–71; Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York, NY: Oxford University Press, 2018).

theorizing how technology shapes and reshapes the nature of interactions, conflict, and warfare between states over time.[24]

To date, scholars investigating cyber forces have focused more on the varying maturity of forces rather than the structural variation. For example, both Gomez (2016) and Robinson et al. (2013) analyze military cyber organizations as one component of a state's national cyber capabilities. While Gomez (2016) only relies on the presence or absence of these organizations in his index, Robinson et al. (2013) assess the maturity of cyber organizations within European Union member states' militaries.[25] Similarly, Smeets (2019) catalogues the maturity of military cyber organizations across NATO-member states, finding that most organizations are still in the nascent stages of development.[26] Although these studies provide valuable insights, a focus on organizational maturity inadvertently homogenizes institutions in terms of mandates, scope of authority, and missions. Even when organizations are at the same stage of development or maturity, there may exist crucial structural differences between cyber forces.

While the United States' cyber force structure has been debated extensively,[27] analysis in a comparative context has been rare. Saltzman (2013) provides an important bridge by categorizing offensive and defensive cyber force postures for China, Russia, the United States,

[24] Geoffrey L. Herrera, *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change* (Albany, New York: State University of New York Press, 2006). For an overview of of cyberspace transforms warfare, see: Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017).

[25] Miguel Alberto N. Gomez, "Arming Cyberspace: The Militarization of a Virtual Domain," *Global Security and Intelligence Studies* 1, no. 2 (2016): 42–65; Neil Robinson et al., "Stocktaking Study of Military Cyber Defence Capabilities in the European Union (MilCyberCAP): Unclassified Summary" (RAND Corporation, 2013).

[26] Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis."

[27] S Nielsen, "The Role of the U.S. Military in Cyberspace," *Journal of Information Warfare* 15, no. 2 (2016): 27–38; Samuel Liles and Jacob Kambic, "Cyber Fratricide," in *6th International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCD COE Publications, 2014), 329–38; Frank J. Cilluffo and Joseph R. Clark, "Repurposing Cyber Command," *Parameters* 43, no. 4 (2013): 111–18; J. L. Samaan, "Cyber Command: The Rift in U.S. Military Cyber-Strategy," *The RUSI Journal* 155, no. 6 (2010): 16–21.

and NATO.[28] Although highlighting variation in militaries, Saltzman's study emphasizes strategic dynamics over the variation in organisational dimensions. To this end, Pernik (2018) investigates different cyber force command structures. In the first publicly available comparison of cyber forces, Pernik identifies three distinct command types: cyber divisions, which are subordinate to larger logistical entities in the military; cyber services, which are standalone functional combat services; and cyber commands, which are standalone combatant commands or branches with the capability and authority to direct and computer network operations.[29] Although an important foundation, this conceptualization only capture a small amount of the possible institutional variation in cyber forces.

This review reveals three major shortcomings in existing works on cyber forces. The first is definitional: scholars have utilized a variety of definitions to identify cyber forces. As such, "[t]here is no common understanding of what constitutes a cyber command."[30] Second, and relatedly, no consistent terminology has emerged for classifying and assessing the military institutions tasked with developing and deploying cyber capabilities. The lack of a common definition—and the blanket usage of the term "cyber command"—has masked important variation in the roles, responsibilities, and scope of institutional arrangements of cyber forces. Finally, as a result, there exists no comprehensive overview of existing cyber forces and no explanation of how cyber force structures change across and within militaries over time.

Considering this discussion, **my dissertation makes two important contributions to the growing literature on cyber conflict**. First, I offer a novel typology for categorizing cyber forces and the respective force structures. By classifying cyber forces according to organizational

[28] Saltzman, "Cyber Posturing and the Offense-Defense Balance."
[29] Pernik, "Preparing for Cyber Conflict: Case Studies of Cyber Command."
[30] Pernik, 1.

model and scale of command**, I identify nine distinct cyber force structures: Subordinated Branch, Subordinated Service, Subordinated Joint, Sub-Unified Branch, Sub-Unified Service, Sub-Unified Joint, Unified Branch, Unified Service, and Unified Joint. The second contribution is empirical: I create the first comprehensive database to catalogue the diffusion of cyber forces and evolution of cyber force structures across state.**

The Argument

Drawing on insights from the diffusion of military innovations and organizational theory, **the central argument of this dissertation is that organizational size—specifically, the size of a state's military organization—is an ever-present but oft-overlooked variable that shapes the implementation of cyber forces and thus the changes in cyber force structure over time**. Implementation is a dynamic process consisting of five interconnected stages: pre-adoption, introduction, modification, expansion, and full implementation. Some implementation efforts may move through each stage, while others may bypass certain stages altogether. Substantively, creating and implementing cyber forces requires both building a mission-oriented, operationally effective organization and integrating that organization into the existing defense bureaucracy. Although these goals pull implementation resources in opposing directions, implementers must achieve both to fully implement a cyber force.

In short, implementers in larger military organizations are more predisposed to initially prioritize bureaucratic integration of cyber forces over operational imperatives, while those in smaller militaries are more likely to prioritize building cyber capabilities. Despite a greater risk tolerance and the availability (relative to smaller organizations) of human and financial capital to build out the cyber mission, larger militaries entail a greater number of competing interests that can threaten the autonomy of cyber forces or lay claim to the cyber mission. As such, implementers in larger militaries are more likely to ensure the bureaucratic integration and organizational survival of cyber forces before prioritizing mission-building. Conversely, smaller militaries are more likely to focus directly on mission-building. Implementers in smaller militaries face a smaller pool of bureaucratic competitors; however, smaller militaries possess a smaller resource base and lack the risk tolerance of larger militaries. Accordingly, implementers are more inclined to vigorously build out the cyber mission to justify an additional strain on financial and human capital. Subsequently, implementers in smaller militaries are likely to pivot to the bureaucratic imperative in attempts to secure future resources.

Size is an obvious factor that matters in contingent and unobvious ways. Organizational size—in conjunction with other factors—helps shape implementation priorities that influence implementation pathways and changes in cyber force structure. While organizational size does not fully explain implementation dynamics, this dissertation asserts that the effects of size on the implementation process cannot be ignored.

Diffusion of Military Innovations: A Necessary but Underspecified Foundation

To examine the spread and implementation of cyber forces worldwide, this dissertation builds on frameworks advanced in the literature on the diffusion of military innovations. While this dissertation does not explicitly examine processes of diffusion, it does ask: "what comes next"? Diffusion provides a necessary precursor and foundation for examining the implementation of an international innovation. As such, exploring the assumptions and shortcomings inherent in the diffusion literature represent a crucial starting point for examining what "comes next"—implementation.

Broadly, diffusion represents a pattern of "[a]n S-shaped rate of adoption over time…[and] different sources/channels at different stages in the innovation-decision process for an individual [unit]."[31] Diffusion can be viewed as a consequence of interdependence between units of analysis.[32] Authors across a range of subfields—most prominently, the international security and public policy subfields—generally agree that diffusion is defined as (1) a process occurring (2) among the members of a social system whereby (3) an innovation is communicated (5) through certain channels (6) over time and where (7) the probability of adopting the innovation is systematically conditioned by the prior choices of others in the social system.[33]

Diffusion studies must thus account for five factors: the transfer object (innovation), the transfer agent, the transfer recipient, the transfer media/medium, and the demand environment/social system.[34] In studies of military diffusion, states and their militaries are naturally the primary transfer agents and recipients of innovations spreading across the international system. Authors have focused broadly on the competitive, normative, and cultural transmission mediums through which innovations diffuse.[35] The innovation at the center of

[31] E. M. Rogers, "A Prospective and Retrospective Look at the Diffusion Model," *Journal of Health Communication* 9, no. S1 (2004): 16.

[32] F. Gilardi, "Transnational Diffusion: Norms, Ideas, and Policies," in *Handbook of International Relations*, ed. Walter Carlsnaes, Thomas Risse, and Beth Simmons, vol. 2 (London: Sage Publications Ltd, 2013), 454.

[33] Francis Stokes Berry and William D. Berry, "Innovation and Diffusion Models in Policy Research," in *Theories of the Policy Process*, ed. Paul A. Sabatier and Chris Weible, 3rd Edition (Boulder, CO: Westview Press, 2014), 310; Gilardi, "Transnational Diffusion: Norms, Ideas, and Policies," 454–55, 473; Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, New Jersey: Princeton University Press, 2010), 19; E. M. Rogers, "A Prospective and Restrospective Look at the Diffusion Model," *Journal of Health Communication* 9, no. S1 (2004): 13; Leslie C. Eliason and Emily O. Goldman, "Introduction: Theoretical and Comparative Perspectives on Innovation and Diffusion," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, California: Stanford University Press, 2003), 11–22.

[34] Barry Bozeman, "Technology Transfer and Public Policy: A Review of Research and Theory," *Research Policy* 29 (2000): 637; B. Weinert, "Integrating Models of Diffusion of Innovations: A Conceptual Framework," *Annual Review of Sociology* 28 (2002): 297–326..

[35] For succinct descriptions and examples of these mediums, see: Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, 20–22; Emily O. Goldman, "Introduction: Military Diffusion and Transformation," in *The Information Revolution in Military Affairs in Asia*, ed. Emily O. Goldman and Thomas G. Mahnken (New York: Palgrave MacMillan, 2004), 5–6; Emily O. Goldman and Andrew L. Ross, "Conclusion: The Diffusion of Military Technology and Ideas- Theory and Practice," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, California: Stanford University Press, 2003), 377–82; Andrea Gilli and Mauro Gilli, "The Diffusion of Drone Warfare?: Industrial, Organizational, and Infrastructural Constraints," *Security Studies* 25, no. 1 (2016): 53–55. For a comprehensive overview and critique of sociological institutionalist accounts of diffusion, see: Colin Elman, "Appendix 4 to: The Logic of Emulation: The Diffusion of Military Practices in the International System" (Dissertation, New York, NY, Columbia University, 1999), 502–44.

diffusion is generally a policy that is new to the government (or unit of analysis) that is adopting it.[36] Studies of domestic public policy in the United States have focused on the spread of innovations such as welfare and civil rights policies,[37] education policies and reforms,[38] tort laws,[39] state lottery policies,[40] the Children's Health Insurance Program,[41] and anti-smoking policies.[42] Diffusion studies in international relations (outside of military innovation) have tended to focus on phenomena such as capital account liberalization,[43] bilateral investment treaties,[44] regime changes,[45] and militarized conflict and war.[46]

In the context of military diffusion,[47] innovations represent "changes in the conduct of warfare designed to increase the ability of a military organization to convert the components of potential military power into actual military power."[48] Additionally, military innovations can be

[36] Berry and Berry, "Innovation and Diffusion Models in Policy Research."

[37] V. Gray, "Innovation in the States: A Diffusion Study," *American Political Science Review* 67, no. 4 (1973): 1174–85.

[38] Gray; M. Mintrom and S. Vergari, "Policy Networks and Innovation Diffusion: The Case of State Education Reforms," *The Journal of Politics* 60, no. 1 (1998): 126–48.

[39] B. C. Canon and L. Baum, "Patterns of Adoption of Tort Law Innovations: An Application of Diffusion Theory to Judicial Doctrines," *American Political Science Review* 75, no. 4 (1981): 975–87.

[40] Francis Stokes Berry and William D. Berry, "State Lottery Adoptions as Policy Innovations: An Event History Analysis," *American Political Science Review* 84, no. 2 (1990): 395–415.

[41] C. Volden, "States as Policy Laboratories: Emulating Success in the Children's Health Insurance Program," *American Journal of Political Science* 50, no. 2 (2006): 294–312.

[42] C. R. Shipan and C. Volden, "Bottom-up Federalism: The Diffusion of Antismoking Policies from U.S. Cities to States," *American Journal of Political Science* 50, no. 4 (2006): 825–43.

[43] Beth Simmons and Zachary Elkins, "The Globalization of Liberalization: Policy Diffusion in the International Political Economy," *American Political Science Review* 98, no. 1 (February 2004): 171–89.

[44] Zachary Elkins, A. T. Guzman, and Beth Simmons, "Competing for Capital: The Diffusion of Bilateral Investment Treaties, 1960-2000," *International Organization* 60, no. 4 (2006): 811–46.

[45] L. E. Cederman and K. S. Gleditsch, "Conquest and Regime Change: An Evolutionary Model of the Spread of Democracy and Peace," *International Studies Quarterly* 48, no. 3 (2004): 603–29; J. S. Kopstein and D. A. Reilly, "Geographic Diffusion and the Transformation of the Postcommunist World," *World Politics* 53, no. 1 (2000): 1–37.

[46] S. A. Bremer, "The Contagiousness of Coercion: The Spread of Serious International Disputes, 1900-1976," *International Interactions* 9, no. 1 (1982): 29–55; B.A. Most and H. Starr, "Diffusion, Reinforcement, Geopolitics, and the Spread of War," *American Political Science Review* 74, no. 4 (1980): 932–46; R. M. Siverson and H. Starr, "Opportunity, Willingness, and the Diffusion of War," *American Political Science Review* 84, no. 1 (1990): 47–67.

[47] Due to significant conceptual and theoretical overlaps, this discussion draws on insights from both the literatures on military innovation and the diffusion of military innovations. On this overlap, see: Goldman, "Introduction: Military Diffusion and Transformation."

[48] Michael C. Horowitz and Shira E. Pindyck, "What Is a Military Innovation? A Proposed Framework" (Working Paper, December 2019), 17, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504246.

further defined along two dimensions.[49] First, innovations can occur at strategic, operational, and/or tactical levels.[50] Second, innovations can be defined in terms of technological, doctrinal, and/or organizational components. Although an innovation can encompass one, two, or all three components;[51] of the three, technological dimensions have usually received the most attention from scholars.[52] Importantly, innovations may only have limited success improving the ability of militaries to generate greater power; wide-ranging impacts are not a pre-requisite for defining innovations.[53]

Shortcomings in the Military Diffusion Literature

The preceding discussion provides an important conceptual foundation for explaining the implementation of cyber forces and the development of cyber force structures over time. Nevertheless, I argue that, on two accounts, existing military diffusion frameworks remain

[49] Some have included a third dimension: the degree of change from existing practices, i.e. whether an innovation represents an incremental change, a disruptive change, or something between the two. However, this is not an inherent characteristic of the innovation—it is a trait that is only defined relative to the potential innovating/adopting military. As such, including this dimension blurs an important distinction between the innovation itself and the innovation/diffusion environment. As will be shown later in the dissertation, the spectrum of change is less a characteristic of an innovation itself and more an implementation response by innovating/adopting militaries. On the potential scales of change (particularly disruptive change), see: Tai Ming Cheung, Thomas G. Mahnken, and Andrew L. Ross, "Frameworks for Analyzing Chinese Defense and Military Innovation," in *Forging China's Military Might: A New Framework for Assessing Innovation* (Baltimore, Maryland: Johns Hopkins University Press, 2014), 30–38; Theo Farrell, "Improving in War: Military Adaptation and the British in Helman Province, Afghanistan, 2006-2009," *Journal of Strategic Studies* 33, no. 4 (2010): 567–94; Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, California: Stanford University Press, 2010); Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, 22–23; Dima Adamsky and Kjell Inge Bjerga, "Introduction," in *Contemporary Military Innovation: Between Anticipation and Adaptation*, ed. Dima Adamsky and Kjell Inge Bjerga (London and New York: Routledge, 2012), 1–6. On the need to conceptually demarcate the innovation from the broader social environment, see: Bozeman, "Technology Transfer and Public Policy: A Review of Research and Theory," 628–30.

[50] Cheung, Mahnken, and Ross, "Frameworks for Analyzing Chinese Defense and Military Innovation," 16–17.

[51] For elaboration on these components of innovation, see: Matthew Evangelista, *Innovation and the Arms Race: How the United States and the Soviet Union Develop New Military Technologies* (Ithaca and London: Cornell University Press, 1988), 51; Goldman, "Introduction: Military Diffusion and Transformation," 7; Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, no. 37 (1994): 30.

[52] Cheung, Mahnken, and Ross, "Frameworks for Analyzing Chinese Defense and Military Innovation," 23–24.

[53] Horowitz and Pindyck, "What Is a Military Innovation? A Proposed Framework," 17. For a countervailing view that argues military innovations are defined in part by large leaps in effectiveness, see: Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* 29, no. 5 (2006): 905–34.

underspecified for addressing the variety of ways in which militaries can implement cyber forces post-adoption. First, studies rarely acknowledge the degree of agency and innovation modulation that is available to potential adopters. Specifically, studies must specify whether the innovation under investigation is a concrete model—i.e. it entails specific policy instruments and a blueprint for implementation—or a broader principle or framework. Second, and relatedly, existing diffusion frameworks tend to treat implementation as part of adoption: successful adoption assumes successful implementation.

Problem 1: Innovation Model or Innovation Principle? Innovative policies and technologies exist on a spectrum from concrete models with specific policy instruments and a blueprint for adoption to broader principles or frameworks.[54] At one extreme, potential adopters are presented with a distinct innovation model. This model prescribes the adoption of certain policy instruments—tools and techniques that link the adoption of an innovation to its implementation[55]—and entails information on how the innovation should be implemented. At the other extreme, an innovation appears as general principle to be adopted, i.e. broad maxims of innovation that provide a general direction for policymakers but do not prescribe specific policy instruments or courses of action regarding implementation.[56] Military diffusion studies rarely explicitly acknowledge which phenomenon—model diffusion or principle diffusion—is under investigation. Two examples, the analysis of new "military models" and carrier warfare, serve to

[54] Gilardi, "Transnational Diffusion: Norms, Ideas, and Policies," 458.

[55] Peter J. May, "Policy Design and Implementation," in *The SAGE Handbook of Public Administration*, ed. B. Guy Peters and Jon Pierre (London: Sage Publications Ltd, 2012), 279–91; Michael Howlett, "Policy Instruments, Policy Styles, and Policy Implementation: National Approaches to Theories of Instrument Choice," *Policy Studies Journal* 19, no. 2 (1991): 1–21; Susana Borras and Charles Edquist, "The Choice of Innovation Policy Instruments," *Technological Forecasting & Social Change* 80 (2013): 1513–22. The discussion of policy instruments has been at the heart of recent public policy research on policy design. For an overview of the policy design literature, see: Michael Howlett, Ishani Mukherjee, and Jun Jie Woo, "From Tools to Toolkits in Policy Design Studies: The New Design Orientation towards Policy Formulation Research," *Policy and Politics* 43, no. 2 (2015): 291–311.

[56] Kurt Weyland, *Bounded Rationality and Policy Diffusion: Social Sector Reform in Latin America* (Princeton, New Jersey: Princeton University Press, 2009), 17–18.

show that that same types of innovations have been portrayed as both concrete models and general principles.

New "military models" in the literature have been examined as both innovation principles and concrete innovation models. Studies of information technology-based (IT) military models, network-centric military models, and the revolution in military affairs (RMA) fall into the former category—broad principles of innovation. For instance, Demchak's (2003) assessment of the spread of IT-based militaries advances five broad maxims related to innovation: doctrinal flexibility, strategic mobility, tailorability and modularity, joint and international connectivity, and the versatility to function in both war and operations other than war. As the author notes, the IT-based "model" is an incredibly broad vision that has been pursued in a variety of ways.[57] Similarly, Junio (2012) defines network-centric military forces as those incorporating "a group of operational concepts that, together, are intended to enable a military to conduct missions quicker and more effectively."[58] Key concepts include: self-synchronization; the organization of the military itself into a network to absorb and disseminate information; increased speed of decision making; enhanced battlespace awareness; and the decentralization of decision making.[59] As with Demchak's study on IT-based militaries, Junio's net-centric "model" is based on broad principles for innovation that can be implemented in different ways. Works on military transformation and RMA offer even broader examples of innovation principles. For example, the edited volume by Terriff et al. (2010) examines the spread of the United States' transformation model to its European NATO allies. This U.S.-based "model" rests on three broad innovation

[57] Chris C. Demchak, "Creating the Enemy: Global Diffusion of the Information Technology-Based Military Model," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, California: Stanford University Press, 2003), 308–12.
[58] Timothy J. Junio, "Marching Across the Cyber Frontier: Explaining the Global Diffusion of Network-Centric Warfare," in *Cyberspaces in Global Affairs*, ed. Sean S. Costigan and Jake Perry (Burlington, Vermont: Ashgate Publishing Company, 2012), 54.
[59] Junio, 54–55.

principles: network-enabled capability, similar to Junio's (2012) network-centric warfare; effects-based operations; and a shift from territorial defense to expeditionary warfare. As the introductory chapter of the volume notes, these are inherently broad concepts for innovation.[60]

At the same time, scholars have assessed the diffusion of more concrete, specific military models. Resende-Santos' (2007) work offers such an example: his study centers on the attempts of Latin American militaries to emulate the Prussian/German military model. He identifies four distinguishing features of the Prussian/German model. The first was a conscription system consisting of short-term service in the first line that built a pool of trained reserves. Conscription was decentralized so that service was done primarily at the local district of enlistment. The second feature of the Prussian model was its system of officer recruitment and instruction; this included a reorganization of military education and changes to curriculum that separated officer training from general military education. Third, the Prussian model organized the general staff according to mission-orientation: it was subdivided into functional departmental groupings so that it could manage all aspects of mass warfare. The general staff was also given extensive autonomy and command authority vis-à-vis civilian.[61] This model is contrasted with the French model. The French model hinged on: a conscription system focused on longer-term service (seven-plus years) for the first line; little distinct education training for general staff officers; and a weak, decentralized general staff that was heavily subordinated to civilians.[62]

Eisenstadt and Pollack (2003) examine another case of model diffusion: the spread of the Soviet model to the Middle East. The authors identify twelve doctrinal and organizational

[60] Theo Farrell and Terry Terriff, "Military Transformation in NATO: A Framework for Analysis," in *A Transformation Gap? American Innovations and European Military Change* (Stanford, California: Stanford University Press, 2010), 5–6.
[61] Joao Resende-Santos, *Neorealism, States, and the Modern Mass Army* (Cambridge: Cambridge University Press, 2007), 95–103.
[62] Resende-Santos, 104–8.

features of the Soviet model: (1) the linkage of force to diplomacy—war served political objectives, and strategy and operations were subordinate to political planning; (2) achieving rapid victory and enemy annihilation through surprise, offense, and continuous operations; (3) echeloned attacks with multiple breakthrough points; (4) the use of air and missile operations and operational maneuver groups to attack through the enemy's depth; (5) an emphasis on preemptive strikes on the enemy's tactical nuclear forces; (6) fast-paced operations with advance rates of roughly 50-70 kilometers per day; (7) maximized freedom of operational commanders and restricted freedom for tactical commanders; (8) detailed operational planning with an assumption that set-piece planning will change; (9) highly mechanized forces; (10) placing the taking as a centerpiece of force structure; (11) and emphasis on combined arms; and (12) the use of air superiority as a key tool for success.[63] Even more so than Resende-Santos' description of the Prussian/German model, Eisenstadt and Pollack provide multiple innovation characteristics and instruments with which to assess diffusion.

Carrier warfare offers an even clearer example of how researchers can define *the same* innovation as both a model and principle. Goldman (2003) identifies two distinct institutional models of carrier warfare from the end of World War I to the end of World War II: the offensive model and the defensive model of carrier warfare. Goldman elaborates:

> The Americans and Japanese adopted the offensive carrier air paradigm. They made air power the centerpiece of their navies, transition to air-centered naval organizations and operations, and concentrated and operated carriers independently in carrier battle groups. The British grafted air power onto existing doctrine, keeping the carrier in a defensive role, subordinate to part of the battle line. They used carriers to hunt down enemy raiders and supply ships, escort

[63] Michael J. Eisenstadt and Kenneth M. Pollack, "Armies of Snow and Armies of Sand: The Impact of Soviet Military Doctrine on Arab Militaries," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, California: Stanford University Press, 2003), 71–72.

> convoys, attack special land targets, conduct ocean sweeps and patrols, and ferry land-based aircraft to fighting zones.[64]

Goldman differentiates these two models along four dimensions: the prevailing air power-battle fleet paradigm; carrier-specific doctrine; the organizational structure within which aircraft carriers were embedded; and the carrier design and the design of the aircraft complement.[65] In contrast, Horowitz (2010) assesses the non-adoption (i.e. failed diffusion) of carrier warfare. He does not define a distinct model of carrier warfare; instead, carrier warfare is defined more as a general principle that entails

> the combined use of fleet aircraft carriers and an array of logistical ships for the purpose of conducting strikes against enemy naval assets and establishing sea control. It uses carriers as mobile airfields, abandoning reliance on naval gunfire as the core of the naval fleet by substituting air-launched weapons for the power of the big gun.[66]

These examples show that military diffusion studies can and do conceptualize innovations as both concrete models and broader principles. However, researchers rarely acknowledge whether they are examining model diffusion or principle diffusion; instead, authors' definitions of innovations act as an implicit signal. For two reasons, this becomes problematic, particularly as studies engage with and build on previous research.

First, the specification of an innovation—whether in the form of a principle or a model with instruments—can affect findings regarding both the degree and rate of diffusion.[67] Scholars that study the same innovation but define it differently (as a model or principle) can reach

[64] Emily O. Goldman, "Receptivity to Revolution: Carrier Air Power in Peace and War," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, California: Stanford University Press, 2003), 276. The Germans and Italians realized the potential of carriers too late for any to be deployed during World War II.

[65] Goldman, 275.

[66] Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, 67–68.

[67] N. van der Heiden and F. Strebel, "What About Non-Diffusion? The Effect of Competitiveness in Policy-Comparative Diffusion Research," *Policy Sciences* 45, no. 4 (2012): 345–58. The specification of instruments can also lead potential adopters to see an innovation as effective; see: Volden, "States as Policy Laboratories: Emulating Success in the Children's Health Insurance Program"; Shipan and Volden, "Bottom-up Federalism: The Diffusion of Antismoking Policies from U.S. Cities to States."

different theoretical conclusions about the dynamics of diffusion. Second, conceptualizing an innovation as a principle or model carries important implications for assessing the degree to which adopters have room for agency and modulation. Model diffusion leaves little room for agency and empirical variation. Because innovations are defined with specific policy instruments and implementation plans, agency and empirical variation remains limited as militaries may choose to fully adopt the model, adopt select components/instruments of the model, or reject the model through either non-adoption or wholesale reinvention of the innovation.[68] Under principal diffusion, however, there exists much more room for agency and empirical variation. There is no standard innovation model from which to deviate; instead, the general innovation principle is adopted. As such, potential adopters are faced with a broader range of adoption and implementation choices and decisions. There is no source of empirical variation in the adoption stage: the broad principle is either adopted or it is not. Changes and variation thus occur during implementation and are relative to how each individual military initially implemented the innovation principle. As a result, model diffusion presents limited agency and variation at the adoption stage for potential adopters; in contrast, principle diffusion allows for greater agency and empirical variation which manifest during implementation.[69] This analytical shift highlights a second, related problem in the military diffusion literature.

Problem #2: Conflating Implementation with Adoption. The second conceptual shortcoming in the military diffusion literature is the conflation of implementation an adoption. Implementation has traditionally received little attention from the military diffusion literature.

[68] For a discussion of these dynamics in relation to military emulation, see: Elman, "The Logic of Emulation: The Diffusion of Military Practices in the International System," 42–44.

[69] Grauer (2015) presents a rare example. Ryan Grauer, "Moderating Diffusion: Military Bureaucratic Politics and the Implementation of German Doctrine in South America, 1885-1914," *World Politics* 67, no. 2 (April 2015): 268–312.

Similarly, military innovation studies tend to focus on explanations for innovation outcomes—specifically the invention and incubation of new technologies and practices—instead of implementation dynamics. Most accounts across both literatures "black box" implementation: it is combined into a single "adoption" stage, where civilian or military leaders decide to adopt an innovation, then provide implementation orders to the relevant military community that faithfully implements the innovation.[70]

In effect, the probability of implementation success is equated with the probability of adoption. As such, these studies can account for the initial introduction of an innovation into a military organization but not the subsequent institutionalization of that innovation.[71] Researchers risk overlooking instances of successful adoption but failed implementation by classifying these cases as failed adoption. Moreover, military innovation studies focus on this dynamic mainly in relation to the "prime movers" of an international innovation; diffusion studies generally focus on the decision calculus of a wider range of potential adopters.

By collapsing implementation into adoption, studies neglect the dynamic and contested nature of implementation and the forms of political and organizational resistance that can emerge in response to implementation. There are a few exceptions; as several have noted, there is a clear distinction between attempting to implement and innovation and actually doing so.[72] In the military innovation literature, Mahnken (2011) and Rosen (1991) conceptualized implementation as a distinct stage that occurs after the speculation and experimentation associated with innovation. In this sense, implementation activities occur after adoption to support the integration

[70] Horowitz and Pindyck, "What Is a Military Innovation? A Proposed Framework," 18.

[71] Adam N. Stulberg, Austin Long, and Michael D. Salomone, *Managing Defense Transformation: Agency, Culture and Service Change* (London: Routledge, 2007), 182.

[72] Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, 21 n. 8.

and routinization of an innovation.[73] In a rare example in the diffusion literature, Grauer (2015) integrates the dynamics of bureaucratic politics into diffusion logics by focusing on the adoption and implementation German military doctrine in Argentina, Brazil, and Chile. His analysis shows that opposing bureaucratic factions can actively stall or sabotage implementation—as the size of the opposing faction grows, the chances of fully implementing German doctrine significantly decrease. Stulberg et al. (2007) deal with similar implementation issues related to the spread of military transformation initiatives: military organizations are much more likely to vigilantly implement transformation when procedural oversight mechanisms are clearly specified and existing managerial norms are utilized.[74]

However, these exceptions only focus on the degree to which an innovation is implementation. As such, accounts of change in military diffusion generally tend to be subsumed under adoption decisions.[75] The challenge, then, is to conceptualize a broader diffusion framework that (1) applies to both model and principle diffusion, (2) applies to all potential adopters of an innovation (prime movers and later adopters), (3) considers adoption decisions, and (4) accounts for a dynamic implementation process in terms of the scope and character of an innovation over time.

[73] Thomas G. Mahnken, "China's Anti-Access Strategy in Historical and Theoretical Perspective," *The Journal of Strategic Studies* 34, no. 3 (2011): 299–323; Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca and London: Cornell University Press, 1991). Although not as formally as Rosen or Mahnken, Kier (1995) does also address several issues related to implementation. Elizabeth Kier, "Culture and Military Doctrine: France between the Wars," *International Security* 19, no. 4 (1995): 65–93.

[74]Stulberg, Long, and Salomone, *Managing Defense Transformation: Agency, Culture and Service Change*.

[75] This is particularly true for examinations of military and strategic culture, which have both been identified as factors shaping divergent adoption decisions. See: Thomas-Durell Young, "Cooperative Diffusion through Cultural Similarity: The Postwar Anglo-Saxon Experience," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, California: Stanford University Press, 2003), 93–113; John A. Lynn, "Heart of the Sepoy: The Adoption and Adaptation of European Military Practice in South Asia, 1740-1805," in *The Diffusion of Military Technology and Ideas*, ed. Emily O. Goldman and Leslie C. Eliason (Stanford, California: Stanford University Press, 2003), 33–62; Eisenstadt and Pollack, "Armies of Snow and Armies of Sand: The Impact of Soviet Military Doctrine on Arab Militaries"; Emily Goldman, "Cultural Foundations of Military Diffusion," *Review of International Studies* 32, no. 1 (2006): 69–91.

This Dissertation's Contributions to Military Diffusion Studies

When taken together, the shortcomings discussed above suggest that military diffusion frameworks need important clarifications and extensions, particularly for cases of principle diffusion. To these ends, **this dissertation makes three contributions to the literature on the diffusion of military innovations. First, I highlight how organizational characteristics mitigate diffusion pressures by constraining or enabling innovation and implementation.** Organizational factors—such as organizational size—filter the international stimuli associated with diffusion[76] by facilitating certain types of innovation and change while constraining others.[77] In doing so, this dissertation moves past claims that portray military organizations as either resistant to change (and thus an obstacle to diffusion) or proactive in seeking out innovation.[78] Instead, I provide a more nuanced claim: organizational characteristics such as size can predispose militaries to pursue certain types of innovation while creating resistance to others. As such, this dissertation sheds important light on the ways in which the characteristics of military organizations can shape the agency and decisions of those implementing an innovation principle.

[76] This is broadly compatible with works on bureaucratic politics. See: Graham Allison and Morton Halperin, "Bureaucratic Politics: A Paradigm and Some Policy Implications," *World Politics* 24, no. 1 (1972): 40–79; Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little Brown, 1971); Morton Halperin, Priscilla Clapp, and Arnold Kanter, *Bureaucratic Politics and Foreign Policy*, 2nd ed. (Washington, D.C.: Brookings Institution Press, 2006); Grauer, "Moderating Diffusion: Military Bureaucratic Politics and the Implementation of German Doctrine in South America, 1885-1914."

[77] Although hinted at, this dynamic has not been rigorously explored. See: Goldman, "Introduction: Military Diffusion and Transformation," 15–16.

[78] On this debate, see: Grissom, "The Future of Military Innovation Studies"; Stuart Griffin, "Military Innovation Studies: Multidisciplinary or Lacking Discipline?," *Journal of Strategic Studies* 40, no. 1–2 (2017): 196–224. For individual positions, see: Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca and London: Cornell University Press, 1984); Kimberly Marten Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955-1991* (Princeton, New Jersey: Princeton University Press, 1993); Deborah D. Avant, "The Institutional Sources of Military Doctrine: Hegemons in Peripheral Wars," *International Studies Quarterly* 37, no. 4 (1993): 409–30; Jack Snyder, *Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca: Cornell University Press, 1984); Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*.

Second, I advance a stage-based conception of implementation for diffusion frameworks and showcase the value of stage-based theorizing. I assert that the implementation dynamic process is comprised of five stages: pre-adoption, introduction, modification, expansion, and full implementation. This framework can account for both partial adoption (introduction) as well as more comprehensive adoption efforts that include institutionalization (full implementation). This also provides as way to assess changes to an innovation during implementation (modification) as well as the degrees to which an innovation is implemented over time (expansion). This framework is particularly important for understanding how innovation principles are implemented across the diffusion process.

Third, this dissertation introduces new methodological tools for testing stage-based hypotheses about adoption and implementation. Specifically, this dissertation utilizes multistate survival modeling to assess variable effects at each stage of the implementation process. The methods used for testing hypotheses must mesh with the assumptions behind different frameworks. In the case of the stage-based framework advanced by this dissertation, traditional modeling techniques—such as logistic regressions (logit and probit) and basic survival modeling—prove both cumbersome and inadequate for assessing stage-based processes. Moreover, the stage-based framework highlights the importance of qualitative case studies, and particularly negative cases to explore why some countries are more likely to move through some implementation stages but less likely to experience others.[79]

[79] On negative cases, see: James Mahoney and Gary Goertz, "The Possibility Principle: Choosing Negative Cases in Comparative Research," *American Political Science Review* 98, no. 4 (November 2004): 653–69.

Research Design

This dissertation is an exercise in theory development to highlight the importance of organizational size in understanding implementation dynamics. As such, the dissertation has three analytical goals: (1) establish that cyber forces are spreading across the globe and that considerable variation exists in cyber force structure both across and within states; (2) illuminate the overall and stage-specific effects of military size on implementation; and (3) construct causal narratives to probe, identify, and differentiate theorized mechanisms.

To these ends, this dissertation employs an integrated multi-method design.[80] The first stage consists of quantitative analysis. More specifically, it uses both a stratified Cox proportional-hazards model and a multistate survival model to assess the overall and stage-specific effects of organizational size, respectively. Although used extensively in epidemiology and biomedical studies,[81] multistate modeling remains rare in political science.[82] As an extension of Cox models,[83] multistate models can model a duration process comprised of multiple stages with a variety of process structures. Stages are defined based on failure events that a subject is at the risk of experiencing; these failure events represent transitions between stages.[84] Like stratified Cox models, multistate models allow transitions to have different underlying rates of

[80] For more on an integrated approach, see: Jason Seawright, *Multi-Method Social Science: Combining Qualitative and Quantitative Tools* (Cambridge, United Kingdom: Cambridge University Press, 2016).

[81] For a comprehensive overview of applying multistate models to these fields, see: Richard J. Cook and Jerald F. Lawless, *Multistate Models for the Analysis of Life History Data*, Monographs on Statistics and Applied Probability (Boca Raton, Florida: CRC Press, 2018).

[82] Several recent exceptions include: Benjamin T. Jones and Shawna K. Metzger, "Evaluating Conflict Dynamics: A Novel Empirical Approach to Stage Conceptions," *Journal of Conflict Resolution* 62, no. 4 (2016): 819–47; Kaitlyn Webster, "Rethinking Civil War" (Dissertation, Durham, Duke University, 2019); Christopher Barrie, "The Process of Revolutionary Protest: Development and Democracy in the Tunisian Revolution of 2010-2011" (Working Paper, August 28, 2018); Baris Ari, "Uncrossing the Rubicon: Transitions from Violent Civil Conflict to Peace" (Dissertation, University of Essex, 2018); Eric Min, "Cheaper Talk: The Changing Nature of Wartime Negotiation in the Post-1945 Order" (Working Paper, University of California, Los Angeles, October 6, 2018).

[83] For a basic overview of the logic behind Cox models, see: Janet M. Box-Steffensmeier and Bradford S. Jones, *Event History Modeling: A Guide for Social Scientists* (Cambridge: Cambridge University Press, 2004), 8.

[84] On how this approach differs from competing risks models, see: Shawna K. Metzger and Benjamin T. Jones, "Surviving Phases: Introducing Multistate Survival Models," *Political Analysis* 24 (2016): 457–77.

occurrence by permitting baseline hazards to vary across transitions. Unlike stratified Cox models, multistate models allow for transition-specific covariates and can thus capture the theoretically differential impact of independent variables at different stages.[85] For quantitative modeling, I introduce a custom-created database of cyber forces worldwide: the Dataset on Cyber Force Structures (DCFS).

The second stage consists of qualitative analysis. This stage hinges on a series of within-case analyses across two militaries—the United States and Estonia—with a preliminary extension to a third, Germany, in the concluding chapter. Both the United States and Estonia represent extreme-on-the-X case selections based on the survival regressions: the U.S. military as an extremely large organization and the Estonian military as an extremely small organization. Because both the U.S. and Estonia represent extreme values of organizational size, they present useful cases for investigating and differentiating causal pathways as well as for assessing measurement error and potential omitted variable bias in my regressions.[86] Moreover, examining the implementation of cyber forces in these countries offers leverage over several key aspects of the project—namely, organizational size and implementation pathways—while theoretically controlling for common effects from the North Atlantic Treaty Organization (NATO). Allies can be a source of information about threats[87] and a source of pressures toward conformity.[88] NATO

[85] Metzger and Jones; Jones and Metzger, “Evaluating Conflict Dynamics: A Novel Empirical Approach to Stage Conceptions.” My approach follows Metzger and Jones (2016) and Jones and Metzger (2016) to satisfy the Markov assumption, i.e. all relationships and probabilities rest on the current stage of occupation and not the entire life history up to a given point.

[86] Seawright, *Multi-Method Social Science: Combining Qualitative and Quantitative Tools*, 92.

[87] Dan Reiter, “Learning, Realism, and Alliances: The Weight of the Shadow of the Past,” *World Politics* 46, no. 4 (July 1994): 490–526.

[88] James D. Morrow, “Alliances and Asymmetry: An Alternative to the Capability Aggregation Model of Alliances,” *American Journal of Political Science* 35, no. 3 (1991): 904–33; Victor D. Cha, “Powerplay: Origins of the U.S. Alliance System in Asia,” *International Security* 34, no. 3 (2010 2009): 158–96.

has also been an international leader in defining the strategic cyber-environment[89] and its members have been at the forefront of developing cyber capabilities.[90]

The evolution of U.S. cyber force structure presents three episodes for analysis: (1) the failed modification of U.S. cyber force structure with the rise and fall of U.S. Air Force Cyber Command (Provisional) from 2006 to 2008; (2) the expansion of the joint force approach into U.S. Cyber Command from 2008-2010; and (3) the elevation of U.S. Cyber Command to a fully unified combatant command (2010-2018). Two episodes are drawn from Estonia: (1) the delegation of cyber responsibilities to the Staff and Signals Battalion in the wake of the 2007 distributed denial of service incident (2007-2009); and (2) the creation of Cyber Command (2010-2018). The preliminary extension to Germany in Chapter 7 analyzes the establishment of the Cyber and Information Domain Service (2013-2017).

In each case study, my goal is to show how organizational size matters contingently with other likely explanations for cyber force implementation.[91] Accordingly, I sketch out two alternative explanations that have the potential to explain implementation dynamics within militaries: adoption-capacity and organizational culture. Along with organizational size, these alternative explanations are compatible with competitive diffusion and limit the scope-conditions of this dissertation to examine the internal implementation dynamics of military organizations. Although broader governmental dynamics and relationships, such as civil-military dynamics, are

[89] J. Burton, "NATO's Cyber Defense: Strategic Challenges and Institutional Adaptation," *Defence Studies* 15, no. 4 (2015): 297–319; Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017).

[90] D. Devai, "Proliferation of Offensive Cyber Weapons: Strategic Implications and Non-Proliferation Assumptions," *Academic and Applied Research in Military Science* 15, no. 1 (2016): 61–73.

[91] On the role of case studies for theory development and creating contingent generalizations, see: Alexander L. George and Andrew Bennett, *Cases Studies and Theory Development in the Social Sciences* (Cambridge and London: MIT Press, 2005), 111–15.

described to some degree in each of the case studies, a full analysis of theoretical explanations related to these issues remain outside the scope of this dissertation.

To evaluate how my argument performs and meshes with alternative explanations in each case, I employ the method of process tracing. This method allows researchers to examine causal process observations within a case to disconfirm or provide support for hypotheses derived from different theoretical explanations.[92] Process tracing links these alternative explanations to specific political, social, and psychological mechanisms, allowing the researcher to differentiate and evaluate causal mechanisms for a specific outcome of interest.[93] By connecting independent to dependent variables through an uninterrupted chain of events, process tracing establishes causal paths that directly link cause to effect.[94] Process tracing also ameliorates concerns over endogeneity by examining the timing and sequencing of causal forces[95] This method is ideal for this project for two main reasons. First, process tracing is a necessary step for detecting omitted variable bias and assessing measurement error in my survival regressions.[96] Second, because a limited number of case studies are proposed, and controlling for all individual case differences for comparisons is nearly impossible,[97] within-case process tracing is needed to increase the number of comparable observable implications for assessing the relative strengths and

[92] Derek Beach and Rasmus Brun Pedersen, *Process-Tracing Methods: Foundations and Guidelines* (Ann Arbor: The University of Michigan Press, 2013); Andrew Bennett and Jeffrey T. Checkel, “Process Tracing: From Philosophical Roots to Best Practices,” in *Process Tracing: From Metaphor to Analytic Tool*, ed. Andrew Bennett and Jeffrey T. Checkel (Cambridge, United Kingdom: Cambridge University Press, 2015), 3–37.

[93] Matthew Evangelista, “Explaining the Cold War’s End: Process Tracing All the Way Down?,” in *Process Tracing: From Metaphor to Analytic Tool*, ed. Andrew Bennett and Jeffrey T. Checkel (Cambridge, United Kingdom: Cambridge University Press, 2015), 154.

[94] David Waldner, “What Makes Process Tracing Good?: Causal Mechanisms, Causal Inference, and the Completeness Standard in Comparative Politics,” in *Process Tracing: From Metaphor to Analytic Tool*, ed. Andrew Bennett and Jeffrey T. Checkel (Cambridge, United Kingdom: Cambridge University Press, 2015), 126–52.

[95] James Mahoney, “Process Tracing and Historical Explanation,” *Security Studies* 24, no. 2 (2015): 200–218; James Mahoney, Khairunnisa Mohamedali, and Christoph Nguyen, “Causality and Time in Historical Institutionalism,” in *The Oxford Handbook of Historical Institutionalism* (Oxford: Oxford University Press, 2016), 71–88.

[96] Seawright, *Multi-Method Social Science: Combining Qualitative and Quantitative Tools*.

[97] Seawright, 107–8.

weaknesses of each alternative explanation. For each case, I evaluate the theory of organizational size, adoption-capacity theory, and organizational cultural logics with a combination of historical data, original interview data, and data generated from recently declassified government documents.

Plan of the Dissertation

The remaining chapters of this dissertation proceeds as follows. Chapter 2 provides an empirical overview of the diffusion of cyber forces and cyber force structures. Specifically, this chapter provides a conceptual foundation for assessing cyber force structures and establishes that the empirical variation in cyber force structures constitutes as process of principle diffusion. Chapter 3 develops my theoretical framework. This chapter advances a novel conceptualization of implementation, describes the major implementation tension surrounding cyber forces, and details the logic of organizational size that underpins my theoretical framework and offers several hypotheses. This chapter also outlines two major competing explanations. Chapters 4 through 6 offer empirical analysis. Chapter 4 presents statistical analysis; the results from both a stratified Cox model and a multistate survival model provide support for my theoretical claims; importantly, this chapter details how the implementation process relates to changes in cyber force structures. Chapters 5 and 6 provide case-based analysis of the evolution of cyber forces in the United States (Chapter 5) and Estonia (Chapter 6). For each case, I provide a brief overview of each military's implementation pathway and trace the changes in cyber force structure to evaluate the empirical validity of my theory and consider the relative explanatory power of the alternative explanations. Chapter 7 concludes the dissertation by summarizing the findings from Chapters 4 through 6 and assessing my theory against the competing explanations. This chapter also extends the framework to initially assess the development of Germany' cyber force structure, looks to future avenues of research opened by this dissertation, and closes by considering the broader academic and policy implications of the study.

CHAPTER 2

Cyber Force Structures:
Conceptualization and Evidence of Principle Diffusion

Introduction

This chapter makes three claims. First, contends that the global spread of cyber forces represents a process of diffusion. Second, this diffusion process is characterized by the lack of a dominant organizational model to guide the implementation of cyber forces. Third, because cyber forces have spread without a distinct model for implementation, this chapter makes the case that scholars must account for implementation dynamics to explain the structural variations in cyber forces.

To these ends, this chapter proceeds in four major sections. The first section defines cyber forces, while the second provides a conceptual foundation for assessing force structures. Third, this chapter advances a novel typology for classifying cyber force structures. The fourth section discusses the diffusion of cyber forces and provides an empirical overview of the growth of cyber forces across states over time. This overview shows that there is no distinct cyber force "blueprint" for states to follow. Instead, as evidenced by the variation in cyber force structures, cyber forces represent a common innovation principle that can be enacted in various ways. The chapter concludes by summarizing and looking to the theory chapter.

What Are Cyber Forces?

While existing definitions of cyber forces[1] provide an important foundation for this study, they nevertheless suffer from vague conceptual boundaries. Pernik (2018), for example, states that a cyber force "generally denotes a standalone structure, branch, or service of the armed forces that directs and controls the three main categories of cyberspace operations [defensive cyber space operations; intelligence, surveillance, reconnaissance cyberspace operations; and offensive operations]."[2] Similarly, Smeets (2019) asserts that "[a] military cyber organization is defined as a command, service, branch, or unit within a government's armed forces which has the authority and mission to conduct offensive cyber operations to disrupt, deny, degrade, and/or destroy (d4 effects)."[3] Both definitions indicate that cyber forces are (1) a kind of organization within the armed forces that (2) maintains some sort of authority over cyber operations (although Smeets' only applies to offensive operations).

A key problem with these and similar definitions is which organizations are excluded. Authority over cyber operations is a crucial delineator. Yet, not all cyber forces will have the mandate over the full spectrum of cyberspace operations (as advanced by Pernik). Additionally, not all cyber forces will have the full capability to undertake offensive operations as laid out by Smeets. Moreover, it is not clear what organizational structures count as cyber forces: both Pernik and Smeets are generally agnostic as to the strategic, operational, or tactical ends pursued by organizations. As such, existing definitions have amorphous conceptual boundaries that are problematic for distinguishing force structures.

[1] Several studies have used the terms "military cyber organizations" or "cyber commands." However, I use "cyber forces" to better facilitate the subsequent discussion of force structures, i.e., "cyber force structure" is more concise than "military cyber organization force structure" and more precise than "cyber command structure." Thus, cyber forces, military cyber organizations, and cyber commands may be used interchangeably.
[2] Pernik, "Preparing for Cyber Conflict: Case Studies of Cyber Command," 2–3.
[3] Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," 165.

To remedy these shortcomings, I assert that ***cyber forces are active-duty military organizations that possess the capability and authority to direct and control strategic computer network operations (CNOs) to impact, change, or modify strategic diplomatic and military interactions between entities***.[4] Computer network operations encompass three types of operations in the cyber domain:

(1) Computer network ***defense*** (CND), which includes operations intended to the prevent compromises to the integrity, confidentiality, or availability—through theft, infiltration, disruption, denial, degradation, or destruction—of information on computers or the computers or networks themselves;

(2) Computer network ***exploitation*** (CNE), encompassing intelligence, surveillance, or reconnaissance (ISR) operations to collect information from an adversary's computers and networks that fall short of disrupting or destroying information; and

(3) Computer network ***attack*** (CNA), or actions taken through a network of computers to disrupt, deny, degrade, or destroy another computer's information or the computers or networks themselves. Espionage and theft only constitute CNAs when information or systems are destroyed in the process.[5]

Importantly, this definition of cyber forces excludes three types of organizations with similar missions.

The first exclusion is civilian defense intelligence agencies such as the United States' National Security Agency (NSA). While there may be significant overlap in cyberspace operations between civilian intelligence agencies and military cyber forces, the primary purposes of these organizations are fundamentally different. Aside from falling outside military chains of command, civilian intelligence agencies are largely focused on information collection. Although cyber forces (such as military intelligence units) can and do collect information, they prioritize

[4] On the impact of computer network operations (i.e. cyber-attacks) on strategic interactions, see: Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*.
[5] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 279–80; Pernik, "Preparing for Cyber Conflict: Case Studies of Cyber Command," 4.

strategic advantage over intelligence-gathering so that intelligence-gathering is in service of and subordinated to gaining strategic advantages.

Second, this definition excludes military cyber-defense organizations comprised purely of reservists.[6] It is true that the integration of reservist and active-duty components is an important component of constructing an effective cyber force,[7] and the use of reservists can entail several benefits. Because the cyber mission is non-traditional, reserve personnel may perform official mission tasks in their capacity as reserves during peacetime like their active-duty counterparts.[8] Additionally, reservists offer a ready pool of personnel with advanced training that is usually obtained in the private sector. They also have ties to communities that can be leveraged to assist state and local agencies.[9]

Although reservist components can (and do) fulfill many of the same duties as active-duty components, their operation is conditional on legal activation, and they do not maintain full-time authority over CNOs. The scope of reservists is further complicated by the ambiguity of cyber conflict and the subsequent formulation of criteria for activating reserves.[10] Despite being a formal component of the military, reservists are volunteers who primarily work in the private or civilian government sectors and hence only serve for limited periods of time.[11] As such,

[6] For a comprehensive comparative look at the use of cyber reserves, see: Marie Baezner, "Study on the Use of Reserve Forces in Military Cybersecurity: A Comparative Study of Selected Countries" (Zurich, Switzerland: Center for Security Studies, ETH Zurich, March 4, 2020), https://doi.org/10.3929/ethz-b-000413590.

[7] Pernik, "Preparing for Cyber Conflict: Case Studies of Cyber Command," 27–28.

[8] Reservists may also (and usually do) have civilian jobs that involve tasks and skillsets that mirror the tasks and skillsets required by active-duty operations. Drew Miller, Daniel B. Levine, and Stanley A. Horowitz, "A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber Missions" (Alexandria, Virginia: Institute for Defense Analyses, September 2013).

[9] Miller, Levine, and Horowitz; Joseph A. Papenfus, "Total Army Cyber Mission Force: Reserve Component Integration" (Master's Thesis, Maxwell Air Force Base, Alabama, Air War College, 2016).

[10] Susan W. Brenner and Leo L. Clarke, "Conscription and Cyber Conflict: Legal Issues," in *2011 3rd International Conference on Cyber Conflict*, ed. C. Czosseck, E. Tyugu, and T. Wingfield (Tallinn, Estonia: CCD COE Publications, 2011), 1–12.

[11] Scott D. Applegate, "Leveraging Cyber Militias as a Force Multiplier in Cyber Operations" (Fairfax, VA: Center for Secure Information Systems, George Mason University, 2012).

reservist organizations are far more fluid than active-duty units. This fluidity can compromise the up-to-date knowledge of operations, scalability, and interoperability required of active-duty organizations.[12] For reservists to function like active-duty components, there must be substantial volunteering past minimum service requirements, an assumption that is unlikely to hold across militaries. Many governments also maintain legal restrictions on the use of reserve funds for operational missions.[13] Therefore, while states may use reservist units in lieu of forming active-duty cyber organizations, reservists do not meet the criteria for cyber forces. Excluded organizations include: Bulgaria's Cyber Defense Unit under the Armed Forces Reserve, Estonia's Cyber Defense Unit of the Estonian Defense League, and Latvia's Cyber Defense Unit of the National Armed Forces.[14]

Finally, military computer emergency readiness teams (MilCERTs), computer incident response teams (MilCIRTs), and computer incident response centers (MilCIRCs) are excluded. These organizations—such as the Jordanian Armed Forces' MilCERT and Moldovan Armed Forces' MAFCIRC[15]—are purely incident response teams that look for and patch military and/or defense network vulnerabilities, develop plans to deal with network outages and malicious attacks, and coordinate appropriate responses [16]. MilCERTs and MilCIRTs work at the tactical

[12] Miller, Levine, and Horowitz, "A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber Missions"; Gregg Curley, "The Provision of Cyber Manpower: Creating a Virtual Reserve," *MCU Journal* 9, no. 1 (Spring 2018): 191–217.

[13] Miller, Levine, and Horowitz, "A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber Missions."

[14] Matteo Gramaglia, Emmet Tuohy, and Piret Pernik, "Military Cyber Defense Structures of NATO Members: An Overview," Background Paper (Tallinn, Estonia: International Centre for Defence and Security (RKK/ICDS), December 2013); Anna-Maria Osula, "National Cyber Security Organisation: Estonia" (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015); Gederts Gelzis, "Latvia Launches Cyber Defence Unit to Beef Up Online Security," *Deutsche Welle*, March 4, 2014, https://www.dw.com/en/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936.

[15] North Atlantic Treaty Organization, "NATO Supports Jordan's National Cyber Defence Strategy," July 19, 2017, https://www.nato.int/cps/en/natohq/news_146287.htm; Adriana Lins de Albuquerque and Jakob Hedenskog, "Moldova: A Defence Sector Reform Assessment" (Stockholm, Sweden: Swedish Defence Research Agency, December 2016), https://www.foi.se/rest-api/report/FOI-R--4350--SE.

[16] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 279.

level to ensure network operability but they do not seek to integrate capabilities on larger operational or strategic scales. While they can be under the control of or report to cyber forces, MilCERTs and MilCIRTs themselves do not constitute cyber forces.

Conceptualizing Cyber Force Structure

Traditional military force structures generally refer to the number and types of combat units that a military can generate and sustain. The central components of force structure have been defined in a number of ways: the composition and structure of organizations; unit functions; capabilities; the costs of operation; or some combination of these factors.[17] However, many of these aspects of force structure become ambiguous when applied to cyber forces. Table 2.1 highlights the problematic nature of mapping traditional force structure categories onto cyber forces.

Unlike the individual unit functions of traditional combat forces in the land, sea, and air domains, the operational functions of cyber forces—CNE, CND, and CNA—are nearly indistinguishable. Both attacks on an adversary's network (CNA) and the defense of one's own network (CND) rest on intrusions into an adversary's networks for intelligence collection (CNE). Moreover, network exploitation, defense, and attack use similar tools and techniques. Thus, at an operational level, unit functions necessarily overlap and are operationally indistinguishable.[18]

Cyber force capabilities are also difficult to quantify. Although human capital can be quantified to some degree—in terms of total personnel and their respective qualifications—the technological dimensions of capabilities remain nearly impossible to assess quantitatively.

[17] Congressional Budget Office, "The U.S. Military's Force Structure: A Primer" (Washington, D.C.: Congress of the United States, July 2016). For various operationalizations of these concepts, see: Iztok Prezelj et al., "Quantitative Monitoring of Military Transformation in the Period 1992-2010: Do the Protagonists of Transformation Really Change More than Other Countries?," *Defence Studies* 16, no. 1 (2016): 20–46.
[18] Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*, 15–96.

Table 2.1. Mapping Traditional Force Structure Components onto the Cyber Mission

	Function	Capabilities	Structure/Composition of Units	Costs of Operation
Land Forces*	Clearly differentiated. Distinct functions include: armored combat, armored personnel carrier, infantry, aviation, special operations.	Quantifiable. Example: the number of armored tanks.	Assessed according to the number of units and the direct and indirect military personnel per unit.	Total of the direct, indirect, and administrative/overhead personnel and O&S costs.
Maritime Forces*	Clearly differentiated. Distinct functions include: Aircraft carrier, surface combat, attack submarines, amphibious ships, amphibious infantry, special operations.	Quantifiable. Example: the number of aircraft carriers.	Assessed according to the number of units and the direct and indirect military personnel per unit.	Total of the direct, indirect, and administrative/overhead personnel and O&S costs.
Air Forces*	Clearly differentiated. Distinct functions include: Tactical aviation, bombers, airlift, refueling, unmanned air systems, special operations.	Quantifiable. Example: the number of long-range bomber planes.	Assessed according to the number of units and the direct and indirect military personnel per unit.	Total of the direct, indirect, and administrative/overhead personnel and O&S costs.
Cyber Forces	**Unable to differentiate.** **CND, CNE, CNA are rarely operationally distinct functions.**	**Difficult to Quantify.** **Capabilities rest on “weapons” that are largely transitory.**	**Difficult to Assess.** **Possible to count units, but nature of direct and indirect personnel remains unclear.**	**Largely Unknown.** **Direct personnel costs provide only concrete insight but remain unreliable.**

*Information on land, maritime, and aviation force structures taken from Congressional Budget Office, “The U.S. Military’s Force Structure: A Primer” (Washington, D.C.: Congress of the United States, July 2016).

Instead of tangible weapons systems (missiles, tanks, submarines, etc.) that have multiple-use ability and can be counted, cyberweapons are comprised of largely digital, transitory elements that have only a temporary ability to access and attack computer networks and systems.[19] An adversary can detect and patch vulnerabilities after a cyberweapon has been used; the attacker's capability also rapidly diffuses to other actors, where it can be modified and redeployed against the original attacker.[20]

The nature of cyber force personnel further complicates force structure assessments: there is no clear distinction between direct "combat" personnel and indirect "support" personnel. Traditional roles played by indirect personnel—such as signals intelligence—are at the heart of network operations for cyber forces' direct personnel. More problematically, data regarding personnel costs, operating costs, and capability acquisitions tend to be inconsistent across countries, with much information remaining classified and unavailable.[21]

Accordingly, I use two criteria for categorizing cyber force structures: (1) the organizational model for command structures and (2) the scale of command over computer network operations. These are two broad, visible dimensions of military organizations that help to define the membership, responsibilities, capacity, and interactions of subsystems in organizations.[22] They provide initial (if imperfect) proxies for assessing the structure of cyber forces and their potential operating costs (i.e., all things equal, larger scales of command should entail higher resource requirements).

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

[20] Benjamin Buchanan, "The Life Cycles of Cyber Threats," *Survival* 58, no. 1 (2016): 39–58.

[21] On the problematic nature of cyber conflict data, see: Christopher Whyte et al., "Rethinking the Data Wheel: Automating Open-Access, Public Data on Cyber Conflict," in *CyCon X: Maximising Effects* (2018 10th International Conference on Cyber Conflict, Tallinn, Estonia: NATO CCD COE Publications, 2018), 9–30.

[22] W. Richard Scott, *Organizations: Rational, Natural, and Open Systems*, Fourth Edition (New Jersey: Prentice-Hall, Inc., 1998), 89–92, 153–94.

First, cyber forces can be organized according to one of three models: a branch model, a service model, or a joint model. As open-system organizations bound together by institutional rules and collective beliefs, militaries are comprised of multiple, interdependent subsystems.[23] These three models provide different arrangements to locate cyber forces within military subsystems (combat or combat support[24]) and define the number of combat services to be included in the cyber force structure.

Under a *branch model*, authority for computer network operations rests primarily in logistical branches, military intelligence agencies, or signals corps that provide specialized, operational assistance to combat subsystems.[25] As part of the combat support subsystem, they are independent from the control of the combat services.[26] Although the combat services can provide personnel to staff cyber forces in the combat support subsystem, forces in this subsystem fall outside the chain of command of service departments. As such, the branch model has a non-service command structure.

Under both the *service* and *joint* models, cyber forces are part of the combat subsystem and are subordinate to existing service structures or appear as an independent service or combatant commands. In the combat subsystem, entities are traditionally tasked with the application of kinetic force through the employment of weapons systems against adversaries.

[23] Goldman, "Introduction: Military Diffusion and Transformation," 16; Scott, *Organizations: Rational, Natural, and Open Systems*, 82–100; Theo Farrell, "Figuring Out Fighting Organisations: The New Organisational Analysis in Strategic Studies," *Journal of Strategic Studies* 19, no. 1 (1996): 122–35.

[24] Combat, combat support, and combat services support are the primary subsystems within military organization. Here, I exclude the combat services support subsystem as combat services support generally refers to administrative roles that support readiness such as acquisitions, transportation, and medical services. Congressional Budget Office, "The U.S. Military's Force Structure," 8–9. For consistency, I employ the combat/combat support/combat services support terminology utilized by the U.S. Army. For an example of this practice, see: Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton and Oxford: Princeton University Press, 2006).

[25] Congressional Budget Office, "The U.S. Military's Force Structure: A Primer," 9–10.

[26] While combat support elements are necessarily present within combat subsystems, combat represents the dominant, overarching functional role for that subsystem.

This subsystem is generally comprised of distinct departments (or commands) for domain-based services (Army, Navy, or Air Force) or other functional combat service branches (such as Rocket Forces or Marines).[27] Cyber forces are organized according to a *service model* when a single combat service retains primary authority for computer network operations. A *joint model* entails the shared distribution of authority over computer network operations across two or more combat services.

The second way to classify cyber force structures is according to the scale of command, which can be categorized as subordinated, sub-unified, or unified.[28] *Subordinated* cyber force structures represent the smallest scale of command: computer network operations are incorporated into existing combat or non-combat commands with only limited alterations. Subordinated force structures support existing missions, technologies, and operating procedures[29] to enhance effectiveness without disrupting the status quo.[30] *Sub-unified* cyber force structures consist of new, specialized cyber sub-organizations that treat computer network operations as an independent mission set. These force structures are usually the product of major reconfigurations of personnel and capabilities within the combat or non-combat subsystems to exploit new technologies or implement novel operational concepts.[31] However, they do not impact the values, beliefs, and power relationships across the entire military. *Unified* cyber force

[27] Although the combat services themselves could constitute a smaller subsystem within the combat subsystem, this level of analysis is below the focus of this typology.

[28] The scale of command also provides insight into the potential resources available and operational capacity of cyber forces.

[29] On the integration of novel practices into existing structures,, see: Farrell, “Improving in War: Military Adaptation and the British in Helman Province, Afghanistan, 2006-2009.”

[30] This categorization maps roughly onto discussions of first-, second-, and third-order changes in organizations. See: Kamalesh Kumar and Mary S. Thibodeaux, “Organizational Politics and Planned Organization Change: A Pragmatic Approach,” *Group & Organization Studies* 15, no. 4 (1990): 357–65; Karl E. Weick and Robert E. Quinn, “Organizational Change and Development,” *Annual Review of Psychology* 50 (1999): 361–86.

[31] Cheung, Mahnken, and Ross, “Frameworks for Analyzing Chinese Defense and Military Innovation,” 30.

structures institutionalize "new ways of war"[32] through the creation of a new branch, combat service, or combatant command to coordinate or integrate efforts in the cyber domain. These force structures generally emerge from a process of sustained innovation and military-wide reorganization that disrupts existing command arrangements by altering the values, beliefs, and interdependencies across multiple subsystems.[33]

A Typology of Cyber Force Structures

These two criteria—organizational model and scale of command—produce nine distinct cyber force structures: (1) Subordinated Branch; (2) Subordinated Service; (3) Subordinated Joint; (4) Sub-Unified Branch; (5) Sub-Unified Service; (6) Sub-Unified Joint; (7) Unified Branch; (8) Unified Service; and (9) Unified Joint. Table 2.2 summarizes this typology.

Subordinated Branch cyber force structures fulfil logistical and/or intelligence functions by integrating computer network operations into the existing command structures of independent communications divisions, signals intelligence units, or larger military intelligence agencies. Examples include: Israel's Unit 8200, an electronics intelligence unit established in the 1950s (subordinate to the Israeli Intelligence Corps in the Israeli Defense Forces Directorate of Military Intelligence) that has been tasked with conducting CNOs; and Estonia's Strategic Communications Center, a unit formerly subordinated to the independent Staff and Signals Battalion that was tasked with carrying out network operations.[34]

[32] The lessons, beliefs, and practices regarding new technological and mission environments. Rosen, *Winning the Next War: Innovation and the Modern Military*.

[33] On military transformation, see: Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions"; Stulberg, Long, and Salomone, *Managing Defense Transformation: Agency, Culture and Service Change*, 16; Terry Terriff, Frans Osinga, and Theo Farrell, eds., *A Transformation Gap? American Innovations and European Military Change* (Stanford, California: Stanford University Press, 2010).

[34] James Andrew Lewis and Gotz Neuneck, "The Cyber Index: International Security Trends and Realities" (New York and Geneva: United Nations Institute for Disarmament Research, 2013); Osula, "National Cyber Security Organisation: Estonia."

Subordinated Service force structures emerge when a single combat service co-opts the CNO mission into existing electronic warfare, signals, or communications units and no other combat services have the capability or mandate to conduct CNOs. The Danish Army's 3rd Electronic Warfare Company from 2009 to 2012 and the Armed Forces of the Philippines' Signals Corps subordinate to the Filipino Army from 2016 to the present provides examples of single-service units with primary responsibilities for cyber operations.[35]

Subordinated Joint structures coordinate the CNO mission when responsibilities are distributed across multiple (more than two) combat services. They are not new sub-organizations; instead, they primarily take on the form of a temporary, issue- or mission-driven joint task force. States with these force structures include the United States from 2001 to 2010[36] and France (Cyber Defense Cell) from 2011 to 2015.[37]

Sub-Unified Branch cyber force structures result from the creation of new divisions or directorates under military intelligence agencies, communications or information systems agencies, or joint staff support directorates. Examples include the Finnish Cyber Defense Division (2015-present) and the Cyber Security Operations Center under the Belgian Military Intelligence Service (2017-present).[38]

[35] "Chapter Four: Europe," *The Military Balance*, 2013; Gilbert P. Felongco, "Philippine Armed Forces Build Up Capability to Fight in Cyberspace," *Gulf News*, November 23, 2016, https://gulfnews.com/world/asia/philippines/philippine-armed-forces-build-up-capability-to-fight-in-cyberspace-1.1934044.

[36] As will be discussed in Chapter 5, Joint Structures for the U.S. include the Joint Task Force – Computer Network Operations (JTF-CNO) from 2001-2004, the Joint Task Force – Global Network Operations (JTF-GNO) in 2004, and the Joint Functional Component Command – Network Warfare (JFCC-NW) from 2005-2010. U.S. Cyber Command, "U.S. Cyber Command History," n.d., https://www.cybercom.mil/About/History/;

[37]Pascal Brangetto, "National Cyber Security Organisation: France," National Cyber Security Organisation (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015).

[38] Pernik, "Preparing for Cyber Conflict"; Kenneth L. Lasoen, "Belgian Intelligence SIGINT Operations," *International Journal of Intelligence and CounteriIntelligence* 32, no. 1 (2019): 1–29.

Table 2.2. A Typology of Cyber Force Structures

	Scale of Command		
	Subordinated	Sub-Unified	Unified
Organizational Model			
Branch Model	(1) Subordinated Branch *Israel (1950s-present)* *Estonia (2009-2018)*	(4) Sub-Unified Branch *Finland (2015-Present)* *Belgium (2017-Present)*	(7) Unified Branch *Estonia (2018-Present)* *Norway (2012-Present)*
Service Model	(2) Subordinated Service *Denmark (2009-2012)* *Philippines (2016-Present)*	(5) Sub-Unified Service *Brazil (2017-Present)* *Nigeria (2018-Present)*	(8) Unified Service *Germany (2017-Present)* *China (2016-Present)*
Joint Model	(3) Subordinated Joint *France (2011-2015)* *U.S. (2001-2010)*	(6) Sub-Unified Joint *U.S. (2010-2017)* *Italy (2017-Present)*	(9) Unified Joint *U.S. (2017-Present)* *Netherlands (2018-Present)*

Sub-Unified Service force structures manifest as new major commands within a single combat service specifically for conducting cyber operations. By reorganizing service personnel and capabilities, this force structure places CNOs at the same hierarchical level as existing service commands and their missions. Although it can be staffed with personnel from other combat services, a Sub-Unified Service structure is under the command of and subordinated to only one combat service. Brazil's Cyber Defense Command (2017-Present) and Nigeria's Cyber Warfare Command (2018-Present) are commands subordinated to the respective armies. Nigeria's command consolidates previous efforts within the Army into a new service command; Brazil's Cyber Defense Command incorporates personnel from the Army, Navy, and Air Force under the sole authority of the Army.[39]

Sub-Unified Joint cyber force structures report to an existing joint unified combatant command but significantly expand the scope of operations for that parent command. Unlike Subordinated Joint structures, Sub-Unified Joint force structures are necessarily comprised of service-level component commands (i.e., at least two services have developed service-level major commands). Both the United States' Cyber Command from 2010-2017 (subordinate to United States Strategic Command) and Italy's Joint Command for Cyberspace Operations (2017-present, subordinate to the Joint C4 Defense Command) fall in this category.[40]

There are three unified cyber force structures: Unified Branch, Unified Service, and Unified Joint. A *Unified Branch* force structure is an independent non-combat military branch

[39] Taciana Moury, "Brazilian Army Invests in Cyber Defense," *Dialogo*, May 12, 2017, https://dialogo-americas.com/en/articles/brazilian-army-invests-cyber-defense; Kingsley Omonobi-Abuja, "Nigerian Army's Cyber Warfare Command Begins Operation," *Vanguard*, August 29, 2018, https://www.vanguardngr.com/2018/08/nigerian-armys-cyber-warfare-command-begins-operation/.

[40] U.S. Cyber Command, "U.S. Cyber Command History"; Italian Ministry of Defence, "Il Sottosegratario Tofalo visita il Comando C4 Difesa e il CIOC [Undersecretary Tofalo visits the C4 Defense Command and the CIOC]," August 1, 2018, https://www.difesa.it/Primo_Piano/Pagine/Il-Sottosegretario-Tofalo-visita-il-Comando-C4-Difesa-e-il-CIOC.aspx.

that holds special armament or battle equipment to conduct missions in the cyber domain. Examples include Estonia's Cyber Command (2018-present) and Norway's Cyber Defence Force (2012-present).[41] *Unified Service* structures hinge on the creation of a new, domain-specific combat service (with a new military department) that receives the same hierarchical standing as other domain-based services (armies, navies, and air forces). Only China's Strategic Support Force (established in 2016) and Germany's Cyber and Information Domain Service (established in 2017) have attained this force structure.[42] *Unified Joint* cyber force structures coincide with the formation of an independent, unified combatant command for the cyber domain that is comprised of at least two service-level component commands. These structures are not subordinated to another combatant command, but instead report directly to the top civilian defense official (via the combatant commander). Examples include United States Cyber Command from 2017 to the present and the Defense Cyber Command in the Netherlands from 2018-present.[43]

The Diffusion of Cyber Forces in Principle

Cyber forces have emerged in every region of the world. However, no clear pattern has emerged among states in terms of creating actual force structures. As discussed in the previous chapter, few military diffusion studies specify whether the innovation under examination entails specific policy instruments and a blueprint for implementation or represents a broader principle. In the case of the former—i.e. "model diffusion"—innovators export a specific incarnation of a new

[41] Estonian Defence Forces, "Cyber Command," n.d., http://www.mil.ee/en/landforces/Cyber-Command; Ministry of Defense of Norway, "Cyberforsvaret offisielt etablert i dag [Cyber Defence Force officially established today]," September 18, 2012, https://www.regjeringen.no/no/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/Nyheter/2012/cyber/id699271/.

[42] "Chapter Six: Asia," *The Military Balance*, 2019; Pernik,"Preparing for Cyber Conflict Command."

[43] U.S. Cyber Command, "U.S. Cyber Command History"; Kaska, "National Cyber Security Organisation: The Netherlands."

technological application, policy paradigm, or an institutional design. By and large, adopters replicate the original innovation model.

Yet, many issue areas—such as the cyber mission and computer network operations—are complex, and do not lend themselves to a single, comprehensive innovation model. In these cases, general principles of innovation emerge that can encompass a multitude of permutations. As such, "principle diffusion" provides broad maxims of innovation that give direction to decisionmakers but do not prescribe specific courses of action for innovation.[44] Therefore, diffusion patterns of cyber forces should indicate that: (1) cyber forces have spread across a large number of states; (2) there is variation in the institutional characteristics of cyber forces, i.e. variation in the cyber force structures; and (3) no dominant cyber force model has emerged over time.

Cyber Forces in the World, 2000-2018

To assess the principle diffusion of cyber forces, I use evidence from a custom-created database: The Dataset on Cyber Force Structures (DCFS). The Dataset on Cyber Force Structures catalogues the evolution of cyber forces and force structures for all United Nations (UN) members with an active military force from 2000 to 2018. An active military force is a necessary precondition for inclusion into the dataset: there can be no cyber force without an active military. As such, the DCFS surveys 172 UN-member states and excludes the 21 member states that do not maintain an active military force.[45] The dataset utilizes five types of sources to code a country's cyber force structure over time: official government publications; reports produced by think tanks or international organizations; peer-reviewed academic works; news

[44] Weyland, *Bounded Rationality and Policy Diffusion: Social Sector Reform in Latin America*, 17–18.
[45] These are: Andorra, Costa Rica, Dominica, Grenada, Iceland, Kiribati, Liechtenstein, Marshall Islands, Mauritius, the Federated States of Micronesia, Monaco, Nauru, Palau, Panama, Saint Lucia, Saint Vincent and the Grenadines, Samoa, the Solomon Islands, Tuvalu, and Vanuatu.

articles from international and regional media outlets; and primary interviews conducted with former policymakers, military officials, industry members, and subject matter experts. For those states with a cyber force, the DCFS captures both the organizational model utilized and the scale of command. The changes in cyber force structure captured by the dataset will be discussed in more depth in Chapter 4. More detail about dataset sources and coding procedures is provided in Appendix 1 of this dissertation.

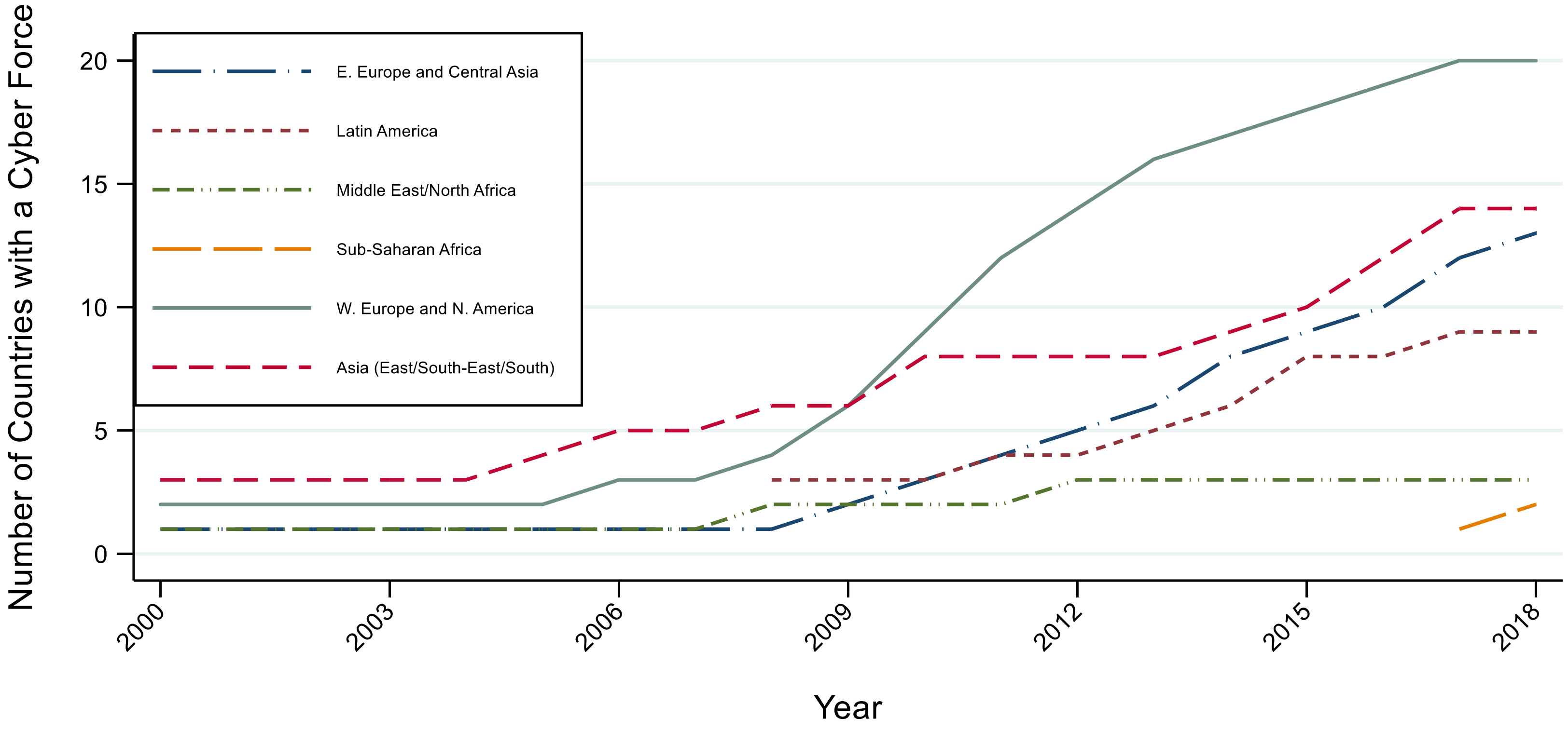
Figure 2.1 charts the spread of cyber forces according to politico-geographic region.[46] From 2000-2004, only seven countries (4.1% of all eligible countries) maintained cyber forces. These seven countries—the United States, Russia, China, Israel, North Korea, Greece, and Thailand—each had cyber forces prior to 2000.[47] By 2018, the number of states with a cyber force increased to 61 (35.5%). Western Europe and North America has experienced the most growth in the number of states with a cyber force—from two in 2000 to 20 states by 2018. Since 2000, Asia (South, South-East, and East Asia combined) has seen a total of 14 states create a cyber force.

Many of the developments outside these two regions have occurred post-2007. Both the Eastern Europe/Central Asia and Latin America regions have had consistent growth in cyber forces since 2007. With Russia as the only state with a cyber force from 2000-2008, by 2018 Eastern Europe/Central Asia was home to 13 militaries possessing a cyber force.

[46] Politico-geographic region coding is drawn from: Jan Teorell et al., “Measuring Polyarchy Across the Globe, 1900-2017,” *Studies in Comparative International Development* 54 (2019): 71–95.

[47] As such, there are observations for these countries that the dataset does not capture since they occur prior to the start of the dataset (making the dataset left-truncated).

Figure 2.1. The Growth of Cyber Forces by Region, 2000-2018



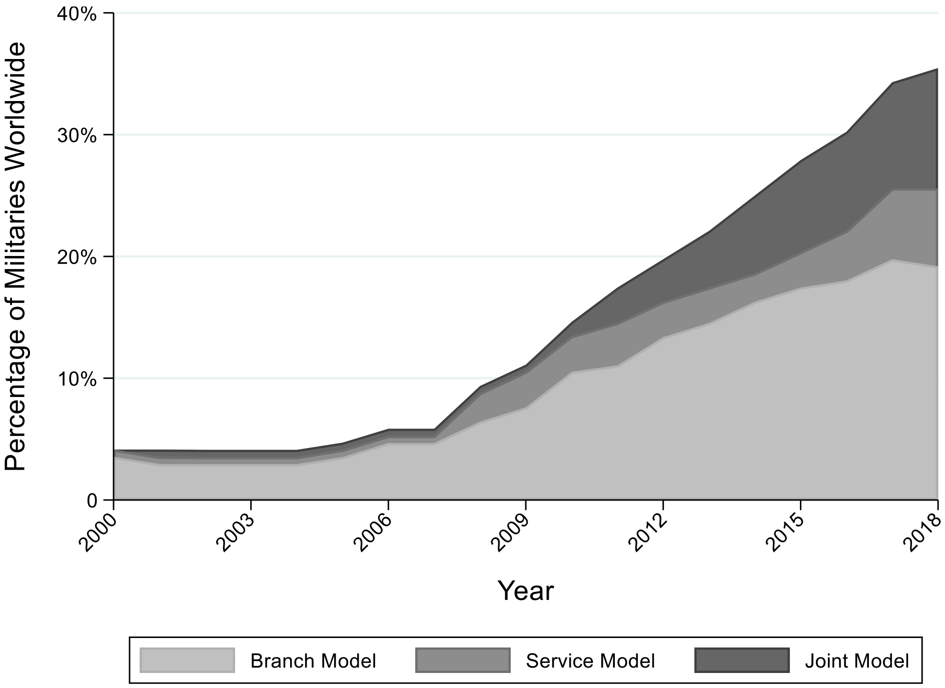
Source: The Dataset on Cyber Force Structures

Three countries created a cyber force in Latin America in 2008 (Argentina, Brazil, and Peru), and the region reached nine by 2018. The Middle East/North Africa (MENA) and Sub-Saharan Africa have seen the least amount of cyber force growth. In addition to Israel, Iran and Turkey have created formal cyber forces in the MENA region. South Africa and Nigeria are the only Sub-Saharan African countries to develop cyber forces.

Figure 2.2 provides insight into the growth of the Branch, Service, and Joint organizational models over time. Worth noting is the post-2007 surge in all three cyber force models. As mentioned in the description of Figure 2.1, Figure 2.2 portrays accelerated growth in the share of states developing cyber forces. In 2007, only 5.8 percent of states (10 total) had cyber forces. This increased to 35.5 percent of all states (61 states) by 2018 with an average growth rate of 2.7% per year (between four and five states each year) since 2007. Significantly, Figure 2.2 portrays increasing variation over time in the distribution of models. In other words, ***as the number of cyber forces has increased, so has the variation in organizational model***.

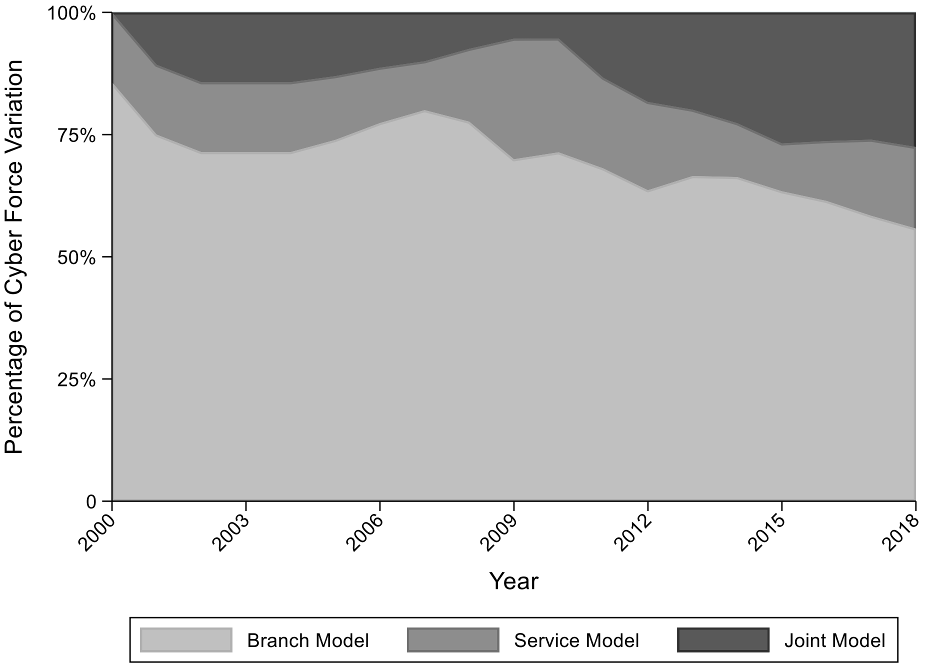
Figure 2.3 shows this trend more clearly. The Branch model accounted for roughly 75 percent of the variation in cyber forces until roughly 2008; this share decreased to approximately 55 percent by 2018. This 20 percent drop in the prevalence of the Branch model, coupled with fluctuations in the number of states utilizing the Service and Joint models, provides support for the diffusion of cyber forces in principle. Although the utilization of the Joint model has noticeable grown over time, the Joint model accounts for just over 25% over the variation in cyber forces and is by no means the dominant paradigm.

Figure 2.2. The Growth of Cyber Forces by Organizational Model, 2000-2018



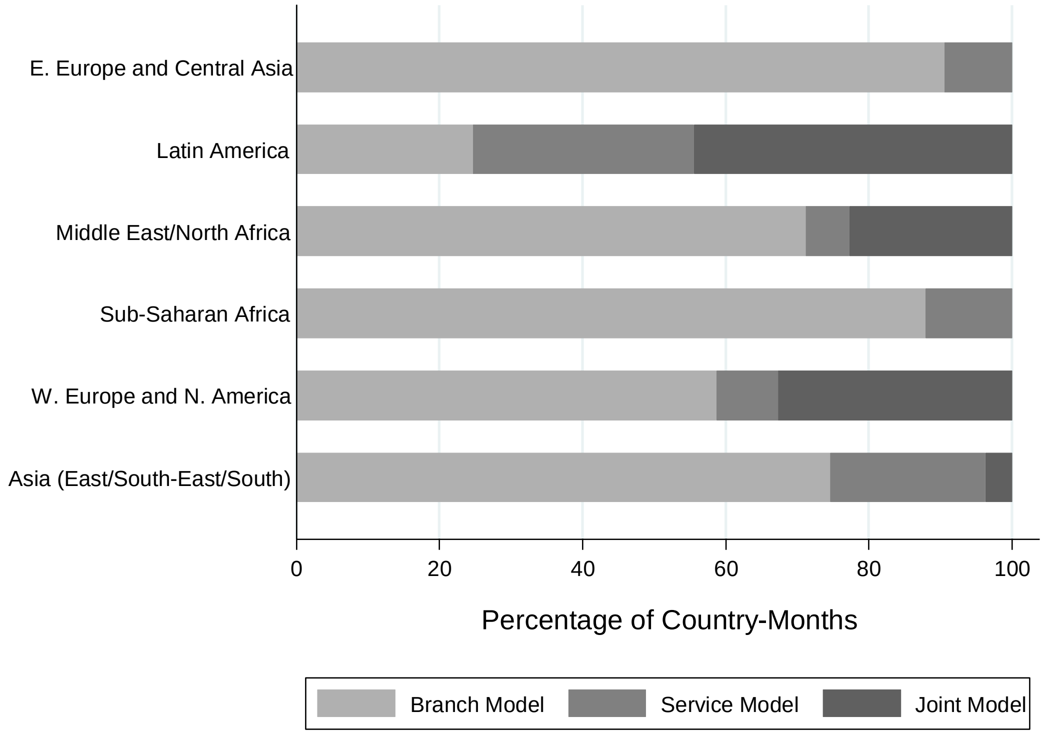
Source: The Dataset on Cyber Force Structures

Figure 2.3. The Distribution of Organizational Models across Cyber Forces, 2000-2018



Source: The Dataset on Cyber Force Structures

Figure 2.4. Distribution of Model by Region



Source: The Dataset on Cyber Force Structures

Geographic clustering has been a key feature in diffusion studies.[48] Figure 2.4 surveys the distribution of organizational model selection by region in country-months. Eastern Europe and Central Asia and Sub-Saharan Africa are the only two areas where the regional prevalence of the Branch model exceeds the international prevalence charted in Figure 2.3 above. The Branch model has accounted for roughly 90 percent of the country-months in Eastern Europe and Central Asia and slightly less than 90 percent in Sub-Saharan Africa. There does appear to be a dominant model emerging in these two regions; however, significant variation occurs in other

[48] For overviews of geographic dynamics and diffusion, see: Emily O. Goldman and Leslie C. Eliason, eds., *The Diffusion of Military Technology and Ideas* (Stanford, California: Stanford University Press, 2003); Berry and Berry, "Innovation and Diffusion Models in Policy Research."

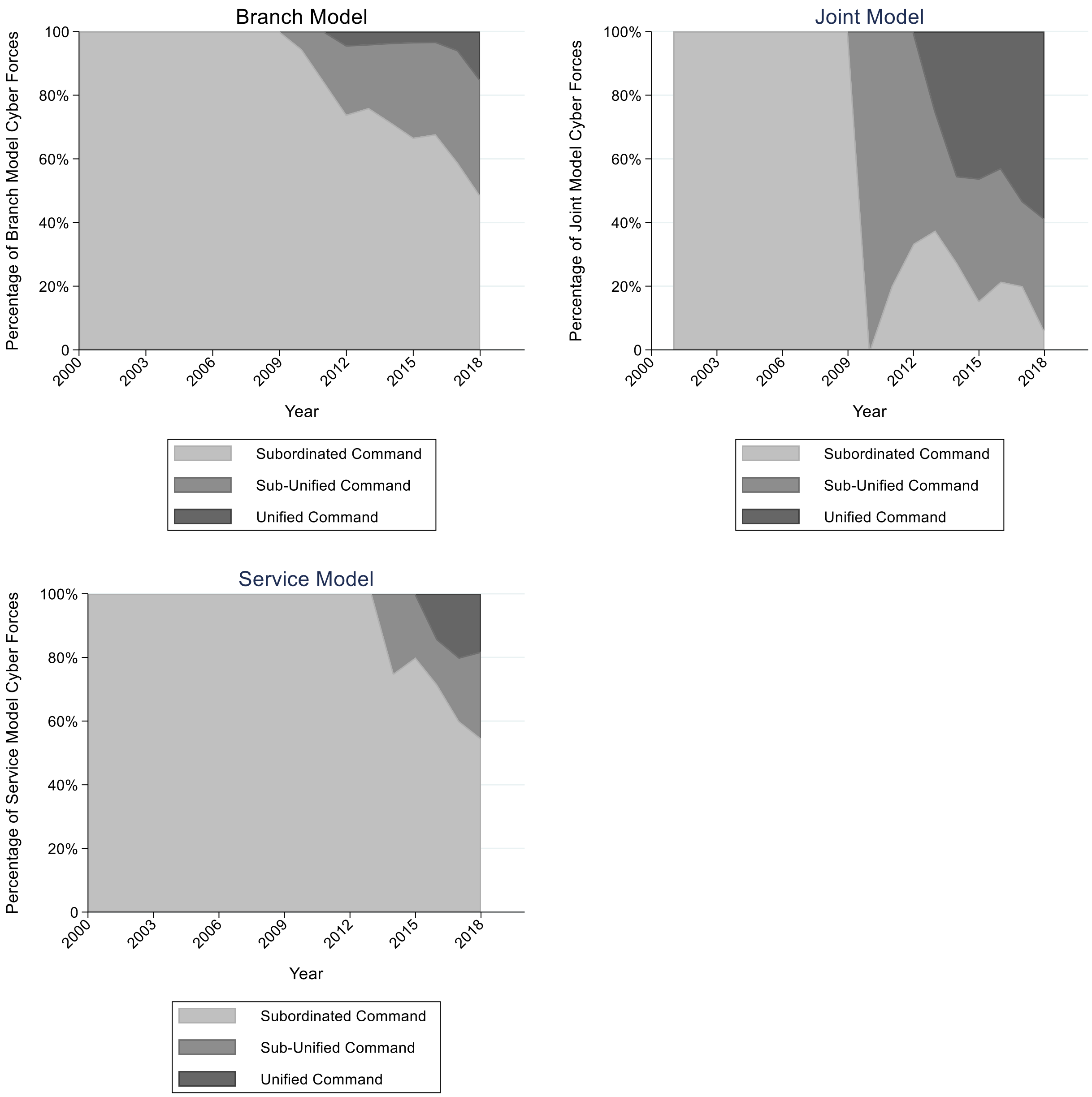
regions. This is particularly the case for Latin America, where the Branch model accounts for approximately 25 percent of the cyber force country-months and the Service and Joint models account for roughly 30 percent and 45 percent of country-months, respectively.

Finally, even across states using a similar organizational model, states have given cyber forces different scales of command. Table 2.3 and Figure 2.5 indicate that, while Subordinated command structures have been the most prevalent across all three organizational models over time, the variation in command scale increases significantly after 2009. The first Sub-Unified commands emerge in 2010, with one Sub-Unified Branch (South Korea's Cyber Command) and two Sub-Unified Joint (U.S. Cyber Command and Iran's Cyber Defense Command) force structures. The Netherlands' Cyber Defense Command represents the first Sub-Unified Service force structure in 2014. Across all three organizational models, Unified command structures only appear after 2012. In terms of command variation, both the Branch and Service models have experienced similar patterns. The Joint model has seen the most volatility in command over time.

Table 2.3. Number of Countries by Cyber Force Structure

		Year				
		2000	*2005*	*2010*	*2015*	*2018*
Model	**Command**					
Branch	Subordinated	6	6	17	20	16
	Sub-Unified	0	0	1	9	12
	Unified	0	0	0	1	5
Service	Subordinated	1	1	5	4	6
	Sub-Unified	0	0	0	1	3
	Unified	0	0	0	0	2
Joint	Subordinated	0	1	0	2	1
	Sub-Unified	0	0	2	5	6
	Unified	0	0	0	6	10
Countries with Cyber Force		7	8	25	48	61
Countries with No Cyber Force		162	162	146	124	111
Total Countries		169	170	171	172	172

Figure 2.5. Distribution of Command Scale by Organizational Model, 2000-2018



Conclusion

States across the globe have increasingly adopted cyber forces since 2000. However, no clear model for creating a cyber force has been at the center of diffusion; instead, states have adopted the general principle of a cyber force. As a result, many structural permutations—captured by the typology advanced in this chapter—have emerged across cyber forces over time. Yet, a crucial question remains: *why* have militaries implemented cyber forces in such different ways? The lack of a clear model for adoption provides an important precondition but cannot fully explain why militaries exhibit varying implementation dynamics. To address the question of implementation dynamics, the next chapter lays out a theory of organizational size that helps explain implementation priorities and pathways.

CHAPTER 3

Theorizing Implementation Dynamics: The Effects of Organizational Size

Introduction

In this chapter, I advance both a novel conceptual framework for understanding implementation dynamics and a theoretical explanation for why the implementation of cyber forces unfolds differently under different organizational conditions. The central claim is that the size of a military organization drives implementation efforts: implementers in larger military organizations are driven to initially prioritize bureaucratic integration of cyber forces over operational imperatives, while those in smaller militaries initially prioritize building capabilities over bureaucratic concerns. In this way, organizational size drives implementation priorities that alter implementation pathways.

This chapter proceeds in six major sections. The first discusses the importance of theorizing implementation as an extension of the diffusion process, particularly when innovations do not entail specific policy instruments or an implementation blueprint. The second section offers a framework for understanding implementation as a process comprised of multiple, discreet stages. I suggest that implementation has five stages: Pre-Adoption, Introduction, Modification, Reinvention, and Full Implementation. The third section pivots to explain the substantive challenges of implementing cyber forces. Specifically, I discuss the tension between implementing a new mission area and integrating cyber forces into the broader bureaucratic environment. Fourth, I lay out my key theoretical claims on the role of military size; this section presents several hypotheses. The fifth section sketches out two alternative explanations:

adoption-capacity and organizational culture. The chapter concludes by summarizing and looking forward to the ensuing empirical chapters.

Principle Diffusion and the Importance of Implementation

As detailed in the introductory chapter of this dissertation, few military diffusion studies specify whether the innovation under examination entails specific policy instruments and a blueprint for implementation or represents a broader principle. In the first instance, potential adopters are presented with a distinct innovation model; this model prescribes the adoption of certain policy instruments and entails information on how the innovation should be implemented. In the latter case, an innovation appears as general principle to be adopted, i.e. broad maxims of innovation that provide a general direction for policymakers but do not prescribe specific policy instruments or courses of action regarding implementation.[1]

As shown in Chapter 2, the diffusion of cyber forces is characterized by both spatial and temporal variation in cyber force structures: force structures vary both across states and within states as cyber forces evolve. More importantly, this variation shows that cyber forces have diffused as a general innovation principle. With no dominant force structure to be adopted, there is no clear cyber force "model" to be replicated. As such, and as will be detailed in Chapter 4, militaries have adopted a cyber force but have implemented force structures in a variety of ways. Although adoption decisions remain pertinent, the variation in cyber force structures speaks to an additional question: why have militaries differed in how they implement cyber forces? A first step is to consider the ways in which implementation can unfold.

[1] Kurt Weyland, *Bounded Rationality and Policy Diffusion: Social Sector Reform in Latin America* (Princeton, New Jersey: Princeton University Press, 2009), 17–18. The issue of "loose bundle" innovations is also addressed by: V. Koontz, "Determinants of Individuals' Knowledge, Attitudes and Decisions Regarding a Health Innovation in Maine" (Dissertation, Ann Arbor, MI, University of Michigan, 1976).

Under the diffusion of an innovation in principle, potential adopters are faced with a greater degree of decision flexibility vis-à-vis the innovation—they can pick and choose which aspects or components to adopt. In this regard, complex, process-based innovations are particularly malleable.[2] As a result, the traditional scholarly focus on adoption becomes problematic: potential adopters are faced with not only the decision to adopt or reject an innovation in principle but also post-adoption decisions to modify or reject certain dimensions of an innovation.[3] As such, typical diffusion frameworks will struggle to explain the empirical variation that occurs as adopters adapt innovations during implementation to fit local political and institutional contexts.[4]

Implementation dynamics offer more nuanced insight into the ways in which adopters shape and reshape innovations across the diffusion process. While adoption encompasses the decision to adopt or reject an innovation principle, implementation is the actual integration of the innovation into the community of interest.[5] The implementation process involves putting to use new technologies or integrating new practices within an organizational setting and requires creating new or changing existing organizational routines and relationships.[6]

[2] Ronald E. Rice and Everett M. Rogers, "Reinvention in the Innovation Process," *Knowledge: Creation, Diffusion, Utilization* 1, no. 4 (June 1980): 502; Jane Fedorowicz and Janis L. Gogan, "Reinvention of Interorganizational Systems: A Case Analysis of the Diffusion of a Bio-Terror Surveillance System," *Information Systems Frontiers* 12 (2010): 81.

[3] Rice and Rogers, "Reinvention in the Innovation Process," 504.

[4] Sanya Carley, Sean Nicholson-Crotty, and Chris J. Miller, "Adoption, Reinvention and Amendment of Renewable Portfolio Standards in the American States," *Journal of Public Policy* 37, no. 4 (2017): 431–58; J. Clark, "Policy Diffusion and Program Scope: Research Directions," *Publius: The Journal of Federalism* 15 (1985): 61–70; H.R. Glick and S.P. Hays, "Innovation and Reinvention in State Policymaking: Theory and the Evolution of Living Wills," *Journal of Politics* 53 (1991): 835–50; Scott P. Hays, "Patterns of Reinvention: The Nature of Evolution during Policy Diffusion," *Policy Studies Journal* 24, no. 4 (1996): 551–66.

[5] Horowitz and Pindyck, "What Is a Military Innovation? A Proposed Framework," 19.

[6] Fedorowicz and Gogan, "Appendix: Reinvention of Interorganizational Systems: A Case Analysis of the Diffusion of a Bio-Terror Surveillance System."

A Framework for Implementation Dynamics

As a *process*, implementation unfolds across a series of multiple, discreet, and interconnected stages.[7] Organization studies have acknowledged that implementing an innovation consists of at least two stages. In the first stage, organizations introduce the innovation. The organization's leaders enable introduction by generating perceptions of the problem being addressed, gathering information, and fostering an attitude toward innovation and evaluation. The second stage concerns the use of the innovation until it becomes a routine.[8]

Although the introduction and routinization of an innovation are both critical stages, they represent only the beginning and end of the implementation process. The implementation process offers the opportunity for adopters to reinvent an innovation.[9] Reinvention refers to the ways in which adopters change or modify innovations through the processes of adoption and implementation.[10] These changes can be to the components of an innovation and/or how an innovation is used. Reinvention becomes particularly important when actors face broadly defined problems, [11] innovations that are too generalized[12] or overly complex,[13] or adopters lack detailed knowledge about an innovation.[14] Reinvention can be idiosyncratic or systematic, where later adopters learn from the experiences of early adopters.[15] Reinvention thus portrays a more

[7] Jones and Metzger, "Evaluating Conflict Dynamics: A Novel Empirical Approach to Stage Conceptions," 820.

[8] Cesar Camison-Zornoza et al., "A Meta-Analysis of Innovation and Organizational Size," *Organization Studies* 25, no. 3 (2004): 331–61; see also: Fariborz Damanpour, "Organizational Innovation: A Meta-Analysis of Effects of Determinants and Moderators," *Academy of Management Journal* 34 (1991): 675–88; G. Zaltman, R. Duncan, and J. Holbek, *Innovations and Organizations* (New York: Wiley, 1973).

[9] The policy "reinvention" literature looks beyond adoption to consider the content of adopted policies. Hays, "Patterns of Reinvention: The Nature of Evolution during Policy Diffusion," 564.

[10] Everett M. Rogers, *Diffusion of Innovations*, 5th ed. (New York: Free Press, 2003), 180.

[11] Rice and Rogers, "Reinvention in the Innovation Process," 501–2, 508–11.

[12] Hays, "Patterns of Reinvention: The Nature of Evolution during Policy Diffusion," 564; Rice and Rogers, "Reinvention in the Innovation Process," 505.

[13] Rice and Rogers, "Reinvention in the Innovation Process," 501.

[14] Rogers, *Diffusion of Innovations*.

[15] Carley, Nicholson-Crotty, and Miller, "Adoption, Reinvention and Amendment of Renewable Portfolio Standards in the American States," 434–35.

complex and dynamic diffusion process, where innovations change and evolve across systems as adopters purposely alter them during implementation.[16]

Many scholars analyzing reinvention, however, note an additional dimension: expansion, whereby an innovation becomes more comprehensive than its initial incarnation throughout the implementation process.[17] After introducing an innovation, many adopters amend initiatives to expand or increase the scope of innovation. Problematically, the post-adoption expansion of an innovation has received little attention from diffusion scholars. Instead of treating amendment/expansion as a distinct decision stage, most studies treat it as another instance of reinvention.[18] However, a multi-staged conception of implementation requires differentiating between the qualitative changes an innovation and the increase in the scope of an innovation.

Defining Implementation Stages

Few studies—whether of diffusion or of organizational innovation—incorporate these dynamics into staged conceptions of implementation. Eveland et al. (1977) stands as an early exception in studies of diffusion. The authors advance a framework of five stages, including: ***agenda-setting***, where organizations identify and define problems; ***matching***, where a potential solution is discussed; ***redefinition***, where the attributes of an innovation are defined according to organizational members and goals; ***structuring***, where members introduce the innovation into organizational structures; and ***interconnecting***, where those tasked with implementation redefine

[16] Hays, "Patterns of Reinvention: The Nature of Evolution during Policy Diffusion," 551–52; S.P. Hays, "Influences on Reinvention during the Diffusion of Innovations," *Political Research Quarterly* 49 (1996): 631.

[17] Hays, "Influences on Reinvention during the Diffusion of Innovations," 632; see also: Glick and Hays, "Innovation and Reinvention in State Policymaking: Theory and the Evolution of Living Wills"; C.Z. Mooney and M. H. Lee, "Legislative Morality in the American States: The Case of Pre-Roe Abortion Regulation Reform.," *American Journal of Political Science* 39 (1995): 599–627.

[18] Andrew Karch, "Emerging Issues and Future Directions in State Policy Diffusion Research," *State Politics & Policy Quarterly* 7, no. 1 (2007): 54–80; Carley, Nicholson-Crotty, and Miller, "Adoption, Reinvention and Amendment of Renewable Portfolio Standards in the American States," 435, 455.

their relationships with the rest of the organization and the external environment.[19] While advancing a multi-stage approach, Eveland et al. place overwhelming emphasis on the dynamics of adoption decisions (agenda-setting, matching, and redefinition). As such, changes can only occur during adoption—for Eveland et al., structuring and interconnection assume a linear and straightforward implementation process.

In surveying subsequent works in public policy, Carley et al. (2017) find that reinvention and amendment can certainly apply to post-adoption implementation efforts. Carley et al. note that previous studies have seen adoption, reinvention, and amendment as mutually exclusive diffusion processes and not discrete stages within a single framework. However, the authors suggest that this is misguided:

> …these are in fact distinct sequential decisions, as lawmakers first decide that they want a general class of policy, then decide what the specific characteristics of that policy should be and, finally, make adjustments to the policy after adoption. Without acknowledging this sequence, there is little theoretical foundation for explaining the evolution of policies as they diffuse over time.[20]

These insights echo the frameworks and findings of organizational scholars studying implementation processes. Recently, Chung and Choi (2018) have advocated for a stage-based conception of implementation in organizational studies. The authors propose that implementation unfolds across four stages, and the power balance between the initiators of an innovation and resistors drive implementation dynamics at each stage. Implementation begins with initiation, where an innovation is introduced into an organization. Subsequently, at the power evaluation

[19] J.D. Eveland, E.M. Rogers, and C.M. Klepper, “The Innovation Process in Public Organizations: Some Elements of a Preliminary Model,” Report to the National Science Foundation (Ann Arbor, MI: University of Michigan, 1977).

[20] Carley, Nicholson-Crotty, and Miller, “Adoption, Reinvention and Amendment of Renewable Portfolio Standards in the American States,” 453.

stage, unaligned members of the organization assess the power differential between the initiators and resistors; at the tactics evaluations stage, the initiators and resistors try to respectively facilitate and inhibit implementation, and their effectiveness is judged by unaligned members. The outcome stage is thus the culmination of power struggles across other implementation stages; innovations can be implemented without change, minimally implemented, modified, or implementation can fail.[21] Although this framework is important for understanding the differential impacts of a variable (in this case, the power balance between initiators and resistors) across the implementation process, Chung and Choi (2018) provide little insight into how the innovation itself changes in the course of implementation.

What is needed, then, is an implementation framework that incorporates changes to the nature or scope of an innovation and the potential for variables to have differential impacts across the implementation process.[22] To these ends, I propose a framework for implementation comprised of five discrete stages: pre-adoption, introduction, modification, expansion, and full implementation.

Stage 1: Pre-Adoption. A fully specified implementation process starts at the pre-adoption stage. This stage is the quintessential starting point for many innovation and diffusion studies. At pre-adoption, actors are faced with the decision to adopt or reject the innovation principle. At this stage, potential adopters define the problems to be addressed by innovation. Additionally, potential adopters identify and target specific models to implement innovation principles in concrete ways.

[21] Goo Hyeok Chung and Jin Nam Choi, "Innovation Implementation as a Dynamic Equilibrium: Emergent Processes and Divergent Outcomes," *Group & Organization Management* 43, no. 6 (2018): 999–1036.
[22] Carley, Nicholson-Crotty, and Miller, "Adoption, Reinvention and Amendment of Renewable Portfolio Standards in the American States," 453.

Stage 2: Introduction. Introduction is the second stage of the implementation process. Although some actors may be able to adopt and implement an innovation to its fullest extent, it is far more likely that limited aspects of an innovation are adopted and implemented in a piecemeal fashion over time. Accordingly, select elements of an innovation principle are adopted and matched to the adopter's specific needs, resources, and abilities. In doing so, introduction marks the initial installation and use of an innovation.[23] At the introduction stage, the innovation usually supports existing organizational goals and status quos.[24] Importantly, the initiators behind the adoption supply information to the communities implementing the innovation. Groups of resistors can emerge in response to the introduction of an innovation that threatens traditional power relations.

Stage 3: Modification. The third stage of implementation is modification, i.e. whether and what qualitative changes have been made to the innovation. After the initial introduction of an innovation, issues may arise that require the redefinition, redesign, or restructuring of the innovation's components. Such reinvention can be driven by: the failure to address problems as originally perceived; difficulties with operational implementation; or resistance from influential competing interests.[25] Competing interests and ideologies are particularly strong influences on the modification of an innovation. Those resisting an innovation may reject or advocate altering parts of an innovation that threaten their resources and traditional power relations. Thus,

[23] Rice and Rogers, "Reinvention in the Innovation Process," 502–3.

[24] On the integration of novel practices into military organizations,, see: Farrell, "Improving in War: Military Adaptation and the British in Helman Province, Afghanistan, 2006-2009."

[25] Rice and Rogers, "Reinvention in the Innovation Process," 501; Hays, "Patterns of Reinvention: The Nature of Evolution during Policy Diffusion," 564.

modification can emerge as an accommodation to resisting forces seeking to influence over the implementation process by threatening the viability of the innovation.[26]

Stage 4: Expansion. After a degree of consensus has been reached regarding the design of the innovation, implementation can proceed with a fourth stage—expansion. Expansion occurs after Introduction and prior to the full implementation of an innovation. Expansion is thus an intermediate step where initiatives increase in scope or comprehensiveness but have not yet been fully implemented. Expansion differs from modification:[27] while modification emphasizes changes in the composition or structure of an innovation, expansion involves an additional influx of resources (such as personnel and spending). Through expansion, organizations develop new operational concepts and goals.[28]

Stage 5: Full Implementation. The final stage in the implementation process is full implementation. At this stage, the innovation has been adopted to its fullest extent and has become routinized within the adopting entity.[29] The full implementation of an innovation can disrupt and alter organizational dynamics, leading to new organizational structures to support new areas of organizational operation. Within militaries, the full implementation of an innovation can institutionalize new paradigms of warfare.[30] Where military innovation involves organizational changes, full implementation entails the creation of an independent, unified military command.[31]

[26] R. K. Yin, “Changing Urban Bureaucracies: How New Practices Become Routinized” (Santa Monica, CA: RAND Corporation, 1978); Rice and Rogers, “Reinvention in the Innovation Process,” 501–3.
[27] Others make this distinction by claiming that amendment constitutes a distinct, second stage of reinvention. Hays, “Patterns of Reinvention: The Nature of Evolution during Policy Diffusion,” 563.
[28] Cheung, Mahnken, and Ross, “Frameworks for Analyzing Chinese Defense and Military Innovation,” 30.
[29] Rice and Rogers, “Reinvention in the Innovation Process,” 499–500.
[30] Rosen, *Winning the Next War: Innovation and the Modern Military*.
[31] Cheung, Mahnken, and Ross, “Frameworks for Analyzing Chinese Defense and Military Innovation,” 33–34.

Figure 3.1. A Simplified View of the Implementation Process

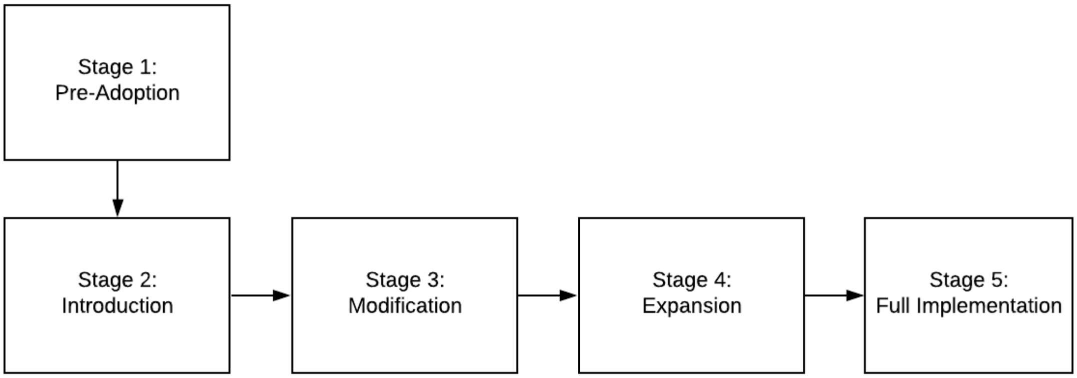


Figure 3.2. A Dynamic View of the Implementation Process

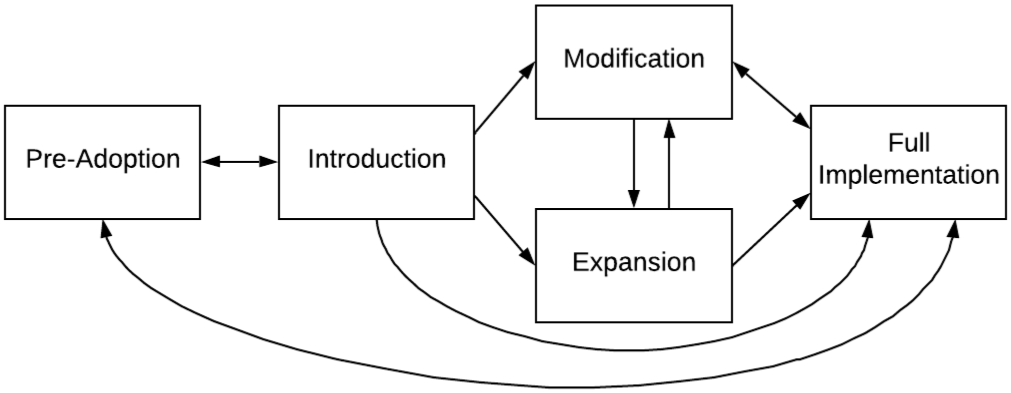


Figure 3.1 summarizes a simplified view of the implementation process described above. This view implies that innovations can and do change over the course of implementation. Importantly, and as will be explored further in Chapter 4, implementation often proceeds in dynamic, nonlinear patterns. Figure 3.2 presents a dynamic view of implementation with multiple pathways.[32] This multi-staged, dynamic framework can capture a variety of changes in cyber force structures within militaries. Moreover, this framework enables the conceptualization and

[32] Several authors have hinted at this dynamics but have not elaborated: Hays, “Patterns of Reinvention: The Nature of Evolution during Policy Diffusion,” 552; Rice and Rogers, “Reinvention in the Innovation Process”; Rogers, *Diffusion of Innovations*.

theorization of the key tensions and drivers at each implementation stage as well as across the entire implementation process.

The Challenge of Implementing Cyber Forces

The primary tension underlying the creation and implementation of cyber forces—and new military organizations more broadly—is the pursuit of two competing goals that pull implementation resources in opposing directions: building out a new mission and integrating the organization into the existing defense bureaucracy. Reaching the Full Implementation stage requires achieving both goals by creating an "ambidextrous" organization: cyber forces must be efficient in daily administrative and interagency processes while adapting to rapid changes in the operational environment.[33] Implementation is thus characterized by a tension between competing operational and bureaucratic imperatives:[34] organizational autonomy facilitates operational

[33] On ambidextrous organizations, see: Jan Kraner, *Innovation in High Reliability Ambidextrous Organizations: Analytical Solutions Toward Increasing Innovative Activity* (Cham, Switzerland: Springer International Publishing, 2018); Sebastian Raisch and Julian Birkinshaw, "Organizational Ambidexterity: Antecedents, Outcomes, and Moderators," *Journal of Management* 34, no. 3 (2008): 375–409. On how organizations must cultivate the ability to switch between operational and bureaucratic modes, see: T. R. Laporte and P. M. Consolini, "Working in Practice but Not in Theory: Theoretical Challenges of 'High Reliability Organizations,'" *Journal of Public Administration Research and Theory* 1, no. 1 (1991): 19–48; Anja Dalgaard-Nielsen, "Organizing Special Operations Forces: Navigating the Paradoxical Pressures of Institutional-Bureaucratic and Operational Environments," *Special Operations Journal* 3, no. 1 (2017): 67. In some cases, switching organizational "modes" can require culture-switching. On culture switching within the U.S. Department of Defense, see: D. P. Moynihan, "A Theory of Culture-Switching: Leadership and Red-Tape during Hurricane Katrina," *Public Administration* 90, no. 4 (2012): 851–68.

[34] This tension between operational and bureaucratic imperatives is at the heart of research on high-reliability organizations (HROs). The literature on HROs was originally developed to describe and explain the commonalities among aircraft carriers, air traffic controllers, and nuclear power plants. HROs manage complex, demanding, and time-critical technologies and operate in socially and politically unforgiving environments where major operational failures can result in destructive or catastrophic consequences, including the loss of life. As such, the operational challenge for HROs is to increase organizational performance while working to prevent and quickly recover from operational failures. To these ends, these organizations must be ambidextrous: they must pursue reliability to handle both known problems and manage unanticipated events. See: Kathleen M. Sutcliffe, "High Reliability Organizations (HROs)," *Best Pract Res Clin Anaesthesiol* 25, no. 2 (June 2011): 134; Laporte and Consolini, "Working in Practice but Not in Theory: Theoretical Challenges of 'High Reliability Organizations,'" 21–24; Paul E. Bierly, Scott Gallagher, and John-Christopher Spender, "Innovation and Learning in High-Reliability Organizations: A Case Study of United States and Russian Nuclear Attack Submarines, 1970-2000," *IEEE Transactions on Engineering Management* 55, no. 3 (2008): 393; Dalgaard-Nielsen, "Organizing Special Operations Forces: Navigating the Paradoxical Pressures of Institutional-Bureaucratic and Operational Environments," 70; Karl E. Weick, "Organizational Culture as a Source of High Reliability," *California Management Review* 29, no. 2 (1987): 112.

control but conflicts with the interdependent nature of the broader military and defense bureaucracy. Implementers must thus pursue autonomy and dedicate resources towards operational effectiveness in the cyber domain while retaining enough political capital to successfully navigate the bureaucratic ecosystem.[35]

Military organizations (and respective suborganizations) are "mission oriented": they have formally designated missions[36] and are predisposed to aggressively pursue the successful execution of those missions.[37] Because of this mission orientation, military organizations pursue autonomy over organizational resources and full operational control.[38] For those implementing a new mission—particularly when that mission is tied to a new organizational structure—autonomy and control over resources help to streamline mission-building. The development of a new mission area entails several observable actions. For newly created organizations, implementing a new mission involves the creation of new career paths and the reorganization of existing and recruitment of new personnel.[39] Developing mission-specific expertise within the organization can require subsequent changes to the curriculum of professional military educational institutions. Strategic and doctrinal changes also support mission development;[40] at the operational level, novel concepts of operation and measures of effectiveness help to refine how the organization executes the mission.[41] Finally, as the mission grows and is refined, the

[35] For an exploration of this tension in the strategic reorganization of Norwegian Special Operations Forces, see: Dalgaard-Nielsen, "Organizing Special Operations Forces: Navigating the Paradoxical Pressures of Institutional-Bureaucratic and Operational Environments."

[36]Morton Halperin, Priscilla Clapp, and Arnold Kanter, *Bureaucratic Politics and Foreign Policy*, 2nd ed. (Washington, D.C.: Brookings Institution Press, 2006), 25; see also: Graham Allison and Morton Halperin, "Bureaucratic Politics: A Paradigm and Some Policy Implications," *World Politics* 24, no. 1 (1972): 40–79.

[37] Moynihan, "A Theory of Culture-Switching: Leadership and Red-Tape during Hurricane Katrina."

[38] Halperin, Clapp, and Kanter, *Bureaucratic Politics and Foreign Policy*, 51; Moynihan, "A Theory of Culture-Switching: Leadership and Red-Tape during Hurricane Katrina."

[39] Rosen, *Winning the Next War: Innovation and the Modern Military*, 20–21.

[40] Mahnken, "China's Anti-Access Strategy in Historical and Theoretical Perspective."

[41] For example, U.S. submarine forces reoriented during World War II to take on Japanese merchant ships. This was a rare case of wartime innovation: no new technology was introduced, and innovation was purely in terms of

organization should push for additional resources to expand. This can even include the establishment of new arms or sub-organizations within the cyber force organizational construct.[42]

However, mission-building does not occur in a vacuum. Pre-existing bureaucracy will typically oppose the creation of a new organization. Some parts of the military may even lay claim to the cyber mission, defining it as part of their own mission.[43] For a new organization to survive, implementers must build out the ability to operate within the broader bureaucratic environment. Successful bureaucracy-building allows cyber forces to assimilate into interagency processes and compete for funding, influence, and legitimacy with the rest of the military establishment.[44] For these reasons, bureaucratization helps insulate the cyber mission from the resistance and opposition of other military organizations. However, existing bureaucracies will possess resource and influence advantages over a nascent cyber force. Accordingly, the primary bureaucracy-building challenge for implementers is grappling with power-asymmetries.[45]

Implementers can employ several strategies to build bureaucratic power. They can engage in coalition-building with civilian actors or with other military actors by appealing to

concepts of operation (CONOPs). Without novel CONOPs and measures of strategic effectiveness, implementation efforts can stall. This was the case with the introduction of the tank into the British military—the British failed to initially develop a corresponding measure of strategic effectiveness. The result was not a failure to use new technology, but instead a failure in organizational implementation. Rosen, *Winning the Next War: Innovation and the Modern Military*, 52, 128, 132.

[42] See broadly arguments made by: Mahnken, "China's Anti-Access Strategy in Historical and Theoretical Perspective"; Rosen, *Winning the Next War: Innovation and the Modern Military*.

[43] On bureaucratic resistance to new organizations, see: Daniel W. Drezner, "Ideas, Bureaucratic Politics, and the Crafting of Foreign Policy," *American Journal of Political Science* 44, no. 4 (2000): 733–35; Halperin, Clapp, and Kanter, *Bureaucratic Politics and Foreign Policy*, 26; Grauer, "Moderating Diffusion: Military Bureaucratic Politics and the Implementation of German Doctrine in South America, 1885-1914." Fights over the cyber mission should be particularly acute when either (1) existing bureaucratic actors define cyber as part of their own organizational essence or (2) when taking on the cyber mission could bring in additional funds and give an organization greater scope to pursue its primary mission. Halperin, Clapp, and Kanter, *Bureaucratic Politics and Foreign Policy*, 38–40.

[44] Dalgaard-Nielsen, "Organizing Special Operations Forces: Navigating the Paradoxical Pressures of Institutional-Bureaucratic and Operational Environments," 71; Halperin, Clapp, and Kanter, *Bureaucratic Politics and Foreign Policy*, 25. Influence is a crucial resource for protecting and enhancing a military organization's mission.

[45] On bureaucratic asymmetries, see: Juliet Kaarbo, "Power Politics in Foreign Policy: The Influence of Bureaucratic Minorities," *European Journal of International Relations* 4, no. 1 (1998): 67–97. On power dynamics and implementation resistance, see: Grauer, "Moderating Diffusion: Military Bureaucratic Politics and the Implementation of German Doctrine in South America, 1885-1914."

common interests.[46] Implementers can also seek to embed cyber forces within another military organization, sacrificing autonomy for mission insulation.[47] Relatedly, cyber forces can gain bureaucratic power through inclusion, i.e. explicitly including bureaucratic competitors in the organizational command structures. Finally, implementers can attempt to quell opposition by narrowing the definition of the cyber mission.[48] However, strategies for bureaucracy-building necessarily compromise autonomy and/or mission definition to preserve organizational existence.[49]

Both mission-building and bureaucracy-building are necessary. The question at the crux of implementation is: how do cyber force implementers prioritize mission- and bureaucracy-building? Initially prioritizing mission-building at the expense of bureaucratic integration can undermine the ability of cyber forces to compete for funding, legitimacy, and bureaucratic influence, all of which can hamper cyber forces' ability to achieve operational effectiveness over the long term. Conversely, by prioritizing assimilation into the defense bureaucracy, cyber forces sacrifice resources for mission-building in a rapidly changing environment, undermining the primary purpose and justification for the organization's existence. As discussed in the next section, overall military size is the key factor driving implementers to prioritize one aspect of organization-building over the other.

[46] Virpi Sorsa and Eero Vaara, "How Can Pluralistic Organizations Proceed with Strategic Change? A Processual Account of Rhetorical Contestation, Convergence, and Partial Agreement in a Nordic City Organization," *Organization Science*, 2020, 1–26, https://doi.org/10.1287/orsc.2019.1332; Paul Spee and Paula Jarzabkowski, "Agreeing on What? Creating Joint Accounts of Strategic Change," *Organization Science* 28, no. 1 (2017): 152–76.
[47] Drezner, "Ideas, Bureaucratic Politics, and the Crafting of Foreign Policy."
[48] Kaarbo (1998) classifies this as an informational strategy. Kaarbo, "Power Politics in Foreign Policy: The Influence of Bureaucratic Minorities," 75.
[49] "In implementing missions that they know to be coveted by another organization, organizations may bend over backward to avoid giving any reason to increase their bureaucratic competitor's share of the mission." Halperin, Clapp, and Kanter, *Bureaucratic Politics and Foreign Policy*, 49.

How Organizational Size Shapes Implementation Dynamics

I assert that organizational size—specifically, the overall size of a state's military—is a crucial variable shaping implementation dynamics. Whereas organizational attributes such as specialization, formalization, and centralization determine the nature of tasks performed within an organization, size concerns the grouping and resources of units within an organization. Organizational size varies along four theoretically important dimensions: the number of functionally differentiated sub-units (horizontal complexity), the levels of hierarchy (vertical complexity), the number of members (human capital), and the amount of financial capital.[50] For militaries, size is relative: measurements along these four dimensions must be compared to the measurements of other militaries to determine whether the military organization is "small" or "large." For theoretical purposes, I assume that, *ceteris paribus*, larger organizations exhibit a greater number of sub-units, more levels of hierarchy, more members, and greater amounts of financial capital.[51]

I argue that organizational size helps mitigate the operational-bureaucratic tension underlying cyber force implementation. In short, larger militaries are more predisposed to initially prioritize the bureaucratic goal over the mission goal, while smaller militaries are more likely to focus on mission-building before pivoting to bureaucracy-building. Despite a greater risk tolerance and the availability (relative to smaller organizations) of human and financial capital to build out the cyber mission, larger militaries entail a greater number of competing

[50] Hendrik Ewens and Joris van der Voet, "Organizational Complexity and Participatory Innovation: Participatory Budgeting in Local Government," *Public Management Review* 21, no. 12 (2019): 1852; see also: H. Mintzberg, *The Structuring of Organizations* (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1979).

[51] It is possible that an organization is designated as large based on an extreme value for one dimension, i.e. has the same levels of horizontal and vertical complexity and financial capital as other organizations but a significantly higher number of members. Although not the focus of this project, future research should examine the whether there are distinct effects of each dimension of size on implementation outcomes.

interests that can threaten the autonomy of cyber forces or lay claim to the cyber mission. implementers in larger militaries are more likely to ensure the bureaucratic integration and organizational survival of cyber forces before prioritizing mission-building.

Conversely, smaller militaries are more likely to focus directly on mission-building. Implementers face a smaller pool of bureaucratic competitors in smaller militaries, meaning that there are fewer interests to lay claim to the cyber mission and threaten the autonomy of cyber forces. However, smaller militaries possess a smaller resource base and lack the risk tolerance of larger militaries. Accordingly, implementers are more inclined to vigorously build out the cyber mission to justify an additional strain on financial and human capital. Subsequently, implementers in smaller militaries are likely to pivot to the bureaucratic imperative in attempts to secure future resources. Personal ties can become crucial at this phase of implementation: despite few available resources, implementers in a small organization can leverage personal ties to advance implementation progress. The rest of this section unpacks the effect of organizational size on the implementation process as a whole as well as its impact across each stage of the implementation process. In doing so, I offer a framework that reconciles conflicting accounts of the role of organizational size.

The Overall Effect of Size

Organizational size can exert both direct and indirect effects on innovation and implementation processes.[52] Existing studies on size and its effect on innovation and implementation outcomes[53] exhibit contradictory findings. In fact, a comprehensive review of the

[52] "Size is a broad organizational variable that not only affects innovation directly, but also indirectly, through its effects on other properties of the organization." Fariborz Damanpour, "Organizational Size and Innovation," *Organization Studies* 12, no. 3 (1992): 395.

[53] Overall, organizational size is more strongly related to the implementation than the initial stages of innovation Damanpour, 378–88.

relationship between size and innovation across organizational theory notes "a single common conclusion, which is that the most consistent result found in the organizational innovation literature is that its research results have been inconsistent."[54]

On one hand, many studies have asserted that large organizations are more likely to undertake and implement radical, wide-ranging innovations than smaller organizations. Large organizations maintain economies of scale for research and development and can more effectively distribute the risks of failure than smaller organizations. With greater financial resources, larger organizations are better positioned to implement innovations than smaller organizations.[55] The greater complexity exhibited by larger organizations also facilitates innovation and implementation:[56] complexity produces a broad knowledge base through a variety of issue specialists and the exchange of ideas[57] across differentiated units.[58] For these reasons,

[54] Cesar Camison-Zornoza et al., "A Meta-Analysis of Innovation and Organizational Size," *Organization Studies* 25, no. 3 (2004): 332; see also: Richard A. Wolfe, "Organizational Innovation: Review, Critique and Suggested Research Directions," *Journal of Management Studies* 31 (1994): 405–31.

[55] Robert S. Dewar and Jane E. Dutton, "The Adoption of Radical and Incremental Innovations: An Empirical Analysis," *Management Science* 32 (1986): 1422–33; R. Germain, "The Role of Context and Structure in Radical and Incremental Logistics Innovation Adoption," *Journal of Business Research* 35 (1997): 117–27; D. A. Levinthal and James G. March, "The Myopia of Learning," *Strategic Management Journal* 14 (1993): 95–112; D. Arias-Aranda, B. Minguela-Rata, and A. Rodriguez-Duarte, "Innovation and Firm Size: An Empirical Study for Spanish Engineering Consulting Companies," *European Journal of Innovation Management* 4, no. 3 (2001): 133–42; H. Forsman and U. Annala, "Small Enterprises as Innovators: The Shift from a Low Performer to a High Performer," *International Journal of Technology Management* 51, no. 1/2 (2011).

[56] Peter M. Blau, "A Formal Theory of Differentiation in Organizations," *American Sociological Review* 35 (1970): 201–18; Walter R. Boland, "Size, External Relations, and the Distribution of Power: A Study of Colleges and Universities," in *Comparative Organizations*, ed. W. V. Heydebrand (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1973), 428–41; Judith R. Blau and William McKinley, "Idea, Complexity, and Innovation," *Administrative Science Quarterly* 24 (1979): 200–219; Alan D. Meyer and James B. Goes, "Organizational Assimilation of Innovations: A Multilevel Contextual Analysis," *Academy of Management Journal* 31 (1988): 897–923; Robert W. Zmud, "An Examination of 'Push-Pull' Theory Applied to Process Innovation in Knowledge Work," *Management Science* 30 (1984): 727–38; Robert M. Marsh and Hiroshi Mannari, "The Size Imperative? Longitudinal Tests," *Organization Studies* 10, no. 1 (1989): 83–95.

[57] Michael Aiken and Jerald Hage, "The Organic Organization and Innovation," *Sociology* 5 (1971): 63–82; John R. Kimberly and Michael R. Evanisko, "Organizational Innovation: The Influence of Individual, Organizational, and Contextual Factors on Hospital Adoption of Technological and Administrative Innovations," *Academy of Management Journal* 24 (1981): 689–713.

[58] R. Caceres, J. Guzman, and M. Rekowski, "Firms as Source of Variety in Innovation: Influence of Size and Sector," *International Entrepreneurship and Management Journal* 39, no. 4 (2011): 437–69; Fariborz Damanpour, "The Adoption of Technological, Administrative, and Ancillary Innovations: Impact of Organizational Factors," *Journal of Management* 13 (1987): 675–88; J. Victor Baldridge and Robert A. Burnham, "Organizational

authors conclude that large organizations are more likely to radically adopt and implement innovations while smaller organizations adopt and implement innovations in an incremental manner.

On the other hand, scholars have suggested that, despite resource advantages, larger organizations face many hurdles that stifle innovation. Larger organizations usually entail higher cooperation costs[59] that slow the connection of capabilities, resources, knowledge, and strategies across different parts of the organization.[60] As such, innovation and implementation proceed more slowly. Moreover, large organizations develop distinct bureaucratic subcultures and entrenched interests that can decrease the efficiency of and even discourage innovation and implementation.[61] Large bureaucracies are slower to react to changes in the strategic environment.[62] Accordingly, smaller organizations are better equipped to adjust to external changes and embrace innovations in a more cost-effective manner than larger organizations. Smaller organizations are thus more predisposed to undertake and implement radical

Innovation: Industrial, Organizational, and Environmental Impact," *Administrative Science Quarterly* 20 (1975): 165–76.

[59] B. Nooteboom et al., "Optimal Cognitive Dissonance and Absorbative Capacity," *Research Policy* 36 (2007): 1016–34.

[60] M. J. Leiblein and T. L. Madsen, "Unbundling Competitive Heterogeneity: Incentive Structures and Capability Influences on Technological Innovation," *Strategic Management Journal* 30 (2009): 711–35; D. Dougherty and C. Hardy, "Sustained Product Innovation in Large, Mature Organizations: Overcoming Innovation-to-Organization Problems," *Academy of Management Journal* 39, no. 5 (1996): 1120–53; P. M. Blau and R. A. Schoenherr, *The Structure of Organizations* (New York: Basic Books, 1971).

[61] Camison-Zornoza et al., "A Meta-Analysis of Innovation and Organizational Size," 338; Michael A. Hitt, Robert E. Hoskisson, and R. Duane Ireland, "Mergers and Acquisitions and Managerial Commitment to Innovation in M-Form Firms," *Strategic Management Journal* 11 (1990): 29–47; Nooteboom et al., "Optimal Cognitive Dissonance and Absorbative Capacity"; Frederic M. Scherer and David Ross, *Industrial Market Structure and Economic Performance* (Boston, MA: Houghton Mifflin, 1990).

[62] W. M. Cohen and D. A. Levinthal, "Absorpative Capacity: A New Perspective on Innovation and Learning," *Administrative Science Quarterly* 35 (1990): 128–52; H. A. Haveman, "Between a Rock and a Hard Place: Organizational Change and Performance under Conditions of Fundamental Environmental Uncertainty," *Administrative Science Quarterly* 37 (1992): 48–75; Fariborz Damanpour and D. J. Wischnevsky, "Research on Innovation in Organizations: Distinguishing Innovation-Generating from Innovation-Adopting Organizations," *Journal of Engineering and Technology Management* 23, no. 4 (2006): 269–91; Leiblein and Madsen, "Unbundling Competitive Heterogeneity: Incentive Structures and Capability Influences on Technological Innovation."

innovations.[63] Large organizations lend themselves to more incremental innovation and implementation.[64]

To reconcile these competing claims, some researchers have postulated that the relationship between organizational size large-scale innovation is curvilinear.[65] This suggests that increases in organizational size facilitates radical innovation; however, after a certain point, larger organizations experience diminishing returns. The larger an organization becomes, the more resources that are required to produce and implement innovations.[66] Drawing on this logic, my first hypothesis is:

> ***H1: The relationship between military size and the risk of completing the implementation process is curvilinear.***

While increases in organizational size—particularly increases in human and financial capital—can enable the faster adoption and implementation of a cyber force, the additional bureaucratic hurdles in larger organizations should negatively impact implementation processes, leading to slower adoption and implementation rates than smaller organizations.

Stage-Specific Effects

A more nuanced way to understand the impact of organizational size on implementation is to assess the effects of size across individual implementation stages. I make four key claims about the role of organizational size. First, larger militaries should be more likely to create and

[63] S. Laforet, "Organizational Innovation Outcomes in SMEs: Effects of Age, Size, and Sector," *Journal of World Business* 48, no. 4 (2013): 590–502.
[64] J. E. Ettlie, W. P. Bridges, and R. D. O'keefe, "Organizational Strategy and Structural Differences for Radical versus Incremental Innovation," *Management Science* 30, no. 6 (1984): 682–95.
[65] J. E. Ettlie and A. H. Rubenstein, "Firm Size and Product Innovation," *Journal of Produce Innovation Management* 4, no. 2 (1987): 89–108; K. Pavitt, "What We Know about the Strategic Management of Technology," *California Management Review* 23, no. 3 (1990): 17–26; K. -H. Tsai and J. -C. Wang, "Does R&D Performance Decline with Firm Size? A Re-Examination in Terms of Elasticity," *Research Policy* 34 (2005): 966–76.
[66] Damanpour, "Organizational Size and Innovation," 386.

introduce a cyber force than smaller militaries due to a higher risk tolerance. Larger organizations tend to have a higher tolerance for risk than smaller organizations, i.e. larger militaries are better able to absorb the risks of innovation failures. This greater risk tolerance stems from two characteristics of large organizations. The greater resource levels of large organizations compared to smaller ones—specifically, greater amounts of human and financial capital—facilitate investments in innovative initiatives.[67] A greater number of organizational members increases the potential pool of issue-expertise and technical know-how needed to introduce an innovation; greater spending levels allow for new ideas to be actualized.[68] At the same time, larger organizations are better able to distribute risks of failure than smaller organizations. As organizations grow in the number of sub-units, failed innovation in one sub-unit is less costly to the overall performance of the organization. Larger organizations have a greater number of sub-units than smaller organizations over which to distribute the effort to compensate for failure.[69]

Accordingly, larger militaries (such as those owned by great powers) possess more material, scientific, and technical capacity and are better able to absorb the risks of innovation than smaller militaries.[70] Moreover, larger militaries face greater systemic incentives to be the

[67] Suk Joon Hwang and Frances Berry, "Deterring Drunk Driving: Why Some States Go Further than Others in Policy Innovation," *International Journal of Environmental Research and Public Health* 16 (2019): 1749–67.

[68] While smaller organizations may possess similar levels of expertise across fewer members, there are fewer opportunities for the cross-fertilization of ideas. Fariborz Damanpour and William M. Evan, "Organizational Innovation and Performance: The Problem of Organizational Lag," *Administrative Science Quarterly* 29 (1984): 392–409; Walter R. Nord and Sharon Tucker, *Implementing Routine and Radical Innovation* (Lexington, MA: Lexington Books, 1987); Aiken and Hage, "The Organic Organization and Innovation"; Kimberly and Evanisko, "Organizational Innovation: The Influence of Individual, Organizational, and Contextual Factors on Hospital Adoption of Technological and Administrative Innovations."

[69] Camison-Zornoza et al., "A Meta-Analysis of Innovation and Organizational Size," 337; see also: Damanpour, "Organizational Size and Innovation"; Michael A. Hitt, Robert E. Hoskisson, and R. Duane Ireland, "Mergers and Acquisitions and Managerial Commitment to Innovation in M-Form Firms," *Strategic Management Journal* 11 (1990): 29–47.

[70] Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*; Damanpour, "Organizational Size and Innovation," 378–88; Camison-Zornoza et al., "A Meta-Analysis of Innovation and Organizational Size," 337.

prime movers of international innovation than smaller militaries.[71] Smaller militaries are therefore more likely to have limited freedom and institutional capacity as well as fewer systemic incentives to introduce new ideas about the use of military forces. In these cases, cyber forces are more likely to be adopted out of strategic necessity.[72] As such, Hypothesis 2 states:

> ***H2: Larger militaries are more likely to transition into Introduction than smaller militaries.***

Second, once a cyber force has been introduced, the organizational model (branch, service, and joint constructs) of a cyber force is more likely to be modified in larger militaries than in smaller militaries. As organizational size increases, so does the number of interests, whether it be an increase in the number of sub-units, levels of hierarchy, or an increase in membership.[73] An increase in the number of competing interests decreases the likelihood that consensus can be reached over cyber force structure: as organizations grow, so do the number of potential veto players.[74] Bureaucratic pressures to veto or assert control over the implementation can emanate from horizontal and/or vertical resistors.[75]

Moreover, as organizations become larger, sub-groups are more likely to develop their own norms, cultures, values, and social dynamics for their operations.[76] As such, the dynamics of bureaucratic politics are likely to be more intense in larger organizations, particularly when

[71] Resende-Santos, *Neorealism, States, and the Modern Mass Army*, 71–75.

[72] Kjell Inge Bjerga and Torunn Laugen Haaland, "Development of Military Doctrine: The Particular Case of Small States," *The Journal of Strategic Studies* 33, no. 4 (2010): 505–33.

[73] Organizational budget constraints can also influence reinvention; Rice and Rogers, "Reinvention in the Innovation Process," 502.

[74] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups*, 2nd ed. (Cambridge, MA: Harvard University Press, 1971), 53–65.

[75] Kaarbo, "Power Politics in Foreign Policy: The Influence of Bureaucratic Minorities."

[76] M. L. Tushman and C. A. O'Reilly, *Winning through Innovation: A Practical Guide to Leading Organizational Change and Renewal* (Cambridge, MA: Harvard Business School Press, 1997).

innovations threaten traditional power relations.[77] Implementation efforts can become embedded in and reinforce existing routines, procedures, and structures.[78] As a result, the pursuit of an autonomous cyber force in large militaries is likely to require extensive coalition-building; the increases the probability that the organizational model of the cyber force is modified.[79] Implementers in larger militaries are therefore more likely to initially prioritize bureaucratic assimilation over mission development after introducing a cyber force.

Conversely, cyber forces in smaller organizations should be less likely to undergo modification than those in larger organizations. Implementers face relatively fewer competing interests, meaning that implementers are less likely to undertake extensive political bargaining than their counterparts in larger organizations.[80] Moreover, because of the higher costs of introduction, most of the bureaucratic negotiation in smaller militaries are likely to occur prior to introduction. Thus, smaller organizations are more likely to bypass the Modification stage, allowing implementers to focus more building out the cyber mission and expanding cyber forces. Hypothesis 3 therefore states:

[77] Morton Halperin, Priscilla Clapp, and Arnold Kanter, *Bureaucratic Politics and Foreign Policy*, 2nd ed. (Washington, D.C.: Brookings Institution Press, 2006). Additionally, the presence of a substantial "old guard" with entrenched interests can exacerbate bureaucratic politics; see: Ryan Grauer, “Moderating Diffusion: Military Bureaucratic Politics and the Implementation of German Doctrine in South America, 1885-1914,” *World Politics* 67, no. 2 (April 2015): 268–312.

[78] I. G. Vaccaro et al., “Management Innovation and Leadership: The Moderating Role of Organizational Size,” *Journal of Management Studies* 49, no. 1 (2012): 28–51; K. Z. Zhou and C. B. Li, “How Strategic Orientations Influence the Building of Dynamic Capability in Emerging Economies,” *Journal of Business Research* 53, no. 3 (2010): 224–31.

[79]For example, decisions regarding the redesign of the U.S. Navy’s submarine design had a number of participants and stakeholders—Congress, the Department of Defense, Navy leadership, contractors, and consultants, among others. These interests debated both performance parameters and cost; negotiation and compromise resulted in a more conservative platform design than initially intended. Changes to design were made primarily to satisfy as many of the stakeholders as possible. Bierly, Gallagher, and Spender, “Innovation and Learning in High-Reliability Organizations: A Case Study of United States and Russian Nuclear Attack Submarines, 1970-2000,” 405. For broader examples of this dynamics, see also: Damanpour, “Organizational Size and Innovation,” 379.

[80] Nord and Tucker, *Implementing Routine and Radical Innovation*, 18; Damanpour, “Organizational Size and Innovation,” 378–88.

H3: Cyber forces in larger militaries are more likely to transition into Modification than those in smaller militaries.

Third, although smaller militaries can focus implementation efforts on expansion, expansion is more likely to occur in larger organizations. With greater resources and capabilities, larger organizations are better able to extend existing knowledge bases than smaller organizations.[81] Smaller militaries are more likely to be handicapped by resource constraints that limit the potential for cyber force expansion.[82] As such, Hypothesis 4 states:

H4: Cyber forces in larger militaries are more likely to transition into Expansion than those in smaller militaries.

Finally, I assert that the transition into full implementation is greatly influenced by providing "proof of concept" to political leaders and other military organizations by linking the operational effects of computer network operations to broader strategic priorities. Successful operational experiences provide crucial feedback to military leaders and political decisionmakers that reduces uncertainty regarding the strategic implications of the cyber domain. Because larger organizations generally have a greater number of interests to which implementers can link operational success, they are likely to present a more opportunities for proof of concept than smaller organizations. This leads to Hypothesis 5:

[81] Beatriz Fores and Cesar Camison, "Does Incremental and Radical Innovation Performance Depend on Different Types of Knowledge Accumulation Capabilities and Organizational Size?," *Journal of Business Research* 69 (2016): 831–48.

[82] Terry Terriff and Frans Osinga, "Conclusion: The Diffusion of Military Transformation to European Militaries," in *A Transformation Gap? American Innovations and European Military Change*, ed. Terry Terriff, Frans Osinga, and Theo Farrell (Stanford, California: Stanford University Press, 2010), 208.

> ***H5: Cyber forces in larger militaries are more likely to transition into Full Implementation than those in smaller militaries.***

Alternative Explanations: Capacity and Culture

Two alternative explanations for the implementation of cyber forces—adoption-capacity and organizational culture—help to shed light on the contingent importance of organizational size. In the brief discussion that follows, I sketch out adoption-capacity theory as well as an explanation resting on organizational cultural logics. I differentiate each explanation from the theory of organizational size by highlighting several shortcomings that indicate the need for additional theorization.

Adoption-Capacity

According to the first alternative explanation, adoption-capacity, competitive pressures drive states to respond to the demonstration of military innovations in one of two ways: internally, by adopting or countering the innovation; or externally, by balancing with an adopter, bandwagoning with the demonstrator, or becoming neutral. Adoption decisions hinge on two factors. The first is the information on adoption requirements transmitted by the demonstration event: the greater certainty states have surrounding the substance of the innovation, the more likely a state is to adopt the innovation. The second factor is the state's ability to meet the financial and organizational requirements for adoption given its current capabilities.[83]

The required financial intensity and required organizational capital for adoption differ by innovation. Financial intensity refers to the required mobilization of resources specific to the innovation. The financial intensity of adopting an innovation is driven by (1) whether the underlying basis of the innovation technology is civilian or military and (2) the cost per unit of

[83] Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*, 30–42.

technology. States are more likely to adopt innovations with a lower financial intensity (civilian basis and low cost per unit) than those with a higher financial intensity (military basis and high cost per unit).[84] Organizational capital refers to a military's ability—in terms of critical task focus, experimentation, and its bureaucratic entrenchment—to undertake the necessary organizational changes (in scope and degree) to implement a given innovation. All else equal, innovations requiring less organizational capital are more likely to be adopted than those requiring a greater amount of organizational capital.[85] Ultimately, states that cannot muster the required financial and/or organizational capital must resort to alternative strategies to innovation.[86]

What then, would adoption-capacity predict for the implementation of cyber forces? In his concluding chapter, Horowitz (2010) extends the adoption-capacity argument to consider cyberwarfare. Horowitz posits that "the construction of cyberwarfare units could require a fairly low level of financial intensity to adopt due to their heavy linkages to commercial enterprises."[87] However, for cyberspace to become a domain for military warfare, innovation "will also probably require large levels of organizational transformation."[88] This indicates that the adoption of cyber forces should require relatively little financial intensity but large amounts of organizational capital to adopt and implement. Moreover, the relative availability of financial and organizational capital should dictate whether a military prioritizes the operational or bureaucratic goal during initial implementation efforts.

[84] Horowitz, 31–33.
[85] Horowitz, 32–39.
[86] Horowitz, 27.
[87] Horowitz, 219.
[88] Horowitz, 220.

Unfortunately, adoption-capacity does not treat implementation as a distinct stage: considerations of implementation costs and the likelihood of success are part of adoption decisions. However, the logic of adoption-capacity suggests that, *ceteris paribus*, most states should easily transition into Introduction: low financial intensity enables adoption, but high organizational capital requirements prevent greater implementation progress. Increases in organizational capital should thus facilitate transitions between the Introduction, Expansion, and Full Implementation stages of the implementation process. This explanation, however, provides little insight into the dynamics of reinvention that take place during the Modification stage. Competing interests in adoption-capacity are only examined in the context of organizational age and bureaucratic entrenchment over time: the older the organization, the more likely that existing bureaucratic players resist any type of change that threatens business as usual. This discussion only implies that a greater number of bureaucratic interests prevents further implementation.[89]

Adoption-capacity differs from the theory of organizational size in another important way: Horowitz's organizational capital is relatively agnostic to the absolute size of an organization. Instead, his framework is more focused on bureaucratic bloating. However, he does note that the two factors may be related, and the issue of organizational size may take on more significance depending on the specific military innovation under examination.[90]

Organizational Culture

The second alternative explanation for cyber force implementation rests on organizational culture. In militaries, organizational culture refers to "those identities, norms, and values that have been internalized by a military organization, and that frame the way the organization views

[89] Horowitz, 37–38.

[90] Horowitz, 38 n. 43.

the world, and its role and functions in it."[91] Culture can shape decisions over which innovations to pursue[92] as well as the scope, pace, and extent of diffusion.[93] According to cultural accounts, competitive pressures—via external threats or strategic setbacks—can provide the impetus for innovation but cannot explain the extent to which the adoption of an innovation occurs.[94]

A key factor pointed to by cultural explanations is the degree of cultural tolerance for innovation, i.e. whether military organizations and their leadership tolerate deviations from orthodox practices and structures.[95] Higher degrees of cultural tolerance increase a military's openness to new ideas and facilitate the flow and absorption of information about an innovation. In this way, militaries are more responsive to strategic setbacks, and adoption is likely to occur faster and more extensively. Conversely, when militaries and their leaders work to enforce a cultural orthodoxy—and thus exhibit lower levels of cultural tolerance—the adoption of an innovation is expected to be limited, partial, or non-existent. Lower levels of cultural tolerance close off militaries to new information and practices and restrict responsiveness to strategic setbacks.[96] In these cases, an orthodox culture curtails the adoption of practices and technologies that are seen as incompatible.[97]

Yet, when innovations diffusion in principle, militaries with low levels of cultural tolerance may still be likely to adopt and adapt the broad innovation principle. In these

[91] Farrell and Terriff, "Military Transformation in NATO: A Framework for Analysis," 8. See also: Jeffrey W. Legro, "Military Culture and Inadvertent Escalation in World War II," *International Security* 18, no. 4 (1994): 115–18.
[92] Kier, "Culture and Military Doctrine: France between the Wars."
[93] Goldman, "Cultural Foundations of Military Diffusion," 70.
[94] Goldman, 90.
[95] Although this has generally been explored at the level of "political culture", the argument is just as applicable to the level of organizational culture. Jack A. Goldstone, "Cultural Orthodoxy, Risk, and Innovation: The Divergence of East and West in the Early Modern World," *Sociological Theory* 5, no. 2 (1987): 119–35; Goldman, "Cultural Foundations of Military Diffusion."
[96] Goldman, "Cultural Foundations of Military Diffusion," 90.
[97] For example, see: Eisenstadt and Pollack, "Armies of Snow and Armies of Sand: The Impact of Soviet Military Doctrine on Arab Militaries"; Lynn, "Heart of the Sepoy: The Adoption and Adaptation of European Military Practice in South Asia, 1740-1805."

circumstances, culturally intolerant militaries can pursue an incarnation of the innovation principle that represents the best "cultural fit" with the organization's existing orthodoxy.[98] For example, an important orthodoxy in many militaries is operational jointness: a culture of jointness promotes and prescribes operational coordination, cooperation, and integration across military services.[99] Those militaries with a high degree of cultural jointness should be biased towards the selection of a joint force cyber force structure, while those who have not or have weakly internalized jointness (and thus have a culture of service-dominance) are more likely to pursue a service-based force structure.

Together, cultural tolerance and fit can help explain both the selection of organizational model for cyber forces and the extent to which it is implemented. Cultural fit provides a logic for assessing the selection of an organizational model for cyber forces;[100] culturally tolerant militaries are expected to implement the chosen model to a greater extent (i.e. at higher levels of command) than culturally intolerant militaries. Importantly, cultural tolerance can change over time and is thus not a static variable.[101] This logic suggests that increases in cultural tolerance should facilitate transitions between the Introduction, Expansion, and Full Implementation stages. Additionally, while cultural "fit" can explain initial organizational model selection, increases in cultural tolerance should also increase the likelihood of Modification. As military organizations become more tolerant of deviations from orthodoxies, there is an increased

[98] For more on cultural fit, see: Jeffrey T. Checkel, "Norms, Institutions and National Identity in Contemporary Europe," *International Studies Quarterly* 43, no. 1 (1999): 83–114.

[99] Jointness Anit Mukherjee, "Fighting Separately: Jointness and Civil-Military Relations in India," *Journal of Strategic Studies* 40, no. 1–2 (2017): 6–34; Joel Wuthnow, "A Brave New World for Chinese Joint Operations," *Journal of Strategic Studies* 40, no. 1–2 (2017): 169–95; Goldman, "Introduction: Military Diffusion and Transformation," 16.

[100] For a comprehensive analysis of the role of culture on the development of the U.S. military's cyber doctrine, see: Sarah P. White, "Subcultural Influence on Military Innovation: The Developmentof U.S. Military Cyber Doctrine" (Dissertation, Cambridge, Massachusetts, Harvard University, 2019).

[101] Goldman, "Cultural Foundations of Military Diffusion," 74.

likelihood that the military opts to change the organizational model of cyber forces to achieve more unorthodox and innovative force structure.

In contrast to organizational size and adoption-capacity, cultural logics do not routinely account for a military's pool of potential resources. Although culturally open militaries may desire to expand and fully implement a cyber force, they may lack the resources to do so. Cultural openness and organizational size may also, to a certain extent, overlap: larger militaries are more conducive to the development of distinct, service-level subcultures that can compete with one another to produce diverse approaches to an innovation.[102]

Conclusion

This chapter has advanced three core claims. The first is that implementing an innovation constitutes a process; as such, diffusion studies require a more nuanced framework for understanding how innovations change over the course of implementation. To these ends, I have proposed a novel framework for implementation based on five discrete stages: Pre-Adoption, Introduction, Modification, Expansion, and Full Implementation. Second, I have asserted that the implementation of cyber forces is characterized by a tension between developing the capacity to carry out the cyber mission and integrating into the defense bureaucracy to develop interagency power and influence. Both are crucial to implementing cyber forces. The issue at the heart of implementation efforts is how to prioritize these objectives.

Finally, I argue that organizational size is an important factor that helps shape implementation dynamics and predisposes implementers to initially prioritize mission-building or bureaucracy-building. In short, larger organizations possess a greater tolerance for risk and a greater pool of resources; however, larger organizations also possess a greater number of

[102] White, "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine."

competing interests. As such, cyber forces can more easily be introduced into the military ecosystem and subsequently expanded. Yet, implementers are likely to prioritize bureaucratic integration to position a nascent cyber force to compete for autonomy and influence. Conversely, smaller organizations have less tolerance for risk and smaller resource bases but fewer bureaucratic competitors. Accordingly, implementers in small organizations are likely to focus on building the cyber mission and pushing for additional resources for expansion without extensive bureaucratic negotiation. In both large and small organizations, providing "proof of concept" by linking operational effects to broader strategic interests is likely to influence the full implementation of cyber forces. Because larger organizations have a broader portfolio of strategic interests than smaller organizations, implementers in large militaries are likely to have more opportunities to prove the worth of cyber forces.

As laid out in the research design section of the introductory chapter, the next three chapters of this dissertation evaluate the explanatory power of my theory to highlight the importance of organizational size. Chapter 4 presents my quantitative analysis. Through a combination of survival models—a stratified Cox model and a multistate survival model—this chapter tests the hypotheses derived from my theory and establishes broad trends in implementation. Chapters 5 and 6 offer within-case qualitative analyses. Using process tracing, I examine the evolution of two cyber forces: the United States' U.S. Cyber Command (Chapter 5); Estonia's Cyber Command (Chapter 6). Importantly, the U.S. case study examines implementation in a large military organization; Chapter 6 on Estonia assesses implementation patterns in a small military. In each case, I interrogate my theorized causal mechanisms and differentiate the them from the mechanisms associated with adoption-capacity and organizational culture. In doing so, I investigate the utility of my theory—in conjunction with the alternative explanations—with a combination of historical and original interview data. Ultimately, the incomplete accounts provided by the alternative explanations highlight the importance of theorizing organizational size. The concluding chapter provides a preliminary extension of the theory to Germany’s Cyber and Information Domain Service (Chapter 7).

CHAPTER 4

Modeling Cyber Force Implementation Dynamics

Introduction

This chapter provides a quantitative test of the hypotheses laid out in Chapter 3. The first section of this chapter summarizes the main arguments of the previous theory chapter: that implementing an innovation is best conceptualized as a process consisting of stages that includes adoption decisions; and that size is the primary factor shaping implementation pathways. The second section discusses the measurement of key variables. Much of this section is devoted to operationalizing the dependent variable—specifically, probability of experiencing a transition event between implementation stages at a given point in time. Accordingly, this section elaborates how implementation stages relate to changes in cyber force structure and identifies the range of possible transitions. The third section details the modeling strategy as well as issues with the data that require attention. The fourth section presents and discusses the results of two statistical models: a stratified Cox model addressing the entire implementation process; and a multistate survival model that assesses transitions between specific implementation stages. Subsequently, the chapter concludes by summarizing and looking forward to the two case study chapters that follow.

Recap: Theory and Hypotheses

The previous chapter has argued that the implementation of cyber forces is a process that unfolds across a series of five interconnected stages: pre-adoption, introduction, modification, expansion, and full implementation. Implementation can proceed in nonlinear patterns, and implementers may not pass through each stage (i.e. they may skip certain stages altogether).

Substantively, the implementation of cyber forces is characterized by a tension between two competing goals that pull implementation resources in opposing directions: building an organization that operates effectively in the cyber domain and integrating that organization into the existing defense bureaucracy. Fully implementing cyber forces requires achieving both goals by creating an “ambidextrous” organization: cyber forces must be efficient in daily administrative and interagency processes while adapting to rapid changes in the operational environment. Implementers must therefore dedicate resources towards operational effectiveness in the cyber domain while retaining enough political capital to successfully navigate the broader bureaucratic ecosystem.

Because militaries can deal with this challenge in different ways, a variety of pathways to full implementation are possible. This is particularly true under the conditions of principle diffusion, where states and their militaries lack a dominant blueprint or roadmap for implementation. **Without clear direction for implementation, what explains the variation in implementation dynamics for cyber forces across militaries? In other words, what causes the implementation of cyber forces to unfold differently across militaries?**

I assert that organizational size—specifically, the size of a state’s military organizations—is a crucial variable shaping implementation dynamics.

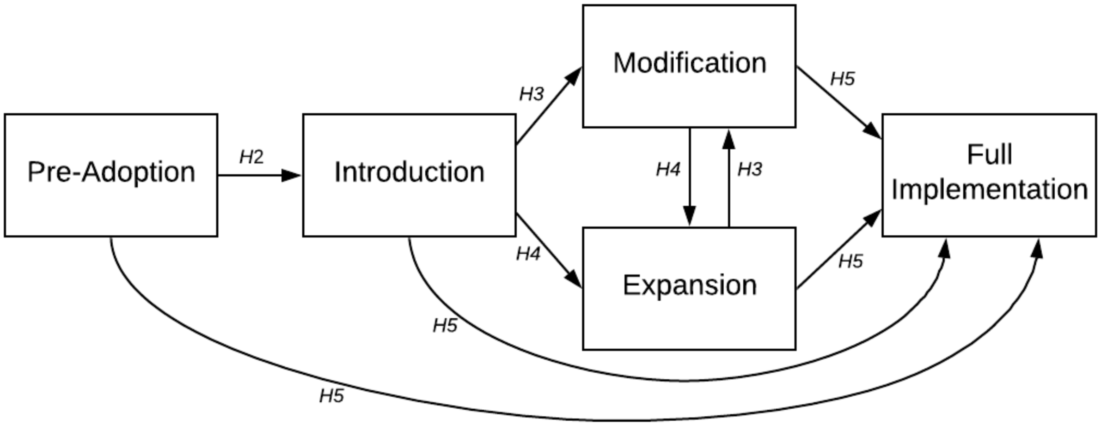
In short, larger militaries are more predisposed to initially prioritize the bureaucratic goal over the mission goal, while smaller militaries are more likely to focus on mission-building before pivoting to bureaucracy-building. Despite a greater risk tolerance and the availability (relative to smaller organizations) of human and financial capital to build out the cyber mission, larger militaries entail a greater number of competing interests that can threaten the autonomy of cyber forces or lay claim to the cyber mission. As such, implementers in larger militaries are more likely to address the bureaucratic integration and organizational survival of cyber forces before prioritizing mission-building. Conversely, smaller militaries are more likely to focus directly on mission-building. Implementers face a smaller pool of bureaucratic competitors in smaller militaries; however, smaller militaries possess a smaller resource base and lack the risk tolerance of larger militaries. Accordingly, implementers are more inclined to vigorously build out the cyber mission to justify an additional strain on financial and human capital. Subsequently, implementers in smaller militaries are likely to pivot to the bureaucratic imperative to increase the likelihood of securing resources in the future.

The argument advanced in Chapter 3 provided five hypotheses. These hypotheses span both the overall (H1) and stage-specific effects (H2-H5) of organizational size over time:

> ***H1: The relationship between military size and the risk of completing the implementation process is curvilinear.***
>
> ***H2: Larger militaries are more likely to transition into Introduction than smaller militaries.***
>
> ***H3: Cyber forces in larger militaries are more likely to transition into Modification than those in smaller militaries.***
>
> ***H4: Cyber forces in larger militaries are more likely to transition into Expansion than those in smaller militaries.***
>
> ***H5: Cyber forces in larger militaries are more likely to transition into Full Implementation than those in smaller militaries.***

Figure 4.1 summarizes a dynamic view of the implementation process with the corresponding stage-specific hypotheses.

Figure 4.1. A Dynamic Model of the Implementation Process with Corresponding Hypotheses.



Measurement

Dependent Variable: Probability of Transition Event over Time

To model the probability of experiencing a transition event over time, this section operationalizes the transitions between implementation stages. Moving between implementation stages rests on changes in cyber force structure. As such, operationalizing transitions between stages requires three important steps: (1) cataloguing the types of changes in cyber force structures; (2) explicating how these changes in force structure underlie changes in the implementation process; and (3) identifying the range of potential implementation transitions.

Changes in Cyber Force Structure. As conveyed in Chapter 2, The Dataset on Cyber Force Structures captures the changes in cyber force structure. Tables 4.1, 4.2, and 4.3 provide an overview of the changes in force structures over time. Table 4.1 summarizes the raw data on transitions between cyber forces structures, while Tables 4.2 and 4.3. shed light on changes in organizational models and scales of command, respectively. A total of 90 cyber force structure transitions have occurred from 2000-2018. Immediately worth noting is that, once a cyber force has been created, there have been no transitions back to No Cyber Force.

Table 4.1. Number of Observed Transitions between Force Structures, 2000-2018

	Next Force Structure									
		Branch			*Service*			*Joint*		
	Subord.	Sub-Uni.	Unified	Subord.	Sub-Uni.	Unified	Subord.	Sub-Uni.	Unified	
Current Force Structure										**Total Transitions**
No Cyber Force	27	8	1	11	1	0	1	3	2	54
Subord. Branch	---	7	3	0	1	2	3	0	1	17
Sub-Uni. Branch	0	---	1	0	0	0	1	0	2	4
Unified Branch	0	0	---	0	0	0	0	0	0	0
Subord. Service	0	1	0	---	2	0	1	1	1	6
Sub-Uni. Service	0	0	0	0	---	0	0	0	1	1
Unified Service	0	0	0	0	0	---	0	0	0	0
Subord. Joint	0	0	0	0	0	0	---	5	0	5
Sub-Uni. Joint	0	0	0	0	0	0	0	---	3	3
Unified Joint	0	0	0	0	0	0	0	0	--	0
										90

Note: --- indicates same stage transition

Source: The Dataset on Cyber Force Structures

The creation of an initial force structure (i.e. any transition from No Cyber Force) accounts for the bulk of transitions that have occurred (54 of the 90 total transitions: 60%). By far, the most common transition has been from No Cyber Force to a Subordinated Branch force structure. This has accounted for 30% of all transitions that have occurred in Table 4.2 (27 out of 90 transitions). Transitions from No Cyber Force into Subordinate Service (11 out of 90, 12.2%) and Subordinated Joint (1 out of 90, 0.01%) have occurred much less frequently.

More broadly, Table 4.1 indicates that most initial cyber force structures result in Subordinated commands—which includes transitions from No Cyber Force into Subordinated Branch, Subordinated Service, or Subordinated Joint force structures—and represent 39 out of 90 total command transitions (43.3%). The Branch model is also the most common selection for initial force structures, with transitions from No Cyber Force into a Branch model numbering 39 out of the 54 total model selection decisions (72.2%).

As noted in Chapter 2 the variation in organization models increases over time. Table 4.2 also details "model switching", i.e. the change from one organizational model to another. **Model switching has only occurred 15 times**; despite the small sample, changes generally tend to favor the selection of a Joint model. Militaries utilizing the Branch model have changed to a Joint model seven times (compared to three transitions from a Branch to Service model). Those employing a cyber force structure based on a Service model have transitioned into a Joint model four times as opposed to one transition into the Branch model. Notably, once a Joint model has been selected, there has been no further model change. Table 4.3 indicates that changes to command levels are more frequent than model switching in Table 4.2.

Table 4.2. Organizational Model Selection Dynamics, 2000-2018

Current	**Next Organizational Model**			
Organizational Model	Branch	Service	Joint	**Total**
No Cyber Force	36	12	6	54
Branch	---	3	7	10
Service	1	---	4	5
Joint	0	0	---	0
Total	37	15	17	69

Source: The Dataset on Cyber Force Structures

Table 4.3. Command Change Dynamics, 2000-2018

Current	**Next Command Level**			
Command Level	Subordinated	Sub-Unified	Unified	**Total**
No Cyber Force	39	12	3	54
Subordinated	4*	17	7	28
Sub-Unified	1	0*	7	8
Unified	0	0	0*	0
Total	44	29	17	90

*Transitions into the same command level are included in this table only when a model change has occurred.

Source: The Dataset on Cyber Force Structures

Although the initial creation of a cyber force accounts for over half of the command selection dynamics (54 out of 90 total, 60%), 40 percent of cyber force structures have experienced some sort of change. This table does include four transitions into the same force structure as the current; this is documented to capture *de facto* changes to the nature of the command due to a change in organizational model. Overwhelmingly, changes in force structure tend to lead to greater levels of command. Subordinated commands have transition into Sub-Unified commands 17 times and into Unified commands three times. Sub-Unified commands generally transition into Unified commands (seven out of eight transitions), with one transition into a Subordinated command. Table 4.1 shows that this transition was from a Sub-Unified Branch into a Subordinated Joint cyber force structure. Finally, the data indicates that Unified commands do not change: there have been no transitions into any other command level, and there have been no model switching from Unified commands (as evidenced by no transitions from a Unified to another Unified command). As of 2018, only 17 states have reached a Unified command level.

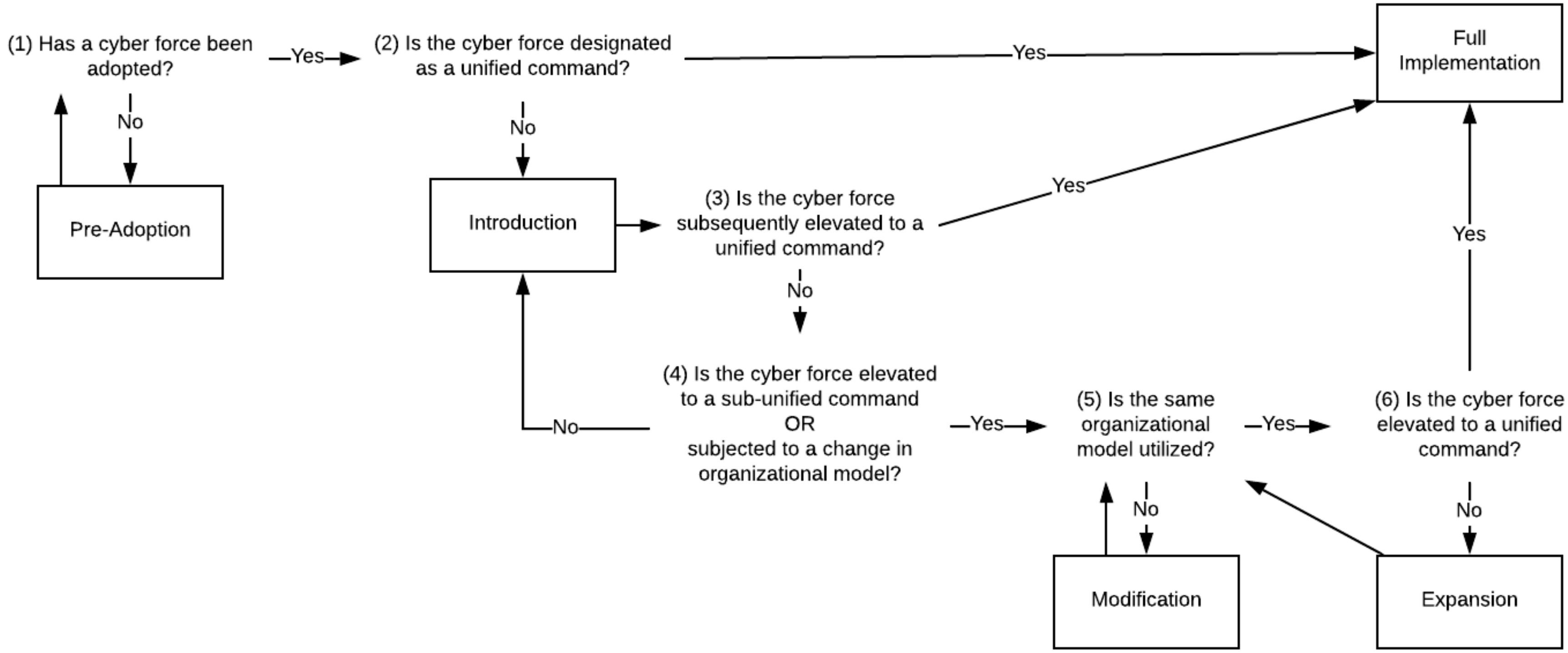
Several insights emerge from this brief overview. First, most initial cyber force structures tend to take on Subordinated commands. Second, subsequent changes in force structures generally entail an increase in the level of command. Third, while model switching is relatively infrequent (representing 15 of the 90 total transitions, 16.7%), cyber forces (with one exception) tend to move into the combat subsystem by adopting either a Service or Joint model. Fourth, the Joint model appears to be a terminal model—once the military moves to a Joint model, it will not transition into any other organizational model. Finally, once a Unified command is reached, there are no subsequent changes in the cyber force's organizational model or command level.

How Changes in Cyber Force Structure Define Implementation Stages. Table 4.4 below summarizes the operationalized definitions for each implementation stage; Figure 4.2 gives additional detail by providing the coding schema used to define implementation stages according to changes in cyber force structures. **Militaries with no cyber force occupy the Pre-Adoption stage. The creation of an initial (non-Unified) cyber force moves militaries from Pre-Adoption into Introduction. Militaries enter Modification after changing the organizational model underpinning cyber force structure; these changes result in a non-Unified command. Expansion entails an increase to the cyber force's scale of command. Expansion hinges on the organizational model matching the previously occupied stage and excludes increases to Unified commands. Finally, Full Implementation coincides with the creation of Unified command for cyber forces.**

Table 4.4. Operationalizing Implementation Stages

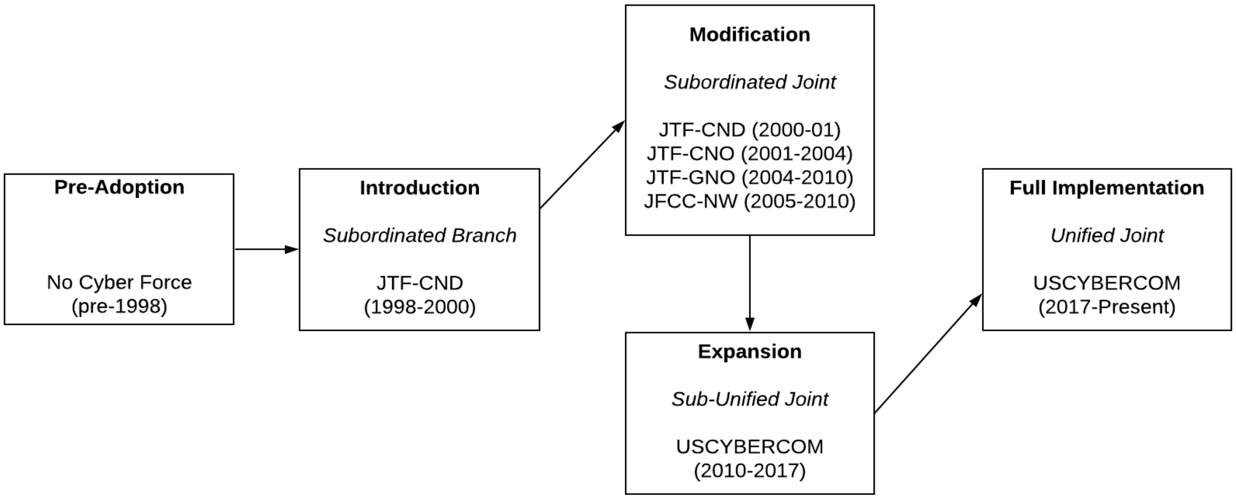
	Stage	Operational Definition
1.	Pre-Adoption	No cyber force.
2.	Introduction	The initial (non-unified) cyber force structure adopted by the military. Can include any organizational model and Subordinated or Sub-Unified command structures.
3.	Modification	Any change in organizational model from the force structure in the Introduction stage. This can include (but does not require) changes in the command level. Excludes any changes that result in Unified commands.
4.	Expansion	An increase in the scale of command; organizational model must match organizational model from the previous stage (otherwise, it is defined under the Modification stage). Expansion occurs only when the previous force structure maintains a Subordinated command.
5.	Full Implementation	The creation of a unified cyber force structure, regardless of the previous stage's organizational model or command structure.

Figure 4.2. Coding Schema for Mapping Changes in Cyber Force Structure onto Implementation Stages


(1) Has a cyber force been adopted?
Yes
(2) Is the cyber force designated as a unified command?
Yes
Full Implementation
No
Pre-Adoption
No
Introduction
(3) Is the cyber force subsequently elevated to a unified command?
Yes
Yes
No
(4) Is the cyber force elevated to a sub-unified command OR subjected to a change in organizational model?
No
Yes
(5) Is the same organizational model utilized?
Yes
(6) Is the cyber force elevated to a unified command?
No
No
Modification
Expansion

A brief look at the development of the United States' force structure provides an example of this operationalization. Before 1998, the U.S. maintained no cyber force, and was thus in the Pre-Adoption Stage. The first cyber force was the Joint Task Force – Computer Network Defense (JTF-CND), established in late 1998 under the Defense Information Systems Agency, a logistical agency. The creation of JTF-CND as a subordinated branch moved the U.S. into the Introduction stage. In 2001, JTF-CND was reassigned to a combatant command (U.S. Space Command); this move modified the organizational model of JTF-CND from a branch to a joint model. Subsequent iterations of JTF-CND (Joint Task Force – Computer Network Operations [JTF-CNO], Joint Task Force – Global Network Operations [JTF-GNO], and Joint Functional Component Command – Network Warfare [JFCC-NW]) reported to U.S. Strategic Command and retained a subordinated joint force structure. The U.S. entered the Expansion stage with the creation of U.S. Cyber Command (USCYBERCOM) as a sub-unified combatant command in 2010. The U.S. reached Full Implementation with the elevation of USCYBERCOM to a fully unified joint combatant command in August 2017. Figure 4.3 visualizes these changes.

Figure 4.3. The Implementation of U.S. Cyber Force Structure over Time



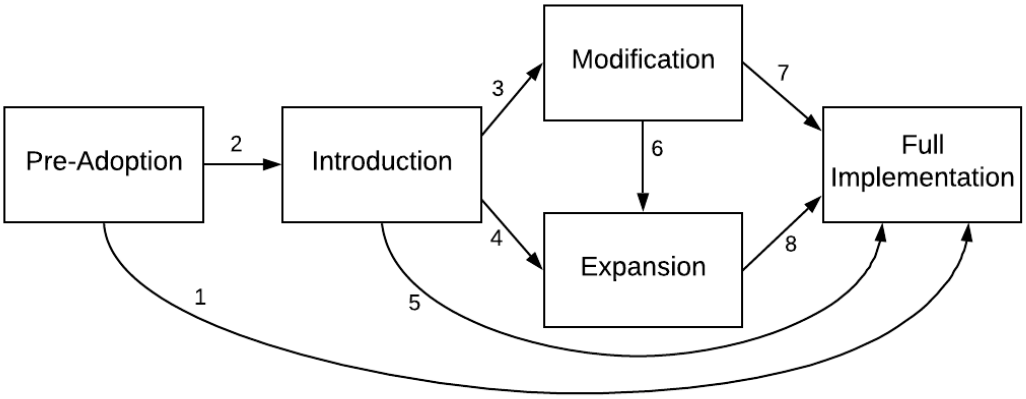
Identifying Potential Transitions. The potential transitions between stages provides a more dynamic and realistic portrayal of the implementation process. All militaries begin in Pre-Adoption. Full Implementation represents the absorbing state—once reached, militaries cannot transition to any other stages. Introduction, Modification, and Expansion are intermediate stages. There are two logical transitions out of the Pre-Adoption stage: Full Implementation with the adoption of a Unified cyber force structure (Transition #1); or Introduction through the creation of a Subordinated or Sub-Unified cyber force (Transition #2). There are three potential transitions out of Introduction: the modification of the cyber force's original organizational model (Transition #3), an expansion of the scale of command (Transition #4), or a move to Full Implementation via creating a Unified force structure (Transition #5). After reaching Modification, militaries can move into Expansion (Transition #6) or Full Implementation (Transition #7) depending on how the command has been elevated. Finally, militaries can leave the Expansion stage by restructuring cyber forces into a Unified force structure (Transition #8).[1] Table 4.5 summarizes these transitions and Figure 4.4 portrays potential pathways.

Table 4.5. Potential Transitions according to Current and Next Implementation Stages

Transition #	Current Stage	Next Stage
1	Pre-Adoption	Full Implementation
2	Pre-Adoption	Introduction
3	Introduction	Modification
4	Introduction	Expansion
5	Introduction	Full Implementation
6	Modification	Expansion
7	Modification	Full Implementation
8	Expansion	Full Implementation

[1] Although it may be possible to transition from Expansion to Modification, the more likely scenario is that changes to the organizational model occur in the transition from Expansion to Full Implementation. Expansion implies an increase in cyber forces' bureaucratic turf; as such, changes in the organizational model are only likely to be accepted if it is accompanied by the greater resources associated with reaching Full Implementation.

Figure 4.4. A Dynamic Model of the Implementation Process by Transition Number



Independent variable: Organizational Size

Two predominant measures of organizational size are the total number of personnel and the financial resources at the disposal of the organization. As personnel represents the more direct and most frequently used measure in organizational studies,[2] I use the total number of active-duty military personnel as my primary measure of size.

At the same time, models must account for spending in some manner to avoid omitted variable bias. However, I avoid using total military spending, as this would include a highly correlated second measure of organizational size and could wash out the actual statistical effects of size. To these ends, I focus on military spending per soldier—specifically, military spending (in USD million) per 1,000 soldiers.[3] Using this measure captures the possibility that militaries can increase (or decrease) spending levels without changing overall size (in terms of personnel). Total military spending (in USD million) is used as an alternative measure in the robustness checks in Appendix 1.

[2] Camison-Zornoza et al., “A Meta-Analysis of Innovation and Organizational Size,” 337.

[3] Former Commander of U.S. Cyber Command General Keith Alexander has suggested that effectively developing an initial cyber force requires about 1,000 soldiers. .James A. Lewis, “Managing New Style Warfare: An Interview with Keith Alexander,” Cyber From the Start, accessed May 10, 2019, https://www.csis.org/podcasts/cyber-start.

Because each of these measures exhibit positive skewness, I log-transform each measure to normalize them and facilitate subsequent modeling. Logging personnel and spending measures is a common practice in organizational studies.[4] To test Hypothesis 1 in the full implementation process model, I include a squared term for the logged personnel measure (the same method is used for spending in the robustness checks. Due to the narrowing of subjects throughout the implementation process, the squared term is dropped in the transition-specific model.

Control Variables

Although organizational size should primarily influence the adoption and implementation of cyber forces, statistical models must account for other factors that facilitate or inhibit adoption and implementation efforts.[5] Accordingly, I include several control variables.

Latent Cyber Capabilities. A state's cyber capabilities should play a critical role in the ability to implement cyber forces. In testing the effect of cyber capabilities on coercive concessions, Valeriano et al. (2018) construct a latent cyber capacity index as a proxy for a state's cyber capabilities. This index captures the infrastructure and knowledge capital from which cyber power is built. The index normalizes six measures before averaging them into a single score. For each country, these measures include: the number of broadband subscriptions per 1,000 people; the number of secure Internet servers per 1 million people; the percentage of high technology exports out of total manufacturing exports; the number of Internet users per 1,000 people; the total number of scientific and technical journal articles published; and the number of residents who have applied for patent applications per year.[6] To account for the

[4] Damanpour, "Organizational Size and Innovation," 386; Camison-Zornoza et al., "A Meta-Analysis of Innovation and Organizational Size," 336.

[5] Camison-Zornoza et al., "A Meta-Analysis of Innovation and Organizational Size," 338.

[6] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York, NY: Oxford University Press, 2018), 59–60; n.10, 152. Data for each measure is taken from the World Bank's World Development Indicators. The World Bank, "World Development Indicators" (Washington, D.C.: The World Bank, 2018).

possibility that there may be a threshold effect for cyber capabilities and implementation, the full implementation model includes a squared measure of the latent cyber capacity index. The squared measure is dropped for the transition-specific model.

Government Cybersecurity Expertise. While states may have the latent cyber capabilities to implement cyber forces, governments may lack sufficient cybersecurity expertise. As with latent cyber capabilities, there may be a threshold effect with expertise. Moreover, expertise can influence implementation decisions: as epistemic communities[7] exchange ideas, they can influence the design and redesign of cyber force structures. To capture the government's degree of cybersecurity expertise, I use an interval measure derived from Mechkova et al. (2019).[8] In the full implementation model, I include a squared measure of cybersecurity expertise. The squared measure is dropped for the transition-specific model.

Regime. Domestic political institutions can affect the adoption and implementation of cyber forces. Gartzke (2001) and Caverly (2014) have noted that democracies tend to have more capital-intensive militaries; this may predispose them to invest in cyber forces.[9] At the same time, centralized institutions in autocracies can facilitate wide-ranging implementation;[10] similarly, Dyson (2008) suggests that, even within democratic regimes, different levels of

[7] "An epistemic community is a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area." P. M. Haas, "Introduction: Epistemic Communities and International Policy Coordination," *International Organization* 46, no. 1 (1992): 3.

[8] Valeriya Mechkova et al., "Measuring Internet Politics: Introducing the Digital Society Project (DSP)," Working Paper #1 (Varieties of Democracy (V-Dem) Project, May 2019). The ordinal measure from Mechkova et al. (2019) is converted by the V-Dem team into an interval measure. See: Daniel Pemstein et al., "The V-Dem Measurement Model: Latent Variable Analysis for Cross-National and Cross-Temporal Expert-Coded Data," V-Dem Working Paper (University of Gothenburg: Varieties of Democracy Institute, 2020).

[9] Erik Gartzke, "Democracy and the Preparation for War: Does Regime Tyupe Affect States' Anticipation of Casualties?," *International Studies Quarterly* 45, no. 3 (2001): 467–84; Jonathan D. Caverley, *Democratic Militarism: Voting, Wealth, and War* (New York: Cambridge University Press, 2014). Fuhrmann and Horowitz (2017) find that the relationship between regime and acquisition of unmanned aerial vehicles (UAVs) is curvilinear. Matthew Fuhrmann and Michael C. Horowitz, "Droning On: Explaining the Proliferation of Unmanned Aerial Vehicles," *International Organization* 71 (2017): 397–418.

[10] Goldman, "Introduction: Military Diffusion and Transformation," 8–9.

executive constraints shape how innovations are implemented.[11] To capture regime type, I utilize the Electoral Democracy Index from the Varieties of Democracy Project (V-Dem). In the robustness check models, I utilize the Regimes of the World Measure from the V-Dem Project.[12]

Strategic Environment. The strategic and competitive environment can incentivize or deter the adoption and implementation of innovations.[13] In particular, the external environment can shape the timing of, strategies for, and extent to which militaries pursue innovation and implementation.[14] To account for the effect of the external environment, I deploy two measures: one that captures the total number of engagements in military conflicts and one that captures the overall intensity of the conflicts in which the military is engaged. For both measures, I use data from the Uppsala Conflict Data Program.[15]

Diffusion. To capture the effects of systemic diffusion, **I create a variable that measures the geometric distance of each state's cyber force structure from the overall cyber force composition of the international system.[16]** In essence, this measures a state's distance from the "global standard" for cyber force structure at a given point in time. For individual states, force structures are coded to capture the extent to which an organizational model is implemented. States are sorted by organizational model using binary variables; (0 if the

[11] T. 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.
[12] Michael Coppedge et al., "V-Dem [Country-Year] Dataset V10" (University of Gothenburg: Varieties of Democracy Institute: Varieties of Democracy (V-Dem) Project, 2020).
[13] Damanpour, "Organizational Size and Innovation," 393–94.
[14] Resende-Santos, *Neorealism, States, and the Modern Mass Army*; Joao Resende-Santos, "Anarchy and the Emulation of Military Systems," *Security Studies* 5, no. 3 (1996): 193–260; Elman, "The Logic of Emulation: The Diffusion of Military Practices in the International System"; Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics*.
[15] Specifically, I use the UCDP Dyadic Dataset to determine state actors participating in conflict. Lotta Harbom, Erik Melander, and Peter Wallensteen, "Dyadic Dimensions of Armed Conflict, 1946-2007," *Journal of Peace Research* 45, no. 5 (2008): 697–710; Therese Pettersson, Stina Hogbladh, and Magnus Oberg, "Organized Violence, 1989-2018 and Peace Agreements," *Journal of Peace Research* 56, no. 4 (2019)..
[16] The dyadic approach outlined below follows the guidance of Gilardi (2014); for more detail, see: F. Gilardi, "Methods for the Analysis of Policy Interdependence," in *Comparative Policy STudies*, ed. Isabelle Engeli and Christine Rothmayr Allison (Springer, 2014), 185–204.

organizational model is not used, 1 if the model is used); force structures are subsequently weighted by scale of command (0.33 for subordinated, 0.66 for sub-unified, and 1 for unified). For example, a state with a Subordinated Branch force structure would have a score of 0 for the service model variable, a score of 0 for the joint model variable, and a score of 0.33 for the branch model variable.

The force structure score of the international system aggregates all state-level scores by (1) summing all state scores by month and (2) dividing the sum by the total number of states with a cyber force structure. This systemic measure captures both the distribution of models across the international system and the degree to which they are implemented via command levels. For example, in a scenario where three states have a Unified Branch, the system score would be 1 for the branch model measure and 0 for the service and joint model measures. This implies stronger systemic pressures to adopt a specific model compared to a scenario where different models populate the system score. In contrast, where three states have cyber forces but have Unified Branch, Unified Service, and Unified Joint force structures, the systemic score would be 0.33 for the Branch Model, 0.33 for the Service Model, and 0.33 for the Joint Model. In this case, systemic pressures to adopt a specific model are much weaker.

The geometric distance between a state's cyber force structure and the systemic distribution of cyber force structures are subsequently calculated by (1) subtracting the system score from the individual state score for each of the three weighted model measures, (2) squaring the results, and (3) taking the square root of the summed results. The formula below summarizes this final step:

$$Euclidean\ Distance = \sqrt{\begin{gathered}(State\ Weighted\ Branch\ Score - System\ Weighted\ Branch\ Score^2) + \\ (State\ Weighted\ Service\ Score - System\ Weighted\ Service\ Score)^2 + \\ (State\ Weighted\ Joint\ Score - System\ Weighted\ Joint\ Score)^2\end{gathered}}$$

The result is a single score that measures the geometric distance of the state's force structure from the systemic distribution. The higher the score, the greater the difference between the state's force structure and the systemic composition of force structures. The lower the score, the closer the state is to the systemic distribution.

Additional variables are discussed and included in the robustness checks in Appendix 2 of this dissertation.

Methods: Multistate Modeling and Data Issues

This chapter employs two main survival modeling strategies to test the hypotheses listed above. First, I utilize a stratified Cox model to assess the overall effect of size on the risk of transitioning through the entire implementation process, thus testing Hypothesis 1. By stratifying according to specific transitions, the stratified Cox model aggregates all transition events but allows the baseline hazard to vary across transitions while assuming common covariate effects over time for each transition. Additionally, stratification is useful for risks where the occurrence of an event does not necessarily entail exiting the sample.[17] This strategy thus provides initial insight into the variables driving implementation dynamics.

The second strategy involves multistate survival modelling to test Hypotheses 2-5. Although used extensively in epidemiology and biomedical studies,[18] multistate modeling remains rare in political science.[19]As an extension of Cox models,[20] multistate models are

[17] Box-Steffensmeier and Jones, *Event History Modeling: A Guide for Social Scientists*, 176.

[18] For a comprehensive overview of applying multistate models to these fields, see: Cook and Lawless, *Multistate Models for the Analysis of Life History Data*.

[19] Several recent exceptions include: Jones and Metzger, "Evaluating Conflict Dynamics: A Novel Empirical Approach to Stage Conceptions"; Webster, "Rethinking Civil War"; Barrie, "The Process of Revolutionary Protest: Development and Democracy in the Tunisian Revolution of 2010-2011"; Ari, "Uncrossing the Rubicon: Transitions from Violent Civil Conflict to Peace"; Min, "Cheaper Talk: The Changing Nature of Wartime Negotiation in the Post-1945 Order."

[20] For a basic overview of the logic behind Cox models, see: Box-Steffensmeier and Jones, *Event History Modeling: A Guide for Social Scientists*, 8.

flexible enough to model a duration process comprised of multiple stages with a variety of process structures. Stages are defined based on failure events that a subject is at the risk of experiencing; these failure events represent transitions between stages.[21] In the context of implementation, multistate models can encompass not only the initial transitions within implementation processes (i.e. adoption), but also the intervening transitions and the termination of the process. Like stratified Cox models, multistate models allow transitions to have different underlying rates of occurrence by permitting baseline hazards to vary across transitions. However, multistate models offer two additional advantages. Unlike stratified Cox models, multistate models allow for transition-specific covariates. By allowing the effects of covariates to vary according to transition, multistate models can capture the theoretically differential impact of independent variables at different stages of implementation. Additionally, using a multistate model enables the calculation of unique transition probabilities based on specific covariate profiles.[22]

Data

Tables 4.6 and 4.7 provide some descriptive information about the data.[23] Although 172 countries are included in the dataset, 17 countries have been dropped as insignificant outliers leaving 155 countries for statistical analysis.[24] Table 4.6 contains information about the number

[21] On how this approach differs from competing risks models, see: Metzger and Jones, "Surviving Phases: Introducing Multistate Survival Models."

[22] Metzger and Jones; Jones and Metzger, "Evaluating Conflict Dynamics: A Novel Empirical Approach to Stage Conceptions." My approach follows Metzger and Jones (2016) and Jones and Metzger (2016) to satisfy the Markov assumption, i.e. all relationships and probabilities rest on the current stage of occupation and not the entire life history up to a given point.

[23] On the structure of multistate data, see: Liesbeth C. de Wreede, Marta Fiocco, and Hein Putter, "The Mstate Package for Estimation and Prediction in Non- and Semi-Parametric Multi-State and Competing Risks Models," *Computer Methods and Programs in Biomedicine* 99, no. 3 (2010): 261–74.

[24] Countries with fewer than 1,500 total active military personnel and countries without any data on military spending, personnel, or a host of control variables have been excluded. These include: Antigua and Barbuda, Bahamas, Belize, Brunei Darussalam, St. Kitts and Nevis, Maldives San Marino, Tonga, Bhutan, Comoros, Sao Tome and Principe, Seychelles, Barbados, Gambia, Cabo Verde, Timor-Leste, and Equatorial Guinea.

of militaries to occupy each stage and the average length of time spent in each stage. While hypotheses have been formulated in terms of risk of event occurrence over time, the following duration information provides useful insight into the data. All militaries in the dataset—aside from the seven countries (the United States, Russia, China, Israel, North Korea, Greece, and Thailand) that are left-truncated—begin in the Pre-Adoption stage.[25] Most countries remain in this stage, and it has the longest average stage length of 210.74 months. 58 states have occupied the Introduction stage; on average, it takes militaries 122.27 months (slightly over 10 years) to transition out of this stage. Seven cyber forces have undergone Modification, which lasts 74.73 months on average (over six years). Expansion has the shortest spell length at 58.26 months on average (just under 5 years) before transitioning to Full Implementation. Twelve militaries have occupied the expansion stage. Only 17 states have completed the implementation process, i.e. transitioned into a Unified cyber force structure. On average, the entire implementation process takes 196.24 months to complete—over 16 years.

Table 4.7 describes each potential implementation pathway and its observed frequency in the dataset. Most militaries reaching a Unified cyber force structure (10 out of 17) have followed the pathway of Pre-Adoption → Introduction → Full Implementation. Three militaries have managed to undertake large-scale adoption and implementation via Pre-Adoption → Full Implementation. Only four militaries have taken more incremental pathways to a Unified cyber force: Pre-Adoption → Introduction → Expansion → Full Implementation and the Pre-Adoption → Introduction → Modification → Expansion → Full Implementation pathways have both occurred twice. One pathway (Pre-Adoption → Introduction → Modification → Full Implementation) has not yet been observed.

[25] "Left-truncation emerges in event history data sets when history prior to the first observation point is unobserved. Box-Steffensmeier and Jones, *Event History Modeling: A Guide for Social Scientists*, 16.

Table 4.6. Mean Stage Length in Months

Stage	N	Spell Length (mean, in months)
Pre-Adoption	148*	210.74
Introduction	58	122.27
Modification	7	74.73
Expansion	12	58.26
Complete Implementation Process	17	196.24

*155 countries total, 7 countries left truncated

Table 4.7. All Potential Implementation Pathways by Observed Frequency

	Pathway	N
1.	P → I → F	10
2.	P → F	3
3.	P → I → E → F	2
4.	P → I →M → E → F	2
5.	P → I →M → F	0
	Total	17

Note: P = pre-adoption; I = introduction; M = modification; E = expansion; F = full implementation.

Model Penalizations

Modeling the implementation process must account for two additional issues: rare events and missing data. Table 4.8 summarizes the number of events by each transition. A total of 89 transitions have occurred,[26] making the number observed transitions rare compared to the number of states at risk across the 18-year period covered by the dataset.

[26] Of the 90 raw transitions described in Table 4.1, only one is not captured in Table 4.6: Denmark's transition from the Offensive Cyber Warfare Unit (a Subordinated Branch cyber force structure) to the Computer Network Operations Unit (a Subordinated Joint cyber force structure). Because Denmark's initial cyber force structure at the Introduction stage was a Subordinated Service structure (the Army 3rd Electronic Warfare Company), the transition between the Offensive Cyber Warfare Unit and the Computer Network Operations Unit represents a second spell of Modification. As such, although a force structure change has occurred, Denmark remains in the Modification stage.

Table 4.8. Number of Observed Transitions

Transition #	Current Stage	Next Stage	*N*
1	Pre-Adoption	Full Implementation	3
2	Pre-Adoption	Introduction	51
3	Introduction	Modification	7
4	Introduction	Expansion	10
5	Introduction	Full Implementation	10
6	Modification	Expansion	4
7	Modification	Full Implementation	0
8	Expansion	Full Implementation	4
		Total:	89

Rare events become problematic for Cox models—overfitting models with rare events can produce biased estimates.[27] As a rule of thumb, analysts modeling rare events should aim for a ratio of one independent variable for every five to ten outcome events.[28] This same guideline can be extended to multistate models. However, as the number of stages and transitions increase, the number of observed transitions drop.[29] This pattern is observed in Table 4.6.

Where an insufficient number of observations exist within a specific transition, there are two potential solutions to reduce biased estimates in multistate models. First, transitions can be collapsed to decrease the number of transitions, thereby increasing the number of observations. A second solution is to hold covariate effects constant across transitions; limiting the number of

[27] For further discussion, see: Menelaos Pavlou et al., “How to Develop a More Accurate Risk Prediction Model When There Are Few Events,” *The British Journal of Medicine* 351 (2015): 1–5; G. Ambler, S. Seaman, and R. Z. Omar, “An Evaluation of Penalised Survival Methods for Developing Prognostic Models with Rare Events,” *Statistics in Medicine* 31 (2012): 1150–61; Robert Tibshirani, “The Lasso Method for Variable Selection in the Cox Model,” *Statistics in Medicine* 16 (1997): 385–95.

[28] Eric Vittinghoff and Charles E. McCulloch, “Relaxing the Rule of Ten Events per Variable in Logistic and Cox Regression,” *American Journal of Epidemiology* 165, no. 6 (2007): 710–18.

[29] A similar issue occurs in repeated spells models: as the number of occurrences increases, the number of observations is likely to decrease A. Colin Cameron and Pravin K. Trivedi, *Microeconometrics: Methods and Applications*, 8th edition (New York and Cambridge: Cambridge University Press, 2009), 655–57..

transition-specific specific covariates in a multistate model can help with model convergence and increase the precision of estimates.[30]

Accordingly, I penalize this chapter's models in three ways that are theoretically and statistically justifiable. First, I reduce the number of total transitions by collapsing transitions #4 (Introduction → Expansion) and #6 (Modification → Expansion). Combining these transitions increases the number of observed transitions to 14 (ten observations from transition #4 and four observations from transitions #6). Statistically, variables maintain the same effects for both transitions. Theoretically, collapsing transitions implies that reaching the Expansion stage entails unique dynamics, regardless of the previous intermediate stage. Second, I collapse transitions #7 (Modification → Full Implementation) and #8 (Expansion → Full Implementation) into one to capture the transition from intermediate stages into Full Implementation. Although combining these transitions only result in four observed transitions, theoretical distinctions prevent any further consolidation with other transitions into Full Implementation. Change from Modification or Expansion to Full Implementation is more incremental in nature than the transitions from Pre-Adoption or Introduction into Full Implementation. As such, combining transitions to improve statistical fit would inappropriately combine transitions that are qualitatively different. For the final penalization, I hold several covariate effects constant across the multistate model. Specifically, the effects of the regime and strategic environment variables are held constant across the entire implementation process. This aids model convergence and helps to avoid overfitting the multistate model.[31]

[30] Metzger and Jones, "Appendix L of Surviving Phases: Introducing Multistate Survival Models."

[31] The results of the subsequent models are robust to alternative specifications of the transition-specific effects. For the key personnel and spending variables, the statistical significance of transition-specific effects remain at the same levels even after (1) holding the effects of all other variables constant across the model, and (2) allowing all other variables (except the strategic environment variables) to have transition-specific effects. Despite the robustness of these covariates, the three variable mentioned in the text are held constant across the model to improve the precision of estimates while allowing the more proximate variables—personnel, spending, government expertise, and latent

The second major issue that models must account for—particularly in the face of rare events—is missingness across the dataset. The dataset has a missingness rate of approximately 4.896% across all potential independent and control variables. Under normal circumstances, this would not be an issue; however, with rare events, listwise deletion of observations threatens to greatly reduce the number of observed outcomes. This is the case for my main statistical models: listwise deletion loses nine observed outcomes, roughly ten percent of all observed transitions. Moreover, this missingness biases regression results to report primarily on the more democratic regimes in the dataset. Missing data for more autocratic regimes is relatively unsurprising—democracies are much more likely to report or record values for the country-time data collected by the World Bank and other entities. However, this dynamic must be accounted for in some manner.[32] Therefore, I employ multiple imputation to address missingness as a source of bias.[33] Accordingly, I use predictive means matching[34] and produce five imputations for analysis.[35] Appendix 2 models the unimputed data along with additional robustness checks.

cyber capacity—to exert transition-specific effects. Models do not converge when either of the two strategic environment variables are allowed to have transition-specific effects.

[32] For a robust overview of the "advanced democracy bias" in data and the benefits of multiple imputation, see: Ranjit Lall, "How Multiple Imputation Makes a Difference," *Political Analysis* 24 (2016): 414–33.

[33] As such, data are not Missing Completely at Random (MCAR); it is more likely that data are Missing at Random (MAR), i.e. democracies are more likely to report military spending data than autocracies (under the assumption that regime type does not determine spending). In this case, listwise deletion introduces bias into regression estimates; multiple imputation can thus serve to reduce biased regression estimates while also recapturing lost variation in the outcome variable. On listwise deletion and multiple imputation, see: Vincent Arel-Bundock and Krzysztof J. Pelc, "When Can Multiple Imputation Improve Regression Estimates?," *Poltical Analysis* 26 (2018): 240–45; Thomas B. Pepinsky, "A Note on Listwise Deletion versus Multiple Imputation," *Political Analysis* 26 (2018): 480–88.

[34] Predictive means matching (PMM) is particularly appropriate for non-normally distributed variables such as those found in country-year data. For more on applying PMM, see: Katherine J. Lee and John B. Carlin, "Multiple Imputation in the Presence of Non-Normal Data," *Statistics in Medicine* 36 (2017): 606–17; Tim P. Morris, Ian R. White, and Patrick Royston, "Tuning Multiple Imputation by Predictive Mean Matching and Local Residual Draws," *BMC Medical Research Methodology* 14, no. 75 (2014): 1–13; Shaun R. Seaman, Jonathan W. Bartlett, and Ian R. White, "Multiple Imputation of Missing Covariates with Non-Linear Effects and Interactions: An Evaluation of Statistical Methods," *BMC Medical Research Methodology* 12, no. 46 (2012): 1–13; Ian R. White, Patrick Royston, and Angela M. Wood, "Multiple Imputation Using Chained Equations: Issues and Guidance for Practice," *Statistics in Medicine* 30 (2011): 377–99.

[35] The number of imputations should be at least equal to the percentage of incomplete cases across the entire dataset. For additional guidance on this rule of thumb, see: White, Royston, and Wood, "Multiple Imputation Using Chained Equations: Issues and Guidance for Practice," 387–88.

Results

The Overall Implementation Process

Table 4.9 presents the results of the stratified Cox model; for interpretation purposes, coefficients are reported.[36] Positive coefficients indicate that the corresponding variable is associated with a higher hazard ratio, i.e. a one unit increase in the variable increases the relative risk of completing the implementation process. Negative coefficients are associated with a lower hazard ratio: a one-unit increase in the respective variable reduces the relative risk of completing implementation. In effect, variables with positive coefficients reduce the median duration of the implementation process, while variables with negative coefficients increase the median duration time of the implementation process. To avoid violating the proportional hazards assumption, I include a covariate that interacts my diffusion measure with time.[37]

Consistent with my expectations for Hypothesis 1, military size as measured by personnel exhibits a curvilinear relationship to the risk of completing implementation over time. The coefficients of the personnel and squared personnel variables indicate that initial increases in organizational size increases the likelihood of transitioning from one stage of implementation into another over time. After a certain point—as indicated by the squared term—increases in size decrease the odds of transitioning from one stage to another. Both coefficients are statistically significant at or above the 95% confidence level.

[36] Interpretation of covariate effects follows the guidelines of Benjamin T. Jones and Shawna K. Metzger, “Different Words, Same Song: Advice for Substantively Interpreting Duration Models,” *Political Science & Politics* 52, no. 4 (2019): 691–95.

[37] Because the data has been imputed, normal PH tests are unavailable in Stata. Therefore, I test the PH assumption in two ways: by including time-varying covariates in the regression to assess significance levels; and by extracting individual imputations and assessing PH violations on each imputation to identify common variables that violate the PH assumption.

Table 4.9: Stratified Cox Model of the Implementation Process

Variables	B/(SE)
Log Total Military Personnel	2.721** (1.033)
Log Total Military Personnel Squared	-0.096* (0.045)
Log Military Spending (USD mil) per 1000 Soldiers	0.282* (0.138)
Government Expertise	2.141* (1.021)
Government Expertise Squared	-0.200* (0.089)
Latent Cyber Capacity	3.387*** (0.897)
Latent Cyber Capacity Squared	-0.248** (0.097)
Democratic Regime	2.539*** (0.642)
Total Active Conflicts	0.577† (0.336)
Intensity of Strategic Environment	-0.305 (0.205)
Diffusion	12.311* (4.966)
Diffusion x Time	-0.074* (0.029)

Note: *p ≤ .05. **p ≤ .01. ***p ≤ .001. †p ≤ .10. Standard errors reported in parentheses. N = 72,006. Failures=89. Imputations = 5.

Specifically, initially each one-unit increase in the log of the total military personnel (2.718 times increase in the total number of personnel) is associated with a 15.191% increase in the hazard ratio when holding all other variables constant. However, after a certain point, each additional one-unit increase in the log of total military personnel is associated with a 1.968% decrease in the hazard ratio (all other variables held constant). Substantively, this means that for every initial 10% increase in the total number of military personnel, there is (holding all other variables constant) an associated 1.294% increase in the hazard of transitioning between implementation stages. Subsequently, after a given point, for each additional 10% increase in the total number of military personnel, there is (holding all other variables constant) a corresponding 0.908% decrease in the hazard of transitioning between implementation stages.

Several other statistically significant relationships are worth noting from this model. Spending per soldier is significant at the 95% confidence level. Holding all other variables constant, a 10% increase in military spending (in USD million) per 1000 soldiers is associated with a 1.027% increase in the hazard of transitioning between implementation stages. In effect, increasing spending by 100 USD per soldier increases the relative risk of transition into the next stage of implementation by 1.027%. As anticipated, both government cybersecurity expertise and latent cyber capabilities exhibit threshold effects: the normal and squared measures indicate that after certain levels are reached, capabilities and expertise no longer accelerate the implementation process. Additionally, having a more democratic regime increases the hazard of transitioning between stages. In terms of the strategic environment, the total number of ongoing conflicts seems to incentivize transitions between implementation stages, albeit at the 90% confidence level. The intensity of these conflicts does not have a statistically significant effect.

Finally, the effect of diffusion is statistically significant. As the original distance between a state’s cyber force structure and the systemic composition of force structures increases, there is a corresponding increase in the hazard of transitioning between stages. Eventually, as seen in the interaction with time, this effect is reversed. Over time, increases in the distance between a state’s force structure and the systemic composition are associated with a decrease in the hazard of moving between implementation stages. This suggests that in the initial stages of diffusion, militaries are more likely to move through the implementation process despite drifting away from the systemic distribution of cyber forces. However, over time, moving away from the systemic distribution slows implementation, while conformity to systemic pressures (i.e. decreasing the geometric distance between a state’s force structure and the systemic composition) increases the hazard of moving through implementation stages. This provides evidence for claims that, while states may face few pressures to conform early in the diffusion process, systemic dynamics encourage conformity over time.

Transition-Specific Model

Table 4.10 presents the results of the multistate survival model; coefficients are reported for each variable according to specific transitions. Positive coefficients indicate that higher values of the corresponding variable increase the probability of observing that transition; negative coefficients indicate that higher values of the specific variable decrease the probability of observing that transition. To facilitate substantive interpretation, I provide simulated transition probabilities over time. As noted in the section on model penalizations, the effects of regime, total conflicts, and conflict intensity are held constant across each transition. To avoid violating the proportional hazards assumption, I include a covariate that interacts my diffusion measure with time for the Pre-Adoption → Introduction transition.

Table 4.10. Multistate Model of the Implementation Process

	Transition							
Covariates	P → F	P → I	I → M	I → E	I → F	M → E	M → F	E → F
Log Total Military Personnel	0.880	0.892***	0.772†	0.408	0.231	0.408	0.459	0.459
	(0.620)	(0.137)	(0.414)	(0.272)	(0.232)	(0.272)	(0.639)	(0.639)
Log Military Spending (USD mil) per 1000 Soldiers	0.695	0.444**	2.303*	1.535*	0.239	1.535*	-0.263	-0.263
	(0.580)	(0.156)	(1.084)	(0.601)	(0.491)	(0.601)	(1.272)	(1.272)
Government Expertise	0.332	-0.207	-0.387	-0.686	0.195	-0.686	-2.028	-2.028
	(0.795)	(0.200)	(0.480)	(0.386)	(0.311)	(0.386)	(1.919)	(1.919)
Latent Cyber Capacity	0.540	1.196***	-0.787	-0.247	1.209***	-0.247	1.141†	1.141†
	(1.291)	(0.246)	(1.199)	(0.608)	(0.370)	(0.608)	(0.616)	(0.616)
Democratic Regime	3.673***	3.673***	3.673***	3.673***	3.673***	3.673***	3.673***	3.673***
	(0.669)	(0.669)	(0.669)	(0.669)	(0.669)	(0.669)	(0.669)	(0.669)
Total Active Conflicts	0.238	0.238	0.238	0.238	0.238	0.238	0.238	0.238
	(0.344)	(0.344)	(0.344)	(0.344)	(0.344)	(0.344)	(0.344)	(0.344)
Intensity of Strategic Environment	-0.140	-0.140	-0.140	-0.140	-0.140	-0.140	-0.140	-0.140
	(0.214)	(0.214)	(0.214)	(0.214)	(0.214)	(0.214)	(0.214)	(0.214)
Diffusion	-17.768	40.447***	7.281*	3.323	4.649	3.323	-2.726	-2.726
	(14.058)	(11.974)	(3.599)	(2.618)	(3.747)	(2.618)	(5.665)	(5.665)
Diffusion x Time	-	-0.343***	-	-	-	-	-	-
		(0.085)						

Note: P = pre-adoption; I = introduction; M = modification; E = expansion; F = full implementation.
**p* ≤ .05. ***p* ≤ .01. ****p* ≤ .001. †*p* ≤ .10. Standard errors reported in parentheses.
N = 72,006. Failures = 89. Imputations = 5.

The transition-specific model provides a more complex picture of the implementation process. Coefficients in the model provide initial support for Hypotheses 2 (Introduction) and 3 (Modification) but provides no support for Hypotheses 4 (Expansion) and 5 (Full Implementation). However, the simulated transition probabilities provide additional details that the model coefficients alone cannot capture. As such, the results of the simulated transition probabilities provide support for Hypotheses 2, 3, and 4 but do not provide support for Hypothesis 5. Therefore, the transition-specific model provides support for all hypotheses except Hypothesis 5.

Table 4.10 presents transition-specific covariate coefficients, while Figures 4.5 and 4.6 use the multistate model to present stacked transition probabilities for two different covariate profiles based on 1,000 simulations over nineteen years. Figure 4.5 portrays the simulated transition probabilities for a large military with approximately 750,000 soldiers (representing the 75th percentile of the logged military personnel measure, roughly the size of the Brazilian military in 2006), while Figure 4.6 presents the simulated transition probabilities for a small military with approximately 40,000 soldiers (in the 50th percentile of the logged measure, roughly the size of Slovakia's military in 2000). All other variables are held constant: both militaries are set in highly democratic countries, with high levels of spending per soldier, high levels of government cyber-security expertise and latent cyber capacity and are engaged in four mildly intense conflicts. These profiles are used for all subsequent figures utilizing simulations.

Figure 4.5. Simulated Stacked Transition Probabilities for a Large Military

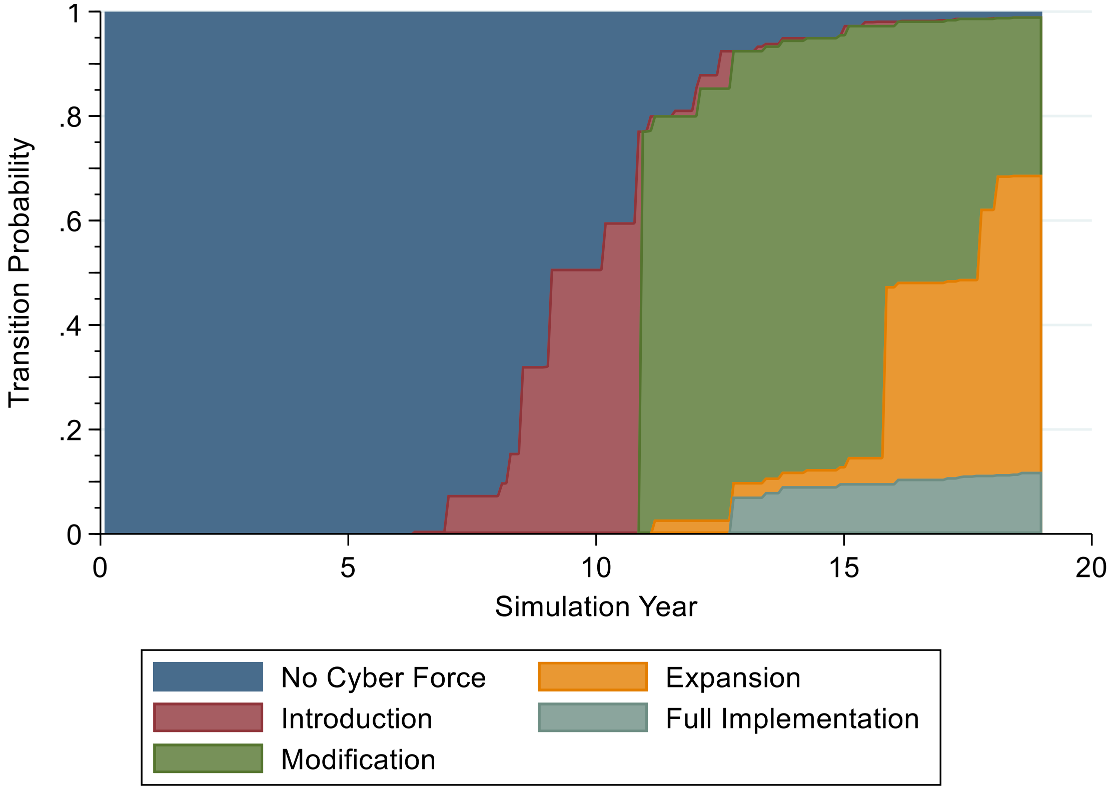
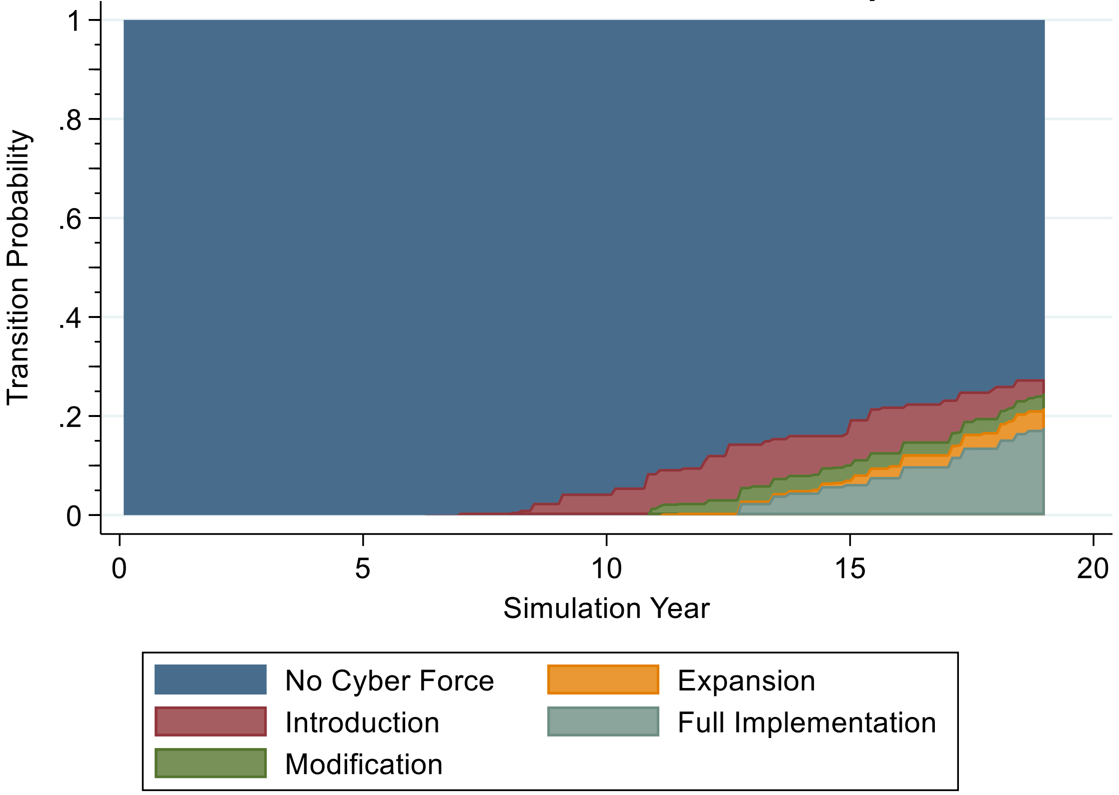


Figure 4.6. Simulated Stacked Transition Probabilities for a Small Military



Results for Organizational Size. All other variables held constant, increases in the log of military personnel are associated with increases in the probability of transitioning from Pre-Adoption to Introduction. The variable's coefficient in the model provides strong support for Hypothesis 2: holding all other variables constant, a 10% increase in the total number of military personnel is associated with a 1.088% increase in the hazard of transitioning from Pre-Adoption to Introduction (at the 99.9% confidence level). The stacked transition probabilities illustrate this relationship. For instance, Figure 4.5 shows that ten years into the simulation, the larger military has roughly a 50% chance of transitioning from Pre-Adoption to Introduction, while Figure 4.6 shows the smaller military has approximately a 5% chance of making the same transition at year ten. At year fifteen, the large military has over a 95% probability of transitioning into Introduction, while the probability of transitioning for the small military remains under 30%.

Both figures also appear to support Hypotheses 3 and 4, with little support for Hypotheses 5. However, the coefficients from Table 4.10 provide mixed support. With statistical significance at the 90% confidence level, the model only provides moderate support for size's effect on transitioning from Introduction to Modification (Hypothesis 3). For every 10% increase in the total number of military personnel, there is a corresponding 1.076% increase in the hazard of transitioning from Introduction to Modification. Coupled with the lack of support (i.e. no statistically significant effect) for Hypotheses 4 (Expansion) and 5 (Full Implementation), these results suggest that organizational size exerts direct effects only the early stages of the implementation process.

However, Figures 4.7, 4.8, 4.9, and 4.10 show that interpretations based on coefficients alone can be misleading. Each figure shows the transition probabilities for the large and small military profiles across the number of years since a cyber force was initially introduced.

Figure 4.7. Simulated Transition Probabilities for Modification over Years Since Introduction

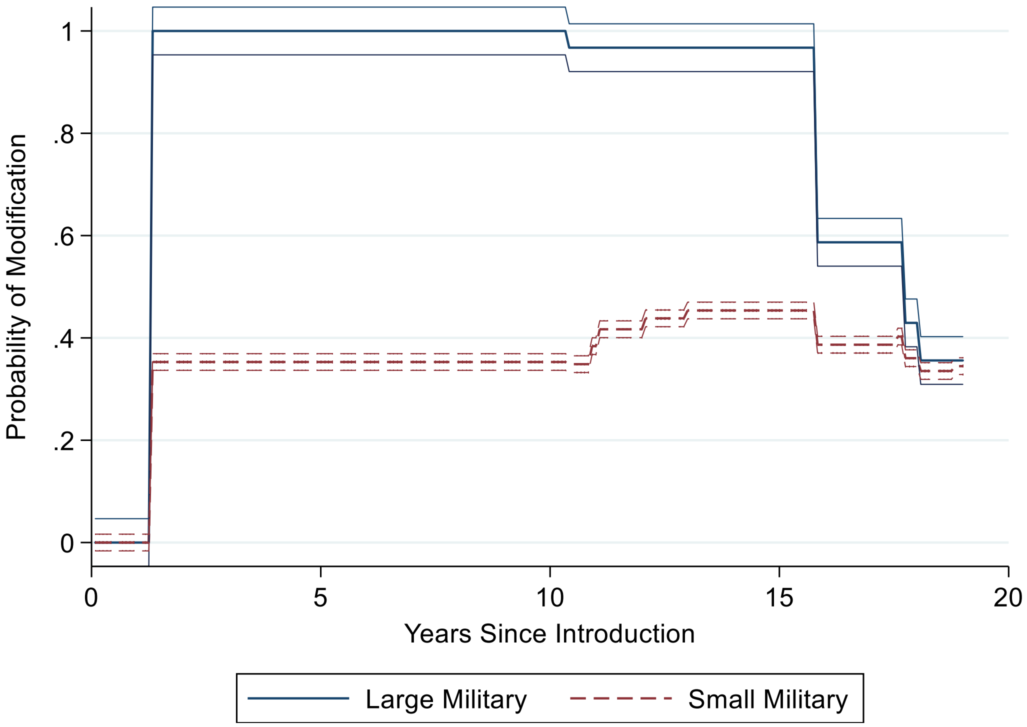


Figure 4.7 compares the probabilities for transitioning into Modification over time since entering Introduction; 95% confidence intervals are displayed. Within the first two years occupying the Introduction stage, the is no statistical difference in the likelihood of the small or large military transitioning into Modification. However, after two years until the 15-year mark, a large military is on average almost 50% more likely to transition into Modification (over a 90% probability) than a small military (approximately a 40% probability). Only after year 15 does the large military's probability of entering Modification significantly decline, and eventually confidence intervals overlap with those of the small military profile near year 17. These overlapping confidence intervals explain the coefficient's level of statistical significance in Table 4.10. Figure 4.7 offers strong support for Hypothesis 3.

Figure 4.8. Simulated Transition Probabilities for Expansion over Years Since Introduction

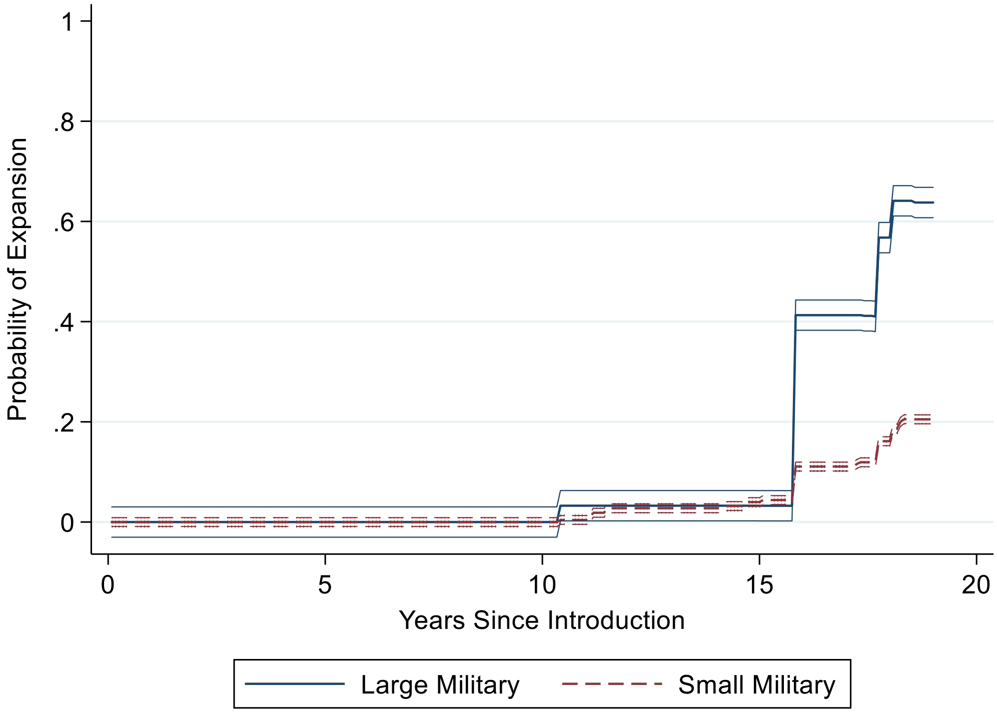


Figure 4.8 provides additional insight into transitions into Expansion. Whereas the coefficients of the logged military size variable provide not support for Hypothesis 4, Figure 4.8 shows qualified support for Hypothesis 4: organizational size only produces a statistically significant effect (i.e. no overlapping confidence intervals between the large and small profiles) after roughly 16 years of a cyber force's existence. At 16 years, cyber forces in a large military have approximately a 40% probability of expanding; at year 19, this probability increases to over 60 percent. Meanwhile, cyber forces in a smaller military have slightly above a 10% probability of transitioning into Expansion at year 16; by year 19, this probability increases to roughly 20 percent.

In line with the variable coefficients in Table 4.10, Figures 4.9 and 4.10 provide no support for Hypothesis 5: cyber forces in large organizations are no more likely to transition into

Full Implementation than are cyber forces in small organizations. Figure 4.9 charts the respective probabilities for transitioning into Full Implementation according to the time since a cyber force has been introduced. To capture the potential that Full Implementation may be more likely out of Pre-Adoption, Figure 4.10 charts transition probabilities over time since Pre-Adoption instead of Introduction. Figure 4.9 indicates that, counter to theoretical expectations, after approximately year 13 of possessing a cyber force, smaller organizations become more likely to transition into Full Implementation than larger militaries. Figure 4.10 shows the mixed effects of size on transitioning from Pre-Adoption to Full Implementation. For roughly the first 12.5 years of occupying Pre-Adoption, there is not statistical difference between the transition probabilities of the large and small military profiles. From years 13 to 15, large militaries become marginally more likely to transition than small militaries; however, after year 17, smaller militaries become more likely than larger militaries to transition into Full Implementation.

When taken in context with the results from the stratified Cox model and the results from Figures 4.5, 4.6, 4.7, and 4.8, the conclusions from Figures 4.9 and 4.10 are unsurprising. Larger militaries have a lower risk (relative to smaller organizations) of completing the implementation process and are more likely to transition into Modification and Expansion as intermediate stages. As such, it makes sense to say that smaller militaries are more likely to reach Full Implementation within a 19-year period: larger militaries are predisposed to occupy more stages for greater periods of time than smaller militaries. As more data on cyber force structures becomes available over time, a necessary extension of this modeling will be to extend simulation time periods to further assess the role of organizational size in reaching Full Implementation.

Figure 4.9. Simulated Transition Probabilities for Full Implementation over Years Since Introduction

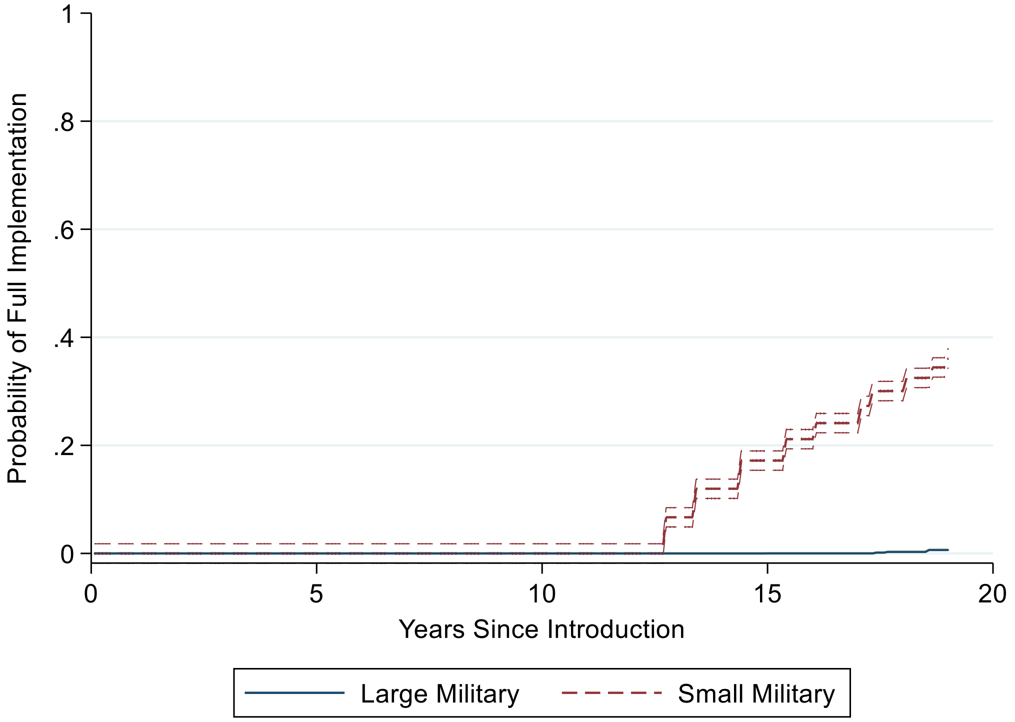
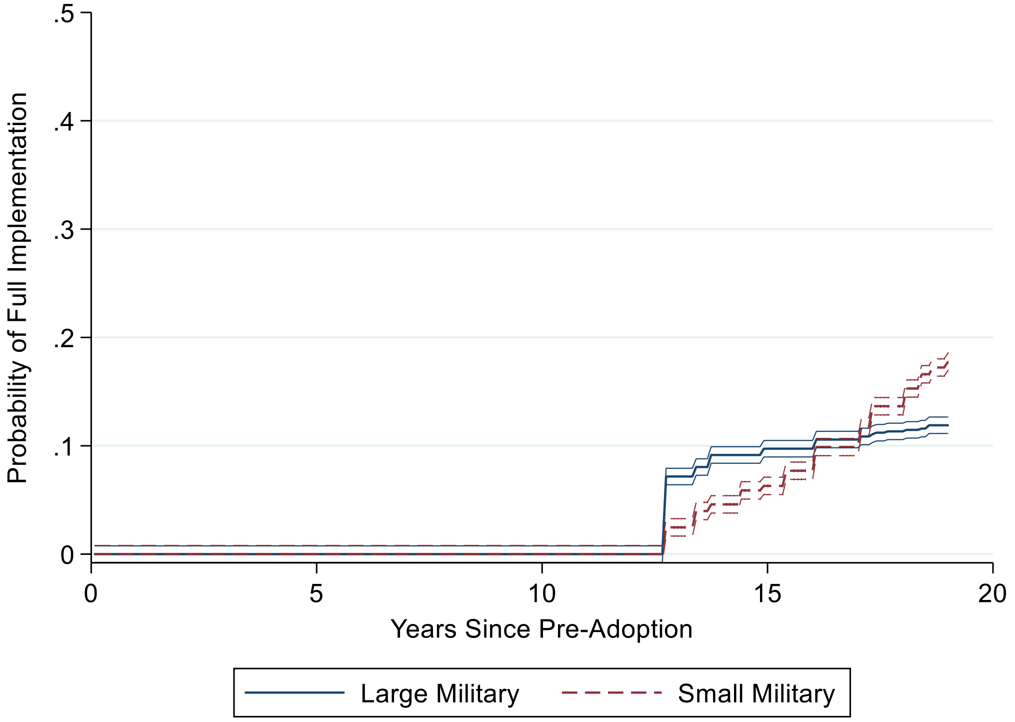


Figure 4.10. Simulated Transition Probabilities for Full Implementation over Years Since Pre-Adoption



Control Variable Results. Of the three background factors held constant in the multistate model, only regime has a statistically significant effect (at the 99.9% confidence level) in Table 4.10. As with the stratified Cox model, increases in the democratic nature of the regime are associated with increases in the hazard of transitioning out of each intermediate implementation stage.[38] The total number of active military conflicts and the intensity of these conflicts have no statistically significant effect on transitions. Of the covariates with transition-specific effects, only government cybersecurity expertise has no statistically significant on any transition.

Increasing spending levels per soldier appears to be a crucial factor across the implementation process in Table 4.10. The log of military spending (USD mil) per 1000 soldiers has statistically significant effects on transitioning from Pre-Adoption to Introduction and from Introduction to Modification. All else held constant, 10% increase in military spending (in USD million) per 1000 soldiers (an increase of 100 USD per soldier) is associated with a 1.043% increase in the hazard of transitioning from Pre-Adoption to Introduction (99.9% confidence level) and a 1.244% increase in the hazard of transitioning from Introduction to Modification. This suggests that relative spending increases facilitate the introduction of an innovation; once introduced, increases in relative spending levels appear to spur competing interests and increase the likelihood that the organizational model underpinning an initial cyber force structures is altered. Spending levels per soldier appear to a critical variable behind expansion. For every one-unit increase in the log of military spending (in USD million) per 1000 soldiers, there is a corresponding 4.641% increase in the hazard ratio in transitioning into Expansion (i.e. Introduction → Expansion and Modification → Expansion) when all other variables are held

[38] Although the constant regime variable is significant, it is worth noting that robustness checks and alternative specifications using transition-specific covariates show that effect of regime is only significant for the transition from Pre-Adoption to Introduction.

constant. Substantively, for each additional 100 USD per soldier, there is a 1.157% increase in the hazard of reaching Expansion.

Latent cyber capacity looks to be a necessary precondition for both the introduction of a cyber force and for reaching Full Implementation when all other covariates are held constant. A 10% increase in latent cyber capacity correlates with a 1.120% increase in the hazard of transitioning from Pre-Adoption into Introduction (at the 99.9% confidence level). A 10% increase in latent cyber capacity is also associated with a 1.114% increase in the hazard of transitioning into Full Implementation from Expansion or Modification, albeit at the 90% confidence level. Increases in latent cyber capacity also facilitates a jump from Introduction to Full Implementation: a 10% increasing in latent cyber capacity is associated with a 1.122% increase in the hazard of transitioning (99.9% confidence level).

Finally, diffusion pressures only exert statistically significant effects on the transitions into Introduction and Modification. Mirroring the pattern identified in the stratified cox model, as the original distance between a state’s cyber force structure and the systemic composition of force structures increases, there is a corresponding increase in the hazard of transitioning from Pre-Adoption into Introduction; eventually, this effected reverses, where an increase in the geometric distance is associated with a decrease in the hazard of moving into the Introduction stage. There is no time-varying effect for the transition from Introduction to Modification: increases in the geometric distance are associated with an increase in the hazard of transitioning.

Conclusion

The statistical analyses in this chapter provides evidence to support my primary claim: organizational size plays an important role in shaping the implementation of cyber forces. More specifically, organizational size exerts direct effects on the implementation process: larger militaries are much more likely than smaller militaries to both introduce cyber forces in a limited manner (support for Hypothesis 2) and modify initial cyber force structures (support for Hypothesis 3). Only after approximately 16 years of possessing a cyber force do large militaries become more likely to expand cyber forces than small militaries (partial support for Hypothesis 4). At the same time, the greater likelihood of transitioning into these intermediate stages means that larger organizations possess a lower risk of completing the implementation process relative to smaller militaries (support for Hypothesis 1). However, this increases the average length of the implementation process for large militaries, making them less likely than small militaries to transition into Full Implementation over the course of 20 years.

The significance of several control variables points to the possible indirect effects of organizational size. Spending increases appear to be crucial for expanding cyber forces. Possessing sufficient latent cyber capacity is a prerequisite for fully implementing cyber forces both in an incremental manner (from the Expansion stage) and in a more wide-ranging fashion (from Introduction). Larger militaries may be better positioned than smaller militaries to increase spending levels per soldier. Moreover, larger militaries might have greater potential to turn latent cyber capacity into actualized capabilities than smaller militaries. As such, organizational size may have indirect effects on the implementation process that are not captured by the models utilized in this chapter. Accordingly, the next two chapters trace the role of size across the implementation of two different cyber forces: Chapter 5 assesses the evolution of U.S. Cyber Command; and Chapter 6 examines the creation of Estonia's Cyber Command. A preliminary assessment of Germany's Cyber and Information Domain Service is provided in the concluding chapter.

Chapter 5

The Origins and Development of United States Cyber Command: Incremental Change in a Large Organization

The U.S. works at a scale that, literally outside of China and Russia, nobody else—our closest allies, nobody—operates at the scale we do.[1]

- Ret. Admiral Michael Rogers
Fmr. Commander U.S. Cyber Command/
Director of the National Security Agency

Introduction

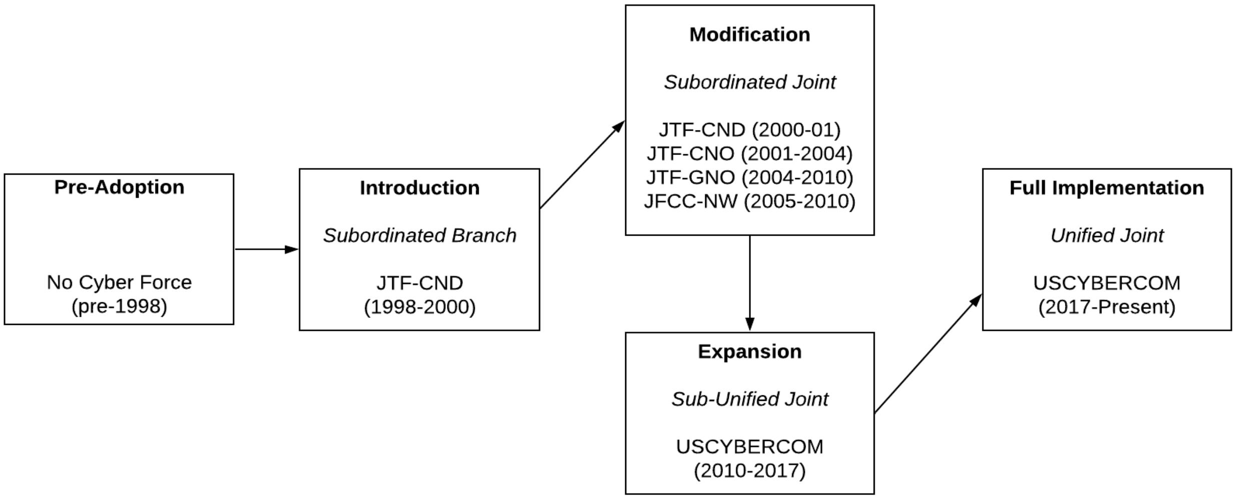
This chapter examines the implementation dynamics in one of the largest military organizations across the globe: the United States Armed Forces. Specifically, this chapter details the development of the United States' cyber force structure and assesses three competing logics advanced in the theory chapter: organizational size, adoption-capacity, and military culture. Using the operationalization advanced in Chapter 4, Figure 5.1 summarizes the changes in U.S. cyber force structure contained in this chapter by listing implementation stages, the corresponding force structure, and the respective institutional body within the military.

The chapter proceeds in five major sections. The first section provides background on the introduction and initial modification of the U.S. cyber force structure by examining organizational initiatives from 1998 to 2005. The second section details an episode of failed modification; specifically, it examines the Air Force's (ultimately failed) attempt to create Air Force Cyber Command (Provisional) as the military-wide locus for conducting computer network operations. The third section examines the stand-up of United States Cyber Command.

[1] U.S. Admiral (ret.) Michael Rogers interview with author, interview by Jason Blessing, Tallinn, Estonia, May 27, 2019.

This section lays out the major arguments and events surrounding an expansion of the existing joint model (a subordinated joint force structure via joint task force). The fourth section examines the decision to elevate U.S. Cyber Command to a unified combatant command and thus transition the U.S. to a unified joint cyber force structure. Finally, the chapter concludes by evaluating the strengths and weakness of each theoretical explanation.

Figure 5.1. The Evolution of U.S. Cyber Force Structure: Implementation Stage, Force Structure, and Institution.



Background: Reorganizations from 1998 to 2005

In the summer of 1998, the United States Department of Defense (USDOD) established the Joint Task Force – Computer Network Defense (JTF-CND) subordinate to the Defense Information Systems Agency (DISA) as the primary office responsible for the protection of USDOD's computer networks.[2] The Joint Task Force was the Defense Department's response to

[2] Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Arlington, VA: Cyber Conflict Studies Association, 2013), 44.

vulnerabilities discovered during the 1997 ELEGIBLE RECIEVER exercise[3] and the ensuing realization of those vulnerabilities during the SOLAR SUNRISE attacks on USDOD networks in February of 1998.[4] Both ELIGIBLE RECEIVER and the SOLAR SUNRISE incident left a crucial question unanswered: 'Who is in charge?'.[5] As the USDOD Chief Information Officer at the time, Art Money had been tasked with developing a coordinating body to fill this role.[6]

The combat services raced to establish new computer network defense and/or information warfare units to stake a claim in the upcoming budgetary battles. The emergence of JTF-CND was a natural first step for USDOD and the combat services to address network defense[7] and initial operating capability was reached by December of 1998. Initial debates over the structure of JTF-CND nearly resulted in the Air Force gaining sole control over the task force; however, the commander of DISA provided an alternative proposal to host JTF-CND. The other combat services agreed with this proposal, as it would prevent the Air Force from capturing new responsibilities and thus more influence.[8] Despite having to operate from temporary trailers in

[3] For details on the exercise and additional resources, see: Michael Martelle, "Eligible Receiver 97," Briefing Book, The Cyber Vault Project (George Washington University, August 1, 2018), The National Security Archive, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations.

[4] On the vulnerabilities discovered, see: K.M. Gode to Louis Freeh, "Re: SOLAR SUNRISE, CITA Matter; OO: HQ," Memo, February 25, 1998, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=3145116-Document-02.

[5] This question was posed by former Deputy Secretary of Defense John Hamre. Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 121.

[6] From the outset of JTF-CND, both Art Money and Lieutenant General Michael Hayden, the Director of the National Security Agency, believed that the cyber mission should be co-located with the NSA at Fort Meade in Maryland. Kaplan, *Dark Territory: The Secret History of Cyber War,* 121.

[7] Department of Defense Historian interview with author, interview by Jason Blessing, Hanover, Maryland, September 25, 2019; Kaplan, *Dark Territory: The Secret History of Cyber War*, 123.

[8] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 44.

the DISA parking lot due to a lack of sufficient office space,[9] JTF-CND reached full operational capability by June 1999.[10]

Originally, Money had planned to incorporate an offensive role (conducting computer network attacks) into JTF-CND. However, both Money and Major General John H. "Soup" Campbell, the one-star Air Force officer in command of the task force, realized that the combat services would not give such responsibility to a small task force that had virtually no command authority. Major General Campbell had successfully lobbied for JTF-CND to be briefed on offensive operations; yet, even this had been undermined by the combat services. Vice service chiefs, at the direction of the service chiefs, continuously redefined attack plans so that they no longer fell under the combat services' requirement to brief the task force. Without a broader charter and a more powerful institutional home, JTF-CND lacked true coordinating power.[11]

In October of 2000, JTF-CND was officially reassigned from DISA to U.S. Space Command (USSPACECOM) by the Unified Command Plan 1999; USPACECOM was also given primary military authority for computer network attacks.[12] Although USSPACECOM was located in Colorado, it was the only command that wanted cyber mission. At this time, the cyber mission did not offer a substantial opportunity for prestige or resource capture, and USSPACECOM's technologically oriented command presented a potential fit for the Task Force. The arrangement with USSPACECOM was a temporary fix; yet through

[9] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 45.

[10] Melissa Hathaway et al., "United States of America: Cyber Readiness at a Glance," Cyber Readiness Index 2.0 (Arlington, VA: Potomac Institute for Policy Studies, September 2016), 25, https://www.potomacinstitute.org/images/CRI/CRI_US_Profile_Web.pdf.

[11] Kaplan, *Dark Territory: The Secret History of Cyber War*, 121–22.

[12] On the changes in the 1999 Unified Command plan, see: Edward J. Drea et al., "History of the Unified Command Plan: 1946-2012" (Washington, D.C.: Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, 2013), 73–77. On USSPACECOM development of computer network defense operations, see: United States Space Command (USSPACECOM), "United States Space Command (USSPACECOM) Concept of Operations (CONOPS) For Computer Network Defense (CND)" (Colorado: United States Government, October 1, 1999), The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3131435-Document-03.

USSPACECOM, JTF-CND gained crucial access to combat authority and resources that were previously not available under DISA.[13] Accordingly, JTF-CND's mission ultimately expanded on April 1, 2001 to include exploitative and offensive operations: the task force was no longer limited to purely computer network defense. To reflect the new mandate, JTF-CND was renamed Joint Task Force – Computer Network Operations (JTF-CNO).[14] This broader scope of authority coincided with the April 2001 release of USDOD's *Joint Publication 1-02, Dictionary of Military and Related Terms*, where the Department advanced an initial definition of cyberspace but did not recognize it as a unique domain.[15]

With the dissolution of USSPACECOM in October 2002, JTF-CNO and the cyber mission (along with USSPACECOM's other units and their missions) were absorbed by U.S. Strategic Command (USSTRATCOM). USSTRATCOM subsequently divided authority over the task force's missions: USSTRATCOMS's Deputy Commander for Network Planning and Integration (a three-star officer who doubled as DIRNSA) oversaw network attacks, while USSTRATCOM's Deputy Commander for Network Operations and Defense (a three-star officer who doubled as the Director of DISA) became responsible for network defense.[16] These authorities were formalized and expanded in February of 2003 with a more comprehensive definition of cyberspace in the *2003 National Strategy to Secure Cyberspace*[17] and the National

[13] Kaplan, *Dark Territory: The Secret History of Cyber War*, 122.

[14] Hathaway et al., "United States of America: Cyber Readiness at a Glance," 25.

[15] Cyberspace was defined as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." U.S. Military Joint Chiefs of Staff, "Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms" (U.S. Department of Defense, April 12, 2001), 89.

[16] Department of Defense Historian interview with author.

[17] Cyberspace was portrayed as a "hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work." United States Government, "The National Strategy to Secure Cyberspace" (Washington, D.C.: United States Government, February 2003), vii, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=2700096-Document-16.

Security Presidential Directive (NSPD)-16.[18] Eventually, in conjunction with the release of the *National Military Strategy* in June 2004—which included specific references to cyberspace as a battlespace and domain[19]—JTF-CNO was expanded and renamed Joint Task Force – Global Network Operations (JTF-GNO).[20]

Responsibilities for computer network attacks were ultimately transferred in January 2005 to Joint Functional Component Command – Network Warfare (JFCC-NW). JFCC-NW emerged from U.S. Marine Corps General James Cartwright's reorganization of USSTRATCOM during his tenure as commander. Only the network attack mission was given to JFCC-NW; the DIRNSA/Commander for Network Planning and Integration at USSTRATCOM retained authority over the new JFCC-NW. Network defense responsibilities remained with JTF-GNO under the STRATCOM-DISA dual hat arrangement.[21] It is against this backdrop that the U.S. Air Force sought the cyber mission and ultimately failed and from which U.S. Cyber Command eventually emerged.

The Cyber Command that Wasn't: The Rise and Fall of the U.S. Air Force Cyber Command (Provisional)

Although JTF-CND had been established under DISA in 1998 instead of the Air Force, the United States Air Force (USAF) had been building a service-level foundation for computer network operations since 1995. The USAF established the nation's first service-level unit to

[18] This document remains classified.
[19] The Strategy implicitly identifies cyberspace as a domain comparable to traditional military domains. It appears to the only joint document advancing this conception until the 2006 *National Military Strategy for Cyberspace*. U.S. Military Joint Chiefs of Staff, "The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow" (Washington, D.C.: United States Government, 2004), https://history.defense.gov/Portals/70/Documents/nms/nms2004.pdf?ver=2014-06-25-123447-627.
[20] U.S. Cyber Command, "U.S. Cyber Command History," accessed July 13, 2019, https://www.cybercom.mil/About/History/.
[21] Department of Defense Historian interview with author.

explicitly incorporate cyberspace in 1995: the 609th Information Warfare Squadron.[22] Therefore, it was no surprise that an Air Force officer—Major General "Soup" Campbell—was tapped to be the first commander of JTF-CND. Despite losing out on command of JTF-CND, the Air Force would continue building its capacity to carry out the cyber mission. The attempted establishment of Air Force Cyber Command Provisional (AFCYBER(P)) under Air Force Secretary Mike Wynne from 2005-2007 demonstrated both the service's ambition and its overreach.

USAF and Mission Expansion

Michael Wynne was nominated as Secretary of the Air Force (SECAF) in June of 2005 (he was confirmed by the U.S. Senate on November 3, 2005). Prior to this appointment, Wynne had been Principal Deputy Under Secretary of Defense for Acquisition, Technology and Logistics (July 2001 – April 2003) and the acting Under Secretary of Defense for Acquisition, Technology and Logistics (May 2003 – June 2005).[23] These roles exposed him to the severe problems with the technology acquisition process and decisions in military and in the Department of Defense. He developed a deep concern over how the Department approached the cyber domain and emerging technologies. In early 2005, Wynne was anticipating that he would be nominated as the new Secretary of the Navy; his goal was to turn the Navy into the "cyber" force—to establish the Navy as the leading strategic and operational force vis-à-vis the cyber domain. Instead, Wynne was surprised by the nomination to head the Air Force. As a result, he pivoted and took his plans to the Air Force to incorporate cyber into the service's mission.[24]

[22] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 344.

[23] U.S. Air Force, "Michael W. Wynne," June 2008, https://www.af.mil/About-Us/Biographies/Display/Article/107896/michael-w-wynne/.

[24] U.S. Air Force/U.S. Cyber Command Consultant interview with author, interview by Jason Blessing, Washington, D.C., March 12, 2019.

After his confirmation in November 2005, Wynne authored a Joint Letter to Airmen detailing why the USAF was uniquely capable of operating in the cyber domain.[25]

Wynne and Chief of Staff of the Air Force General Michael "Buzz" Moseley announced the service's revised mission in December 2005. The new mission statement detailed that the Air Force would be the service to "deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in air, space, and cyberspace."[26] However, no one in the Defense Department knew what the inclusion of cyberspace meant for the service or even what it meant in a broader strategic sense.[27] To shed more light on the implications of the new cyber mission, in January 2006 SECAF Wynne created the Cyberspace Task Force to develop recommendations for strategy, operational concepts, and doctrine for the USAF.[28] At the same time, Wynne sent a memo to SECDEF Rumsfeld indicating that the Air Force was planning to forge a new military orientation towards computer network operations, i.e. that the USAF would carry out computer network attacks as a military operation.[29]

The Air Force's drive to incorporate the cyber mission was not necessarily a surprise to the other combat services and the Joint Staff. The Air Force had been talking internally about the cyber domain prior to Wynne, particularly in the wake of the September 11, 2001 attacks. However, discussions regarding computer network operations and approaches to cyberspace were not tied to counterterrorism. Instead, the Air Force initially argued in 2002 that the cyber mission was an expansion or extension of the space mission. As the service that had the most

[25] U.S. Air Force, "New SECAF Sends 'Letter to Airmen,'" November 3, 2005, https://www.af.mil/News/Article-Display/Article/132876/new-secaf-sends-letter-to-airmen/.
[26] Michael Wynne, "Letter to the Airmen of the United States" (United States Air Force, December 7, 2005), quoted in Johannes Moore, "From Conception to Birth: The Forces Responsible for AFCYBER's Evolution" (Maxwell Air Force Base, Alabama, Air University, 2014), 33.
[27] U.S. Air Force/U.S. Cyber Command Consultant interview with author.
[28] Moore, "From Conception to Birth: The Forces Responsible for AFCYBER's Evolution," 32.
[29] Moore, "From Conception to Birth: The Forces Responsible for AFCYBER's Evolution," 41.

resources and personnel invested in the space domain, USAF officials thought it only natural that the Air Force should be the primary driver in the cyber domain. Thus, it made sense to explore a service-based construct within the Air Force to develop and carry out the cyber mission.[30] Even though the other services had heard this line of argumentation for some time, there was still a perception after Wynne's announcement about mission expansion —particularly within the Joint Staff—that the Air Force was out to set the military agenda for cyberspace and capture any future resources. Officers outside the Air Force thus thought that the service's mission expansion would focus on seizing existing and new resources at the expense of generating better outcomes for the Department of Defense and the nation in cyberspace.[31]

Towards a USAF Major Command for Cyber

The release of the Quadrennial Defense Review on February 6, 2006 appeared to validate the Air Force's concern over cyberspace: the review discussed the dangers of attacks on U.S. critical infrastructure or the Internet.[32] By Fall 2006, the idea of establishing a major command for the cyber mission within the Air Force had begun to emerge as the institutional response to the service's newly expanded mission. The Cyberspace Task Force had concluded its work and presented its findings at the Air Force's CORONA Conference, a tri-annual summit attended by the Secretary of the Air Force, the Chief of Staff, all four-star general officers, and select three-star officers. At the conference, the task force presented two potential arrangements for an Air Force command structure for the cyber domain: the creation of a Numbered Air Force to be

[30] U.S. Admiral (ret.) Michael Rogers interview with author.

[31] U.S. Admiral (ret.) Michael Rogers interview with author.

[32] United States Department of Defense, "Report of the 2006 Quadrennial Defense Review," Quadrennial Defense Review (Washington, D.C.: United States Government, February 6, 2006), 21–51, 89, https://archive.defense.gov/pubs/pdfs/QDR20060203.pdf.

subordinated to an existing major command; or the creation of a new Major Command dedicated to the cyber mission.[33]

Many of the existing Major Command commanders at the conference preferred a Numbered Air Force over a new Major Command for three reasons. First, a Numbered Air Force would have more influence over operational warfighting: Numbered Air Forces provided personnel and doctrinal ideas to combatant commanders, while Major Commands rarely performed these functions. Second, the Major Command commanders thought that the cyber mission lacked the resources needed to justify the formation of a new Major Command. Third, the creation of a new Major Command would take away resources from existing Major Commands; no commander was willing to relinquish mission resources when a new Numbered Air Force could provide assets to an existing Major Command. Despite these objections, the task force advocated for the creation of a New Major Command. Secretary Wynne agreed with the task force.[34]

On November 2, 2006, Wynne announced that the Eighth Air Force, a Numbered Air Force, would be the service's designated command for cyberspace and would lead the transition into a new, cyber-specific Major Command.[35] While the Eighth Air Force maintained a portfolio of capabilities related to network warfare and intelligence, surveillance, and reconnaissance, the force's primary mission was to control strategic, long-range nuclear-capable bombers.[36] Spearheading the development of a new Major Command for the cyber domain represented a drastic departure from the Eighth Air Force's existing expertise. Yet, at the direction of Secretary

[33] Moore, "From Conception to Birth: The Forces Responsible for AFCYBER's Evolution," 39–41.
[34] Moore, 39–41.
[35] C. Todd Lopez, "8th Air Force to Become New Cyber Command," *Air Force Print News*, November 15, 2006, https://www.8af.af.mil/News/Article-Display/Article/333953/8th-air-force-to-become-new-cyber-command/.
[36] 8th Air Force/J-GSOC, "8th Air Force," August 3, 2010, https://www.8af.af.mil/About-Us/Fact-Sheets/Display/Article/333781/8th-air-force/.

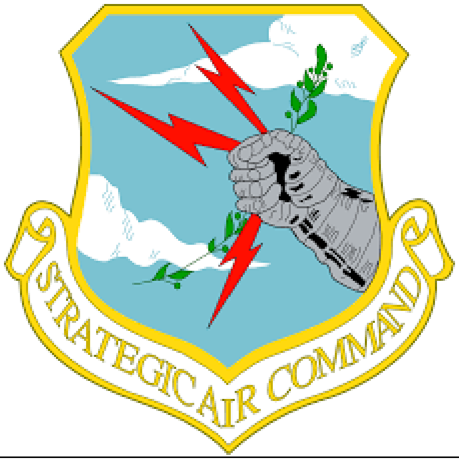
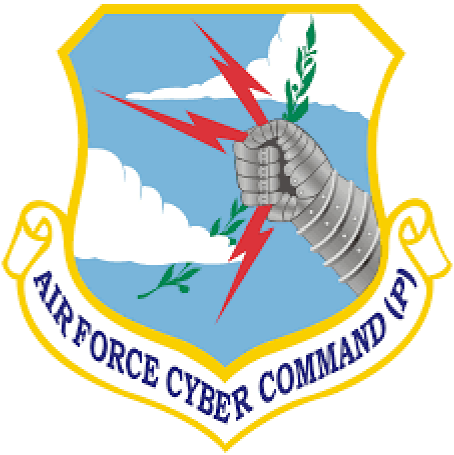
Wynne, Chief of Staff General Moseley ordered Lieutenant General Robert Elder, the commander of the Eighth Air Force, to redefine air power by integrating both kinetic and non-kinetic capabilities with the dual goal of presenting combatant commanders with a spectrum of warfighting capabilities and enhancing the USAF's presence at USSTRATCOM.[37]

The selection of the Eighth Air Force imparted an additional strategic meaning to a new major command. The Eighth Air Force had been renowned for partnering its strategic bombers with the United Kingdom's forces in World War II; they had also been the primary force underlying U.S. Strategic Air Command, which was responsible for two legs of the U.S. nuclear triad (the Navy possessed the third) until the creation of U.S. Strategic Command. In delegating the development of a new cyber command to the Eighth, the USAF was sending a signal that, like with the nuclear mission, it would lead the way to and shape the cyber domain.[38] Figure 5.2 elaborates this intent by comparing the nearly identical shields for U.S. Strategic Air Command and the subsequent Air Force Cyber Command (Provisional).[39]

There was some confusion, however, over what the new major command would actually look like. Most in the Air Force expected the Eighth Air Force to incorporate computer network operations into their existing mission and thus transform into a "global effects" command led by a three-star general. But Wynne declared that the new major command would be led by a new four-star general, placing it on equal footing with Air Combat Command and Air Force Space

[37] Moore, "From Conception to Birth: The Forces Responsible for AFCYBER's Evolution," 41–42. At the time, the Commander of the Eighth Air Force was dual-hatted as the Commander of the Joint Functional Component Command for Space and Global Strike (JFCC-SGS). "Department of Defense Appropriations for Fiscal Year 2006," Pub. L. No. H.R. 2863, § Committee on Appropriations, Subcommittee on Defense (2005), 525.
[38] Department of Defense Historian interview with author.
[39] The author thanks the Department of Defense Historian for pointing out the intended similarity in command shields. Department of Defense Historian interview with author.

Figure 5.2. Comparison of Shields for U.S. Strategic Air Command and Air Force Cyber Command (Provisional)

Strategic Air Command Shield	**Air Force Cyber Command (Provisional) Shield**
	
Source: U.S. Air Force, "Air Force Art: Strategic Air Command (SAC) Shield (Color)," https://www.af.mil/News/Art/igphoto/2000639834/.	*Source: Robert Krause, "Air Force Cyberspace Symposium Now a Reality," Eighth Air Force Public Affairs, November 29, 2007, https://www.8af.af.mil/News/Article-Display/Article/333938/air-force-cyberspace-symposium-now-a-reality/.*

Command. However, a four-star position was highly unlikely: it was the same rank held by unified combatant commanders and required legal changes to the U.S. Code.[40]

Moreover, the initial delegation of the Air Force's cyber mission to a command known best for strategic bombing flew in the face of the larger trend at the Department of Defense which saw the other combat services expand their intelligence, surveillance, and reconnaissance (ISR) divisions to include computer network operations in the cyber domain.[41] The merger of the

[40] Josh Rogin, "Air Force to Create Cyber Command," *FCW: The Business of Federal Technology*, November 13, 2006, https://fcw.com/articles/2006/11/13/air-force-to-create-cyber-command.aspx.

[41] Department of Defense Historian interview with author. As listed later in this chapter, these initiatives would eventually become the service components to U.S. Cyber Command.

other service's cyber and ISR capabilities reflected the Department's larger concern with ISR capabilities heading into 2007—namely, the need for greater ISR capabilities for commanders in Iraq and Afghanistan.[42] The surge of U.S. troops in Iraq, announced in January 2007, required a corresponding surge in ISR capabilities to support the warfighting effort.[43] At the same time, increasing difficulties on the ground in Afghanistan compounded the need for additional ISR capabilities.[44]

The Department of Defense faced three major problems in meeting the increased demand for ISR. First, General Atomics, the single company that made Predator drones and the corresponding ground stations that processed information collected by the drones, had limited production capacity and could not fully meet the Department's demands. Second, the Department required additional manned, propeller-driven reconnaissance aircrafts (like the Navy's P-3 aircraft) at a time when the services, and particularly the Air Force, sought to phase out these aircrafts.[45] Third, the Department lacked an adequate supply of intelligence analysts, linguistic specialists, and broader data fusion capabilities. For newly appointed Secretary of Defense Robert Gates, the underlying cause of the struggle to increase ISR capabilities was a "peacetime mindset" pervasive through the services and the Department as a whole. The United States was engaged in two wars; yet, the Department of Defense lacked a sense of urgency and

[42] This strategic context underpinned the 2006 strategy for cyberspace operations. See: Chairman of the United States Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations" (Washington, D.C.: United States Government, December 2006), The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=2700103-Document-23.

[43] On the decision to surge in Iraq, see: Kelly McHugh, "A Tale of Two Surges: Comparing the Politics of the 2007 Iraq Surge and the 2009 Afghanistan Surge," *SAGE Open* 5, no. 4 (2015): 1–16.

[44] David Rohde and David E. Sanger, "How a 'Good War' in Afghanistan Went Bad," *The New York Times*, August 12, 2007, https://www.nytimes.com/2007/08/12/world/asia/12afghan.html.

[45] For example, while the Department was attempting to mobilize every possible intelligence asset for the wars, the Air Force was planning to end funding by summer 2008 for the U-2, a Cold War-era spy plane that was still providing crucial intelligence for efforts on the ground. Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York: Alfred A. Knopf, 2014), 130.

the services continued to plan for “the next war” instead of participating in the current ones in Iraq and Afghanistan.[46]

Gates felt that the Air Force in particular (in which he had served in the late 1960s) lacked the enthusiasm and urgency to develop greater ISR capabilities for the efforts in Iraq and Afghanistan. Despite embracing the drone mission in the 1990s and 2000s—and repeated attempts to gain control over all drone programs and capabilities—the Air Force continued to prioritize F-22s and new bomber planes better suited to nation-state wars. The lack of emphasis on the drone mission was clear on two accounts. First, in mid-2007, the Air Force had no plans to increase the number of drone crews: they were only providing 48 crews consisting roughly of 80 people and three drones each—a far cry from what Gates thought was necessary. Second, the Air Force had made drone-flying an unappealing career path. While the Army used both warrant officers and non-commissioned officers to fly the Warrior drone (that service’s version of the Predator), the Air Force mandated that only flight-qualified aircraft pilots could fly drones. In effect, this limited the supply of Air Force officers to fly drones. Although drone pilots and fighter pilots required the same credentials, flying actual planes offered more opportunities for career advancement within the Air Force. Thus, Secretary Gates directed the Air Force to increase its capacity to conduct Predator drone missions and would not allow the service to take control of the drone missions of other services. In response, General Moseley initiated a study to examine how the Air Force could increase the number of Predator crews by October of 2008.[47]

[46] Gates, *Duty: Memoirs of a Secretary at War*, 127–29.
[47] Gates, *Duty: Memoirs of a Secretary at War*, 127–29.

Establishing AFCYBER(P) amidst Turmoil in the Air Force

Despite Secretary of Defense Gates' criticisms of the Air Force's slow progress to increase the number of drone crews and the service's persistent emphasis on "the next war,"[48] Air Force Secretary Wynne moved forward with the plan to establish a new Major Command dedicated to cyberspace. On September 17, 2007, Wynne announced the activation of the Air Force Cyberspace Command (Provisional) – AFCYBER(P) – a new Major Command that would bring previous service capabilities under a single commander.[49] As a provisional command, AFCYBER(P) had no actual forces—authorization would only occur once the command gained initial operating capability. Until the command became operational, all direction in terms of policy and doctrine were delivered through the Commander of Air Force Network Operations under the Eighth Air Force.[50] The goal for the command was to reach initial operating status by October 2007 and to establish three preliminary components to the command: and a traditional electronic communications component, an electronic warfare component, and a network warfare component. These three dimensions of the command would consolidate existing programs from across the Air Force.[51] Major General William Lord was tapped to lead this effort as commander of AFCYBER(P).

[48] Gates, *Duty: Memoirs of a Secretary at War*, 130.

[49] U.S. Air Force, "Air Force Secretary Announces Provisional Cyber Command," September 19, 2007, https://www.af.mil/News/Article-Display/Article/125683/air-force-secretary-announces-provisional-cyber-command/.

[50] CHIPS Magazine, "Interview with Air Force Major General William T. Lord, Air Force Cyberspace Command (Provisional) Commander," *CHIPS: The Department of the Navy's Information Technology Magazine*, September 2008, https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=2760.

[51] Greg Bruno, "The Capital Interview: General William Lord on Cyberspace and the Future of Warfare" (Council on Foreign Relations, April 1, 2008), https://www.cfr.org/interview/capital-interview-general-william-lord-cyberspace-and-future-warfare.

In October of 2007, the Air Force announced that AFCYBER(P) would be located at Barksdale Air Force Base in Louisiana.[52] However, the provisional command would have to delay its timeline for initial operating capacity for four major reasons. The first was related to funding. No new money had been allocated for the standup of a new Major Command—AFCYBER(P) had to work through the Air Force's corporate structure to streamline the funding that existed for programs across the service.[53] However, this effort was complicated by the fact that Lieutenant General Elder, Major General Lord, and the commanders to be subordinated to AFCYBER(P) were wary of absorbing the resources of other commanders across the Air Force.[54] Additionally, Major General Lord had projected that the new command would require a budget of roughly 5 billion dollars per year over five years with approximately 10,000 personnel assigned to the command.[55] This projection came at a time when the Air Force was making significant cuts to personnel and spending to finance new fighter planes: 20,000 enlisted personnel had just been phased out of the service, and a further reduction of 20,000 enlisted personnel was scheduled to be completed by 2011.[56]

Second, the role of the new command vis-à-vis combatant commands and the other services was not at all clear. Major General Lord portrayed two conflicting functions. On one hand, AFCYBER(P) would maintain a sole focus on computer network defense within the Air Force:

> We have talked to Naval Network Warfare Command [NETWARCOM] and the Army's NETCOM [Network Enterprise Technology Command] because they

[52] The selection of a location for AFCYBER(P) was itself an intensive process. Several Air Force bases and their respective localities competed for the headquarters by offering land and other incentives such as academic and research tie-ins for the command. Ultimately, Air Force Leadership chose Barksdale AFB as it was the home to the Eighth Air Force, which led the AFCYBER(P) initiative; Mary Graham, "Welcome to Cyberwar Country, USA," *WIRED*, February 11, 2008, https://www.wired.com/2008/02/cyber-command/?currentPage=all.

[53] Bruno, "The Capital Interview: General William Lord on Cyberspace and the Future of Warfare."

[54] U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[55] Bruno, "The Capital Interview: General William Lord on Cyberspace and the Future of Warfare."

[56] Graham, "Welcome to Cyberwar Country, USA."

> have been established longer than we have…there is a direct correlation to what [the Navy's] NETWARCOM does and what we will do for the Air Force. Terrestrial networks and airborne networks will be our responsibility.[57]

There would be little operational overlap with the other services—overlap would only occur in the sense that all the services provided forces to USSTRATCOM. Collaboration with the other services was expected to be largely administrative in nature.[58] On the other hand, a more expansive role was envisioned once the command reached full operational capacity. As a force provider for combatant commands, AFCYBER(P) would train and equip its personnel in order to provide offensive capabilities to combatant commanders.[59] Yet, several issues remained unclear: the scope of personnel provision to the combatant commands; how offensive operations would be deployed and interact with other service capabilities; and how the major command would relate to JTF-GNO and JFCC-NW.

A third hurdle also complicated the stand-up of AFCYBER(P): the Air Force itself lacked a clear vision of the boundaries of the cyber mission and the new command's responsibilities. In addition to the consolidation of previous efforts, Air Force leadership also justified the creation of AFCYBER(P) in terms of the service's dependence on technology and the cyber domain.[60] According to Major General Lord, "One of the reasons that the Air Force decided to stand up this capability is because of the Air Force's dependence on technology in command and control of our own forces. If you are flying a Predator from Las Vegas over Afghanistan, that is a thin command and control link."[61] However, this reasoning—the service-wide dependence on

[57] CHIPS Magazine, "Interview with Air Force Major General William T. Lord, Air Force Cyberspace Command (Provisional) Commander."

[58] CHIPS Magazine.

[59] CHIPS Magazine, "Interview with Air Force Major General William T. Lord, Air Force Cyberspace Command (Provisional) Commander."; Bruno, "The Capital Interview: General William Lord on Cyberspace and the Future of Warfare."

[60] Bruno, "The Capital Interview: General William Lord on Cyberspace and the Future of Warfare."

[61] CHIPS Magazine, "Interview with Air Force Major General William T. Lord, Air Force Cyberspace Command (Provisional) Commander."

cyberspace—created internal confusion over who would actually be included in the new mission set. Prior to the activation of AFCYBER(P), Lieutenant General Elder led the effort at Barksdale Air Force Base with representatives from across the Air Force to stand up the new command dedicated to the cyber domain. Almost everyone in the Air Force had sent a representative. Each looked around with the same question: well, why are you here? The responses were indicative of the Air Force's problem. 'I'm in communications, so I do cyber. I do intelligence work—that's cyber. I'm a bomber; we rely heavily on cyberspace, so I do cyber too.' The Air Force still did not have a clear picture about what cyber meant for a new Major Command, to the service, or even in a broader strategic sense.[62]

The final reason why the implementation of AFCYBER(P) suffered dealt with reorienting the service to address the cyber mission area while still undertaking existing mission sets—namely, the nuclear mission. While the Eight Air Force had been preoccupied with on-ramping the new cyber command, they experienced a gradual erosion of standards regarding the handling of nuclear weapons. Just eighteen days prior to the activation of AFCYBER(P), this erosion of standards manifested in an incident at Barksdale Air Force Base (the soon-to-be home of the new Major Command). In his memoirs, Secretary of Defense Gates recounts the incident:

> On August 30, 2007, a B-52 bomber took off from Minot Air Force Base in North Dakota at 8:40 a.m. carrying six air-launched cruise missiles, each armed with a nuclear weapon capable of explosive power more than ten times that of the atomic bomb dropped on Hiroshima. The plane landed at Barksdale Air Force Base in Louisiana at 11:23 a.m. It was parked there without any of the stringent security measures required for such weapons. At ten that evening, a member of the munitions crew at Barksdale discovered that the warheads were not mock training rounds but actual nuclear weapons that had been loaded in error. Only then was the incident reported to the National Military Command Center (NMCC) as a 'Bent Spear' event—'an incident involving nuclear weapons, warheads, components or vehicles transporting nuclear material of significant interest.'[63]

[62] U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[63] Gates, *Duty: Memoirs of a Secretary at War*, 239-40.

The next day, August 31, Lieutenant General Mosely reported the incident to Secretary Gates, who notified President Bush. Bush directed Gates to investigate the incident, and the Air Force immediately conducted and inventory of its nuclear weapons and launched its own investigation into the event.[64] This incident and the ensuing investigation would eventually undermine all progress made towards the realization of AFCYBER(P).

Nuclear Fallout, Missing Missiles, and the Suspension of AFCYBER(P)

On October 19, 2007, less than one month after the Minot-Barksdale nuclear mishandling incident, Air Force Secretary Wynne announced the findings of the Air Force's internal investigation. The inquiry linked the incident to a gradual erosion of adherence to the Department of Defense's nuclear weapons-handling standards. In response, Wynne immediately relieved three colonels and four noncommissioned officers of their commands and positions.[65] After Wynne's announcement, Secretary Gates directed an additional investigation to be led by General (retired) Larry Welch—a former Air Force Chief of Staff now associated with the Defense Science Board within the Defense Department. General (ret.) Welch and the Board would study the Minot-Barksdale incident as part of a broader, more comprehensive examination of nuclear handling policies and procedures across the Department. Welch eventually briefed the U.S. Senate Armed Services Committee of the Defense Science Board inquiry on February 12, 2008: the Minot-Barksdale incident occurred due to an increasing lack of both resources and attention in the Air Force to adequately perform the service's nuclear mission. The implications were clear: in the midst of setting up AFCYBER(P), the Eight Air Force had compromised its

[64] Gates, *Duty: Memoirs of a Secretary at War*, 240; Peter Grier, "Misplaced Nukes," *Air Force Magazine*, June 26, 2017, https://www.airforcemag.com/article/misplacednukes/.
[65] Gates, *Duty: Memoirs of a Secretary at War*, 240; Grier, "Misplaced Nukes."

primary mission. In the wake of Welch's testimony, Gates ultimately decided to let the Air Force determine any additional disciplinary measures to be taken related to the incident.[66] (Duty, 241).

Things did not get any better for the Air Force as the year progressed. A mislabeled missile shipment to Taiwan in March 2008 would provide additional evidence of the Air Force's lack of attention to the nuclear mission. On March 21, Secretary Gates was notified that the Taiwanese military had mistakenly received a shipment of four intercontinental ballistic missiles (ICBMs). The original shipment, ordered in August 2006, was for helicopter batteries. The Taiwanese immediately alerted their U.S. security assistance contact that they had received the ICBMs; while the missiles were non-nuclear, the shipment did contain nose cones and the associated electronics. Fearful that the Chinese government might interpret this shipment as an aggressive move, on March 24 Secretary Gates notified the Senate Armed Services Committee, the Senate Appropriations Committee, and the Chinese ambassador of the mistake.[67] After this second incident involving the Air Force's mishandling of weapons, Gates announced in a press conference that Admiral Kirkland Donald—head of the Navy's nuclear programs—would investigate the Taiwanese shipment.[68] Admiral Donald's initial report to Gates, delivered on April 15, indicated that (1) the Taiwanese had not tampered with the nose cones on the ICBMs and (2) that the mislabeling had occurred as an accident without nefarious intent. To Gates, this confirmed that the Air Force no longer maintained adequate nuclear standards.[69]

[66] Gates, 241.

[67] U.S. Department of Defense, "DOD News Briefing on Mistaken Shipment to Taiwan with Secretary of Air Force Wynne, Lt. Gen. Ham and Principal Deputy Undersecretary Henry," March 28, 2008, https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=4179; Gates, *Duty: Memoirs of a Secretary at War*, 241.

[68] U.S. Department of Defense, "DOD News Briefing with Secretary Gates from the Pentagon," June 5, 2008, https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=4236; Gates, *Duty: Memoirs of a Secretary at War*, 241-242.

[69] Gates, *Duty: Memoirs of a Secretary at War*, 242. A third, non-weapons related incident – a cremation incident at Dover Air Force Base on May 9, 2008 – also tarnished the Air Force's reputation (248-249).

These two incidents involving the Air Force occurred amidst Gates' frustration with the service over his continued push to increase ISR efforts for the wars in Iraq and Afghanistan.[70] In late April, Gates had established an ISR task force to expand capabilities in response to Admiral Mike Mullen's briefings on the Department's initiatives. A few days after creating the task force, Gates delivered a speech to Air Force personnel emphasizing the need for unorthodox thinking and cultural change: the service needed to focus on the wars it was already fighting instead looking forward to the "next war."[71] Despite the importance of unmanned aerial vehicles to the wars in Iraq and Afghanistan, Air Force leadership would not commit to Gates' vision: drones were a crucial part of the service's future and should be a significant and permanent part of warfighting capabilities. For example, in summer of 2008, the Air Force had between twelve and eighteen drone crews at Creech Air Force Base in Nevada that were each only piloting unmanned crafts for roughly 60 hours a month. The base increased the crews' flight hours only after two Department of Defense officials visited and reported the situation back to Secretary Gates.[72]

The Air Force's nuclear troubles culminated in June of 2008. On June 2, Admiral Mullen emailed Secretary Gates in response to Admiral Donald's finalized report. Admiral Mullen stated that "'the decline in the nuclear mission in the Air Force is representative and symptomatic of a greater decline, for which I can tie responsibility directly to the two most senior leaders…I believe the Air Force leadership has to be held accountable." Marine Corps General James Cartwright, the Vice Chairman of the Joint Chiefs of Staff who had expertise on nuclear issues

[70] Gates, 248.
[71] U.S. Department of Defense, "Remarks to Air War College (Montgomery Alabama)," April 21, 2008, https://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1231.
[72] Gates had visited Creech Air Force Base in Nevada earlier in 2008 and observed the lethal technology of Predator and Reaper drones; he could not understand why the Air Force resisted the mission. Gates, *Duty: Memoirs of a Secretary at War*, 131–32.

due to his previous command of USSTRATCOM, concurred with Mullen's recommendation to Gates. Moreover, President Bush supported the dismissal of Air Force leadership.[73] Accordingly, on June 5, 2008, Secretary Gates requested the resignations of both Air Force Secretary Wynne and his Chief of Staff General Mosely,[74] and he recommended Mike Donley and General Norman Schwartz as their replacements, respectively. Admiral Mullen had been sent to notify General Moseley while Deputy Secretary of Defense Gordon England had been tasked with notifying Wynne.[75]

The removal of Air Force leadership entailed the removal of support for AFCYBER(P). For many in the Defense Department, the decline in the Air Force's nuclear handling standards was directly related to the service's attempt to set up AFCYBER(P). The firing of Wynne and Moseley would redirect the service's attention to core missions and current war efforts. For others who held grudges against the Air Force—such as Deputy Secretary England, a former Secretary of the Navy—removal of top leadership also represented an opportunity to punish the service that acted as "rebels" by expanding into the cyber mission as a political power grab.[76] Without the support of its new top leadership and increasing pressure from the Department of Defense, the Air Force suspended AFCYBER(P) in August of 2008.[77] The next month, the Air Force announced that the command would officially be downgraded to become a Numbered Air Force—the Twenty-Fourth Air Force—under the Air Force Space Command.[78]

[73] Gates, *Duty: Memoirs of a Secretary at War*, 243.

[74] Kristin Roberts, "Air Force Leadership Fired over Nuclear Issue," *Reuters*, June 5, 2008, https://www.reuters.com/article/us-usa-airforce/air-force-leadership-fired-over-nuclear-issue-idUSWAT00960720080606.

[75] U.S. Air Force/U.S. Cyber Command Consultant interview with author; Gates, *Duty: Memoirs of a Secretary at War*, 244.

[76] U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[77] Noah Shachtman, "Air Force Suspends Controversial Cyber Command," *WIRED*, August 13, 2008, https://www.wired.com/2008/08/air-force-suspe/.

[78] David Axe, "Air Force Establishes 'Reduced' Cyber-War Command," *WIRED,* August 18, 2009, https://www.wired.com/2009/08/air-force-establishes-new-reduced-cyber-war-command/.

After the announcement, General Schwartz, the new Air Force Chief of Staff, wrote a letter in September stating that the service would craft a new implementation strategy for its nuclear deterrence capability. This would have impacts for several other mission areas, including cyber. While the letter floated an idea for a new Major Command to create global effects (i.e., a strategic air command with a cyber component)[79] one major question remained: now that the Air Force has lost AFCYBER(P), who would get the cyber mission? As a whole, the Department did not really know how to implement a "cyber command," and nobody wanted to dip into anyone else's funding to set up a new command. However, many in the Air Force—including Secretary Donley and General Schwatrz, who had held a number a joint positions in the military—agreed that if the Air Force could not have the command and the mission, then any new command dedicated to the cyber domain should be a joint-service endeavor. The Air Force had slowly aligned with a broader consensus emerging across the Department of Defense: the need to establish a joint, sub-unified cyber command. Eventually (and ironically), the Twenty-Fourth Air Force would become part of Air Forces Cyber, the Air Force's service component to U.S. Cyber Command. The very same Air Force contingent that had intended to be the leader in the cyber domain would follow the pattern of the other services by merging with the intelligence wings of the Air Force (the Twenty-Fifth Air Force) to create a component for a new joint command.[80]

U.S. Cyber Command, Part I: Expanding the Joint Approach

At the same time that the Air Force was activating AFCYBER(P), the idea for what would become an expanded joint approach to cyberspace—U.S. Cyber Command—had been gaining support.[81] In fact, Secretary Gates had acknowledged the broader importance of the cyber

[79] J. G. Buzanowski, "Gen. Schwartz Addresses Air Force Future" (U.S. Air Force, September 16, 2008), https://www.af.mil/News/Article-Display/Article/122408/gen-schwartz-addresses-air-force-future/.
[80] U.S. Air Force/U.S. Cyber Command Consultant interview with author.
[81] Department of Defense Historian interview with author.

mission after assuming office at the end of 2006. Shocked by the daily number of attempted intrusions into military networks, Gates sent an inquiry to the Pentagon's deputy general counsel about when a cyber incident would constitute an act of war according to international law. (Notably, Gates did not receive a response until December 31, 2008, when the counsel replied that the threshold for a military response to cyber incidents was a political consideration, not a legal one).[82] However, the Air Force's argument for a service-based approach acted as a springboard: the development of capabilities at the service-level was great for the Air Force, but what would a joint-warfighting approach look like? AFCYBER(P) had made this broader conversation about a joint approach much more explicit in the Pentagon. While a joint approach to the cyber domain had been the basis for JFCC-NW and JTF-GNO (and its previous incarnations), the joint task force construct lent itself to the creation of stovepipes. With only a two- or three-star commander, the joint task force structure could not impose true coordination upon the services, operational knowledge and expertise tended to "stovepipe" with the individual services with little sharing amongst the other services.[83]

Laying Foundations for a New Command

One of the main advocates of a joint-service approach to cyber was Admiral Michael McConnell. Sworn in as Director of National Intelligence on February 20, 2007, McConnell sought to elevate cyber issues on the defense agenda. Despite the limited bureaucratic tools at the disposal of the Office of the Director of National Intelligence—McConnell could not set budgets or hire or fire personnel[84]—McConnell actively built support for his initiatives by linking cyber-security issues to the post-9/11 strategic environment.

[82] Kaplan, *Dark Territory: The Secret History of Cyber War*, 214.
[83] U.S. Admiral (ret.) Michael Rogers interview with author.
[84] Kaplan, *Dark Territory: The Secret History of Cyber War*, 171–72.

While the Air Force's strategic justification for AFCYBER(P) rested on a future war against great power foes, DNI McConnell grounded cyber initiatives in the context of existing military engagements. McConnell entered office shortly after the January 2007 announcement of the surge in Afghanistan. With the shift in strategy and a new commander in General David Petraeus, a plan to deploy offensive cyber means against insurgents in Iraq had been devised and honed by devised by General Petraeus, General Stanley McChrystal (Commander of Joint Special Operations Command and Commander of Joint Special Operations Command Forward), General John Abizaid (Commander of U.S. Central Command until March 16, 2007), Director of the National Security Agency Keith Alexander, and DNI McConnell. This plan reached President Bush in late April 2007.[85] McConnell saw this as a window of opportunity and subsequently scheduled a briefing with President Bush to explain the proposal. McConnell met with the president on May 16, 2007. Within ten minutes of the briefing, Bush had cut off McConnell to approve the plan. McConnell, stunned, adeptly pivoted from briefing the president on offensive operations to discuss broader issues of computer network defense. McConnell made the case that 9/11 could have been much worse had terrorists hacked into a major bank and contaminated its files—there would have been far more economic damage done than occurred with the destruction of the Twin Towers. Bush, furious at the thought of another 9/11-scale incident, gave McConnell 30 days to 'solve it'.[86]

McConnell's briefing resulted in the formulation of a comprehensive national initiative in May 2007 that would be presented to President Bush several months later. In addition to getting

[85] Kaplan, *Dark Territory: The Secret History of Cyber War*, 173.

[86] Kaplan, *Dark Territory: The Secret History of Cyber War*, 173–76. "It was a rare thing for a president to be briefed on cyber offensive operations—there hadn't been many of them, at this point—and the proposal came at a crucial moment: a few months into Bush's troop surge and the shift to a new strategy, new commander, and new defense secretary." Kaplan, *Dark Territory: The Secret History of Cyber War*, 173.

the president's attention, McConnell had continuously built support behind a cyber-security agenda. He inserted himself into decision processes wherever possible: he stayed as close as he could to the Oval Office and arranged not-so-random drop-ins to visit White House aides and cabinet secretaries who were unaware of their own stakes in cyber policy. To build support for his agenda, McConnell would deliver memos to cabinet secretaries—memos that the secretaries themselves had written the previous week. He would explain that the Chinese had hacked it from the secretary's computer, and that Department of Defense intelligence had hacked it back from Chinese computers. Many secretaries and aides immediately scheduled full-scale briefings to learn more about cyber issues and McConnell's solutions.[87]

Ultimately, McConnell set in motion what would become National Security Presidential Directive 54 (NSPD-54) signed by President Bush on January 9, 2008. NSPD-54 set in motion the Comprehensive National Cybersecurity Initiative that would clarify the cyber-security roles and responsibilities across the federal government.[88] Shortly thereafter, Congress approved $17.3 billion for McConnell's five-year implementation plan. While primarily focused on the protection of civilian agencies, the Initiative outlined in NSPD-54 remained classified: the National Security Agency (NSA) was tasked with providing technical support to the Department of Homeland Security. In reality, this was more than support—the NSA led implementation efforts due to its extensive resources and expertise.[89] Importantly, NSPD-54 provided a foundation and momentum for the Department of Defense to assess the military's current joint task force structure for conducting computer network operations.[90]

[87] Kaplan, *Dark Territory: The Secret History of Cyber War*, 172-73.

[88] United States Government, "National Security Presidential Directive (NSPD-54)/Homeland Security Presidential Directive (HSPD)-23," January 8, 2008, https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[89] Kaplan, *Dark Territory: The Secret History of Cyber War*, 178–80.

[90] Department of Defense Historian interview with author.

Debating Force Structure Alternatives

Shortly after President Bush signed NSPD-54, Secretary of Defense Gates set in motion a series of studies to examine the organization of the Department of Defense's cyber capabilities and provide ideas for new, alternative arrangements.[91] These studies produced a clear consensus: the Department was poorly organized to deal with cyber threats.[92] The current arrangement for the military services via a joint task force structure, although a necessary first step to deal with computer network operations, tended to create stovepipes of skills and expertise within the service components. Task force commanders generally lacked the authority and resources to impose true coordination across the services.[93]

Accordingly, in May of 2008, Secretary Gates directed a departmental-level review of all cyber roles and missions[94] to be led by the Quadrennial Roles and Missions Review's Cyber Team. The team proceeded under the direction of Principal Deputy Undersecretary of Defense (Policy) Christopher "Ryan" Henry and USSTRATCOM' s Deputy Commander, Vice Admiral Carl Mauney.[95] After the studies concluded, the ensuing debates over the military's cyber force structure hinged on four issues: whether the military should maintain primary cyber responsibilities in the first place; the appropriate organizational model for a military-based approach; the potential scale of command; and defining a new military structure's relationship to the National Security Agency.

[91] U.S. Cyber Command, "U.S. Cyber Command History."

[92] Gates, *Duty: Memoirs of a Secretary at War*, 449.

[93] U.S. Admiral (ret.) Michael Rogers interview with author.

[94] U.S. Cyber Command, "U.S. Cyber Command History."

[95] Michael Warner, "US Cyber Command's Road to Full Operational Capability," in *Stand Up and Fight: The Creation of US Security Organizations, 1942-2005*, ed. Ty Seidule and Jacqueline E. Whitt (Carlisle, PA: Army War College Strategic Studies Institute, 2015), 123.

Title 10 vs. Title 50 Orientation. Gates' department-wide review rekindled a debate between the DOD and the Intelligence Community: should cyber responsibilities rest primarily with the military or with civilian intelligence agencies? There continued to be significant overlap between military and intelligence presences in cyberspace. Like the military, intelligence agencies—particularly, the Central Intelligence Agency (CIA) and the National Security Agency (NSA)[96]—possessed both offensive and defensive cyber capabilities.[97] However, the CIA and the broader Intelligence Community had traditionally claimed operational responsibility for conducting network attacks.[98] The development of a more robust military presence in the cyber domain naturally raised questions over the appropriate legal framework for conducting cyber operations, i.e. whether operations would be carried out under Title 10 or Title 50 authority. Title 10 provided the legal authority for the executive branch to carry out military operations; Title 50 authorized the executive branch to conduct intelligence activities and covert action.[99] Categorizing cyber operations under either legal regime would entail different reporting requirements as well as different operational and strategic emphases.[100]

A Title 50 orientation would place cyber operations under the purview of intelligence activities. In doing so, cyber operations would constitute either clandestine operations or covert actions, where the role of the U.S. government would not be publicly acknowledged. Covert

[96] Even though the NSA is a component of the Department of Defense (unlike the CIA), it has a substantial civilian workforce and capacity to operate under non-military authorities. Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy* 5 (2012): 607.

[97] A full review of civilian intelligence cyber capabilities—and how the military coordinates with those civilian elements—is outside the scope of this dissertation.

[98] Omry Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking," *Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 37, 41.

[99] Aaron P. Brecher, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations," *Michigan Law Review* 111, no. 3 (December 2012): 425–26; Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3 (2011): 87–88.

[100] Brecher, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations," 425–26.

cyber actions would require the president to produce written findings to congressional intelligence committees on the importance of an operation to national security in advance of carrying out that operation.[101] Conversely, a Title 10 orientation would designate cyber operations as military activities and place cyber responsibilities primarily under the military. Unlike the rigorous reporting requirements for operations carried out under Title 50 authorities, many "execute orders" given to the military would not require advance notice to Congress.[102] However, computer network operations collapsed the traditional distinctions between intelligence collection, covert action, and traditional military activity—the same line of code could be used for both intelligence collection and network disruption.[103]

The CIA and other civilian intelligence agencies argued that cyber operations did not constitute traditional military activities and should be subjected to the Title 50 oversight requirements—and should thus primarily be the responsibility of the Intelligence Community, not the Department of Defense.[104] Intelligence agencies also asserted that a Title 50 orientation would provide greater latitude for conducting network operations—conducting cyber operations in a military capacity would limit action to wartime contexts in geographic warzones, a factor

[101] Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," 126.

[102] Brecher, "Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations," 427; Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," 126. There are times, however, when a military operation could be deemed covert action. This occurs when an operation is (1) conducted by military personnel (2) under military direction and control (3) according to an order issued or authorized by the Secretary of Defense and (4) the military's role in the operation is not or will not be publicly acknowledged. Wall, 136.

[103] The convergence of Title 10 and Title 50 operations in the cyber domain has followed the same general pattern as special operations. See: Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," 580; Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," 121.

[104] Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," 140.

complicated by networks operating across multiple countries.[105] As a result, a military organization would be unable to retaliate against an adversary in peacetime settings.[106]

More importantly, for the CIA, maintaining cyber operations under Title 50 authorities would reduce the likelihood that military operators disrupted enemy networks and servers, thus alerting adversaries of network presences and burning sources of intelligence.[107] This tension between the Intelligence Community's preference for network exploitation and the preference of the military for network attack had manifested earlier in 2008. In partnership with the Saudi Arabian government, the CIA had set up a "honeypot" website to monitor extremists, identify attackers, and gain information about terrorist plots in Saudi Arabia. However, by early 2008, military officials in U.S. Central Command (USCENTCOM) became concerned that the site was actually facilitating terrorist operations. USCENTCOM had tracked dozens of Saudi jihadists who had entered Iraq to carry out attacks and requested that the site be shut down.[108]

A task force was assembled to discuss an operation that would take down the CIA-backed website. The task force consisted of representatives from the Department of Defense, the Department of Justice, the Office of the Director of National Intelligence, the National Security Council, the CIA, and the NSA. Debates centered on whether to go forward with the operation and whether the operation would be carried out under Title 10 or Title 50 authorities. General Alexander, Director of the NSA, had made the case that taking down the site was a legitimate operation—and a traditional military action given that extremists were using the site to plan

[105] Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," 610.
[106] Derek B. Johnson, "Rogers: CyberCom Lacks Authority, Resources to Defend All of Cyberspace," *FCW: The Business of Federal Technology*, February 27, 2018, https://fcw.com/articles/2018/02/27/rogers-congress-sasc-nsa.aspx; Chris Bing, "Command and Control: A Fight for the Future of Government Hacking," *Cyberscoop*, April 11, 2018, https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/.
[107] Bing, "Command and Control: A Fight for the Future of Government Hacking."
[108] Ellen Nakashima, "Dismantling of Saudi-NSA Web Site Illustrates Need for Clearer Cyberwar Policies," *The Washington Post*, March 19, 2010, https://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html?sid=ST2010031901063.

attacks in Iraq. The CIA did not support taking the site down, arguing that doing so would create a significant loss of intelligence and would damage cooperative relationships with foreign intelligence agencies.

After considering the potential collateral damage, military interests prevailed: USCENTCOM was adamant that the site posed a risk to the lives of American troops, and CIA representatives knew the site would be dismantled by the military.[109] Accordingly, a team from Joint Functional Component Command – Network Warfare (JFCC-NW) carried out the operation to take down the website. However, the operation inadvertently disrupted over 300 servers across Saudi Arabia, Germany, and the United States. Although some Saudi officials had been informed of the operation prior to its execution, they were still outraged over the loss of intelligence. The CIA resented the operation, maintaining that the website had produced valuable intelligence.[110]

After the operation, the CIA requested an official review of U.S. law for cyber operations, arguing that the operation had disregarded existing deconfliction mechanisms between military actions and ongoing intelligence operations.[111] The Agency claimed more broadly that network attacks constituted covert actions: both operations and sponsors were meant to be concealed from both adversaries and other actors in the cyber domain. As such, offensive cyber operations were only to be conducted by the CIA under Title 50 frameworks. Ultimately,

[109] Nakashima.

[110] Nakashima.

[111] At the time, an informal interagency panel had been formed to deconflict operations between JFCC-NW and the Intelligence Community. This panel of interagency points of contact provided an unofficial forum for notifying potential stakeholders. Should the panel not reach an agreement over whether to proceed with an operation, questions surrounding the operation would be elevated to an existing construct between the Department of Defense, the Department of Justice, and the Intelligence Community, However, a simple majority vote at both the panel and broader interagency levels would allow an operation to proceed despite any dissent. Laurie A. Mulford, “Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. Cyber Command” (National Defense University, Washington, D.C.), 23–24, https://apps.dtic.mil/dtic/tr/fulltext/u2/a587698.pdf.

the Title 10-Title 50 issue went unresolved—any ruling or interpretation of the law would create a precedent where no legal basis existed.[112] As a result, the lack of precedent allowed debates in late 2008 over enhancing military posture in cyberspace to proceed without legal restrictions.

The Organizational Model. At least three alternative structural alternatives for military organization emerged throughout the Defense Department's review process. Two organizational models received serious consideration: a service-based model and the existing joint approach.[113] The service-based arrangement would entail the creation of a new military service for the cyber domain. For three reasons, both civilian and military officials eventually dismissed this approach.

First, the service approach would face immense political costs and hurdles. A new service would require new legislation and the establishment of new bureaucratic processes to integrate the service into existing interagency dynamics. Theoretically, a new service was possible; however, the general consensus was that only a large-scale war would be likely to facilitate such a massive political rift within the Department.[114] Second, a new service raised major concerns about the strategic integration of cyber tools into other warfighting efforts. The payoff of a service-based approach was the prospect of in-depth technical expertise. However, the risk was that a narrow, cyber-intensive organization would fail to understand the application of cyber means in a broader strategic context. This narrow aperture would fail to optimize outcomes in cyberspace and other domains.[115]

[112] Mulford, 24, 46. Ellen Nakashima, "Cyber-Intruder Sparks Massive Federal Response - and Debate over Dealing with Threats," *The Washington Post*, December 8, 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_print.html.

[113] The author was not privy to the details of the third model under consideration. U.S. Admiral (ret.) Michael Rogers interview with author.

[114] Department of Defense Historian interview with author.

[115] U.S. Admiral (ret.) Michael Rogers interview with author.

Moreover, many military commanders approached the service-based approach with lessons drawn from the prior restructuring of special operations forces. For example, Admiral Mike Rogers, Director of Intelligence for U.S. Indo-Pacific Command at the time, was strongly opposed to a service-level arrangement for cyber based on the success of U.S. Special Operations Command. As Admiral Rogers recounts, the decision to create a joint command for special operations forces provided a strong analogy against the creation of a cyber service:

> I lived through this once before in my career that I can remember. In the aftermath of Desert I [Operation Desert Shield in 1990], you get some people making the argument that special operations are so unique—so specialized, so narrow, so misunderstood by the conventional or traditional military—that we need to create a separate service. This had been the argument throughout the 1980s, that we needed a separate service. Ultimately, we decided in the late 1980s that the best construct was a joint warfighting construct, and from this was ultimately borne Special Operations Command. We ultimately decided the best solution was not a service, but a joint warfighting construct. I look at how that played out for us in Desert I and over the course of next 30 years and I think 'boy that was a smart decision.'[116]

The Special Operations Command analogy certainly lent credibility to the idea of building on the existing joint approach to cyberspace,[117] particularly given the implications special operations had for the Title 10-Title 50 debate in cyberspace.[118] But this was not the sole (or even primary) reason why a joint construct remained more popular than other organizational models.

The primary selling point for advocates of a joint command was that it would execute the cyber mission in an operational framework consistent with the Department of Defense's broader methodology. Why have one approach for everything else and create a new approach for cyber? Other military components worked within and understood the joint framework for operations.

[116] U.S. Admiral (ret.) Michael Rogers interview with author.

[117] Many would later use the USSOCOM analogy as a way to think about integrating CYBERCOM into broader defense efforts. Christopher Paul, Isaac R. Porche III, and Elliot Axelband, "The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces" (Santa Monica, CA: RAND Corporation, 2014).

[118] Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate."

Keeping the joint arrangement would align cyber forces with the existing core processes and decision-making venues of the Department. An alignment with existing practices ameliorated concerns many feared under the service approach, i.e. greater potential technical expertise at the expense of strategic integration with other commands.[119]

At the same time, a revised joint approach could build on existing interests and relationships, particularly among the combat services. A joint combatant command for cyber would place the services as force providers; this would have the two-fold effect of capitalizing on the expertise and ethos within each service while structuring inter-service competition. On one hand, each service would get a share of the cyber mission, and pooling service-level expertise could enhance effectiveness. On the other hand, by giving each service a stake in the cyber mission, a joint command could redirect inter-service from the question of 'who gets the mission?' to the more productive question of 'how do we carry out the mission?'. In this way, a joint approach could facilitate healthier inter-service competition.[120] On this last point, many commanders recalled their experiences in the pre-Goldwater-Nichols military as an argument against creating a new service. The Goldwater-Nichols Act of 1986 fundamentally changed how the services interacted: it removed operational control of forces from the services chiefs and transferred it to combatant commanders. Prior to the Goldwater-Nichols Act, each of the services planned and operated independently and according to different standards. This bred intense operational and bureaucratic conflicts and competition. Having served through the pre-

[119] U.S. Admiral (ret.) Michael Rogers interview with author.

[120] U.S. Admiral (ret.) Michael Rogers interview with author. Admiral Rogers would elaborate further: "This idea that we're just going to parse everything out to everybody [the services]—you assign it to Cyber Command, but you're just going to parse it out to everybody, so everybody's happy and they feel like they win. We don't do ISR that way, we don't do SOF that way, we don't do ballistic missile defense that way. All these areas where we have a fundamental mismatch between resources and requirements…you've got to treat cyber like any high-demand low-density resource. The same approaches we use for the rest of the Department, the exact same thing we've got to do for cyber."

Goldwater-Nichols era, commanders were not eager to consider a service construct for fear of renewed interservice animosity.[121] For these reasons, the joint command emerged as the least politically costly option; it would produce fewer negative political externalities than the creation of a cyber-specific service.

Unified vs. Sub-Unified Command. With preferences congealing around a revision of the existing joint structure, command elevation became the next pressing question: should the new force structure be implemented as an independent, unified combatant command (COCOM) or elevated to a sub-unified combatant command that operates under an existing COCOM? Traditionally, when Joint Task Forces are elevated to a new command in DOD, they transition into a sub-unified command before reaching unified combatant command status. Many supporters of the joint command thought the organization would eventually reach a unified command; it would just take time.[122] However, there were several in DOD who advocated for a unified command from the outset.

Chief among those pushing for a unified command was DNI McConnell. He had continually urged SECDEF Gates to create a separate, unified combatant command to coordinate responses to cyber threats.[123] General Keith Alexander, a three-star general and Director of the NSA at the time, had also supported a unified command.[124] Both believed that a unified command—with the resources of a four-star general—would help drive changes in not only the operational execution of the cyber mission, but also the execution of Department of Defense

[121] U.S. Admiral (ret.) Michael Rogers interview with author. On the Goldwater-Nichols Act, see: United States Congress, "Goldwater-Nichols Department of Defense Reorganization Act of 1986," Pub. L. No. 99–433 (1986), https://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf.

[122] U.S. Admiral (ret.) Michael Rogers interview with author; James A. Lewis, "The Fifth Domain: An Interview with William Lynn," Cyber From the Start, accessed April 12, 2019, https://www.csis.org/podcasts/cyber-start.

[123] Gates, *Duty: Memoirs of a Secretary at War*, 449; Kaplan, *Dark Territory: The Secret History of Cyber War*, 185.

[124] Department of Defense Historian interview with author.

missions more broadly.[125] Together with General James Cartwright, Vice Charmain of the Joint Chiefs of Staff and previous Commander of U.S. Strategic Command, McConnell and Alexander sent a letter in early October 2008 to Secretary Gates recommending the creation of Cyber Command as a unified combatant command.[126]

Secretary Gates had largely agreed with the letter of recommendation but had told McConnel that a unified command was not feasible. The main constraint on creating a unified Cyber Command was the recent stand-up of U.S. Africa Command (USAFRICOM).[127] USAFRICOM became the tenth unified combatant command reaching initial operating capability September 28, 2008 and full operating capability October 1, 2008. Gates relayed that too much political capital had been spent creating USAFRICOM; as Gates later recollected: "I thought the president and Congress would balk at yet another major command."[128] Some resistance to a unified command also came from the Joint Chiefs of Staff, who saw no need to create a brand new command. Moreover, there existed an unspoken rule of thumb across both Congress and the Department of Defense (including the military): no more than ten unified combatant commands. As USAFRICOM was the tenth, there was no room for a unified Cyber Command.[129]

What Gates could do, he told McConnell, was create a sub-unified command under U.S. Strategic Command, where JTF-GNO and JFCC-NW were located.[130] USSTRATCOM had

[125] U.S. Admiral (ret.) Michael Rogers interview with author.
[126] James A. Lewis, "What Keeps You Up at Night? An Interview with Michael McConnell," Cyber From the Start, accessed April 26, 2019, https://www.csis.org/podcasts/cyber-start.
[127] Lewis, "What Keeps You Up at Night? An Interview with Michael McConnell."
[128] Gates, *Duty: Memoirs of a Secretary at War*, 249.
[129] Department of Defense Historian interview with author; Lewis, "The Fifth Domain: An Interview with William Lynn."(DOD HISTORIAN) (Lynn interview w/ Jim
[130] Lewis, "What Keeps You Up at Night? An Interview with Michael McConnell."

developed a cyberspace strategy earlier that year in February[131] and made the most sense given the political and resource limitations on creating a new command. Creating a subordinate command under USSTRATCOM was the quickest way to stand up Cyber Command,[132] and few overtly opposed the idea.[133] McConnell did push back—USSTRATCOM had a wonderful mission but a lot on its plate, and it was hard to effectively undertake signals intelligence with the current demands on the command—but to no avail.[134] If a new joint Cyber Command would materialize, it would have to be as a sub-unified command.[135]

The Dual-Hat Arrangement. The October 2008 letter from McConnell, Alexander, and Cartwright to Secretary Gates also contained a crucial recommendation: authority over the command should be merged with authority over the NSA, i.e. the Commander of Cyber Command and the Director of the NSA should be the same person. This "dual-hat" arrangement, they argued, was needed both to ensure that Cyber Command had resource access—particularly with regards to talent—and to quell an inevitable bureaucratic conflict. A key issue the May

[131] United States Strategic Command, "CDRUSSTRATCOM CONPLAN 8039-08 (U)" (Offutt Air Base, NE: United States Government, February 28, 2008), The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4356235-United-States-Strategic-Command-CDRUSSTRATCOM.

[132] Lewis, "The Fifth Domain: An Interview with William Lynn."

[133] Lewis.. More importantly, there was little resistance from General Kevin Chilton, the Commander of USSTRATCOM (Department of Defense Historian interview with author). Weiner (2016) has suggested that the Defense Intelligence Systems Agency (DISA) would have, as part of the initially conceived arrangement, been downgraded and absorbed as a component of U.S. Cyber Command; he claims DISA remained independent due to leadership resistance to give up the mission and autonomy (Craig J. Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (Doctoral Dissertation, Fairfax, VA, George Mason University, 2016), 303–4). However, this claim is suspect. DISA is a combat support agency and reorganizing a support agency under a combatant command would be highly unlikely. What is more, such a transference would have to go through labor unions: DISA employees are unionized, and Intelligence Community and military personnel are not. DISA employees would have had to been de-unionized to make a merger even remotely possible. Department of Defense Historian interview with author.

[134] Lewis, "What Keeps You Up at Night? An Interview with Michael McConnell." Gates would later be briefed in December by a blue-ribbon panel on USSTRATCOM's management of the nuclear weapons stockpile; the conclusion echoed McConnell: USSTRATCOM had too many missions and should be restricted solely to the nuclear mission. James R. Schlesinger, "Report of the Secretary of Defense Task Force on DOD Nuclear Weapons Management: Phase II: Review of the DOD Nuclear Mission" (Arlington, VA, December 2008), 54.

[135] Several had seen the value of U.S. Forces Korea, another sub-unified command that operation under U.S. Indo-Pacific Command. Department of Defense Historian interview with author.

2008 departmental-level review directed by Secretary Gates dealt with the relationship between offensive and defensive computer network operations. Part of McConnell's vision for Cyber Command was to combine offensive and defensive elements under a single commander.[136] By summer 2008, discussions had begun in earnest about merging JFCC-NW and JTF-GNO, the respective homes of offensive and defensive operations.[137] The real question was how to combine the two joint task forces in a way that made operational and bureaucratic sense.[138]

Both McConnell and Alexander knew that network attack, defense, and exploitation operations relied on the same technology and similar skillsets.[139] Technology and expertise were both concentrated at Fort Meade; if a new command were to succeed, it had to have some sort of relationship—and ideally, colocation—with the National Security Agency. The NSA workforce had the highest level of skill in the nation: exploiting computer networks (for example, via the extraction of information) without leaving a fingerprint was far more challenging than the military's concern with degrading network capabilities.[140] Having access to this talent pool would make a Cyber Command far more effective in carrying out its mission, particularly since service personnel rotate in and out of joint commands.[141]

At the same time, McConnell and Alexander acknowledged the tension between exploitation and attack operations—degrading a computer network can compromise intelligence collection efforts by notifying defenders of an adversarial presence on their networks.[142]

[136] Kaplan, *Dark Territory: The Secret History of Cyber War*, 185.

[137] U.S. Cyber Command, "U.S. Cyber Command History."

[138] Department of Defense Historian interview with author.

[139]James A. Lewis, "Managing New Style Warfare: An Interview with Keith Alexander," Cyber From the Start, accessed May 10, 2019, https://www.csis.org/podcasts/cyber-start; Lewis, "What Keeps You Up at Night? An Interview with Michael McConnell"; Kaplan, *Dark Territory: The Secret History of Cyber War*, 178–80.

[140] Lewis, "What Keeps You Up at Night? An Interview with Michael McConnell."

[141] Lewis, "Managing New Style Warfare: An Interview with Keith Alexander."

[142] The White House held a similar view: the cyber mission could not be delegated to the military alone, as it would constitute fratricide for intelligence. U.S. Air Force/U.S. Cyber Command Consultant interview with author.

Moreover, the NSA behaved like any other bureaucracy: they did not like to share sensitive technical information or intelligence with military operations commands, even for national security purposes.[143] The solution was to structurally force cooperation, as military commanders and NSA directors would have no interest in carrying out each other's mission if left to their own devices.[144] As such, McConnell, Alexander, and Cartwright recommended the integration of offensive, defensive, and exploitative operations under a single commander. This would also entail transferring JTF-GNO from DISA to the commander of JFCC-NW, the Director of the NSA, who would simultaneously act as the commander of the new Cyber Command.[145]

The Tipping Point: SIPRNet Compromise

With debates over cyber force structure settling on **a sub-unified joint command under U.S. Strategic Command**, the creation of the new command was only a matter of time. The tipping point for bureaucratic change came in late October of 2008 with the compromise of the Department of Defense's Secret Internet Protocol Router Network (SIPRNet), a computer network used to transmit classified information and widely used by the military.

On Friday October 24, 2008 at approximately 4:30 PM EST, U.S. Central Command (USCENTCOM)—the unified command responsible for operations in both Afghanistan and Iraq—experienced a breach of its computer networks that included SIPRNet.[146] The NSA, at the

[143] Lewis, "What Keeps You Up at Night? An Interview with Michael McConnell"; Kaplan, *Dark Territory: The Secret History of Cyber War*, 185.

[144] Even after the dual-hat agreement, USCYBERCOM and the NSA experienced bureaucratic rifts; one such example pertains to parking issues. Once established, new parking rules had been instituted, where USCYBERCOM personnel would be entitled to the best parking spots that were closest to the building during specific hours; NSA personnel were now forced to park in the back of the lots. In one instance, after designated parking hours had lapsed, a technical professional for the NSA parked in the Commander's parking spot. Because of the hierarchical culture, military personnel in USCYBERCOM were shocked and demanded the car removed. However, NSA personnel indicated that their staff member had simply followed the new parking rules with no violation. U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[145] Department of Defense Historian interview with author.

[146] General Alexander has noted that initial signs of suspicious activity were detected roughly ten days prior on October 14. Lewis, "Managing New Style Warfare: An Interview with Keith Alexander."

invitation of USCENTCOM,[147] investigated the breach that afternoon. Richard Schaeffer, head of the NSA’s Information Assurance Directorate, had assigned his Red Team—the same unit responsible for conducting the ELIGIBLE RECEIVER exercise in 1997—to inspect USCENTCOM’s networks. The team discovered several beacons attached to a malicious worm: the worm was programmed to penetrate the classified network, extract information, and the beacons would transmit the extracted information back to the worm’s source.[148] As far as leadership in the military, the NSA, and the Office of the Secretary of Defense knew, this was the first time an adversary had compromised a classified military computer network.[149]

Schaeffer reported the Red Team’s findings back to General Alexander. They suspected the malicious worm to be Russian-made, a hypothesis that would later be confirmed in 2009 by Deputy Secretary of Defense Bill Lynn. The breach had occurred after a USB flash drive, infected with the *agent.btz* virus by Russian foreign intelligence, was found in a parking lot of a U.S. military base in Afghanistan and subsequently inserted into an air-gapped DOD computer. The malicious worm had then spread across classified networks. Alexander called both Secretary Gates and Admiral Mike Mullen, the Chairman of the Joint Chiefs of Staff, to inform them of what Schaeffer’s team had found. Shortly thereafter, Alexander, Schaeffer, and four others sat down in Alexander’s office to discuss solutions.[150] The remediation effort that emerged—codenamed “Buckshot Yankee”—involved writing a software program that would reroute the beacons to send the extracted information to a storage bin on NSA networks. Within 22 hours, the program has been successfully tested at Fort Meade and deployed to SIPRNet and other

[147] Legal restrictions prevented the NSA from entering a classified network without explicit invitation. Lewis.
[148] Kaplan, *Dark Territory: The Secret History of Cyber War*, 181.
[149] Kaplan, 181–82.
[150] Lewis, “Managing New Style Warfare: An Interview with Keith Alexander.”

military networks at approximately 2:30 PM that Saturday. Within 22 hours, the NSA had detected, diagnosed, and remediated the compromise.[151]

That Monday morning, October 27, Admiral Mike Mullen called an emergency meeting about the SIPRnet compromise to discuss the scope and immediate next steps since USCENTCOM was conducting two wars. To his shock, the service chiefs had sent colonels to attend the meeting; he needed to meet with three- and four-star commanders, not colonels. As a result, Mullen scheduled a teleconference later that morning with McConnell, Alexander, and General Chilton of USSTRATCOM to figure out who was in charge of these types of problems and what the plan would be. General Chilton asserted that, because JTF-GNO reported to USSTRATCOM, he should take the lead. When Mullen pressed for his plan, Chilton pivoted and deferred to Alexander.[152] Unfortunately, USSTRATCOM and the combat service components of JTF-GNO lacked the expertise of the NSA: the default response of the military commands was to count the number of computer systems as they would with physical military equipment.[153] Alexander saw this as an opportunity to drive home the point that only the NSA had the expertise to take the lead; military efforts moving forward must include the NSA.[154] The dual-hat option for Cyber Command became more attractive.

The SIPRNet compromise and Buckshot Yankee remediation efforts convinced Secretary Gates that McConnell, Alexander, and Cartwright were correct—dual-hatting a cyber command with the NSA was the right call. And it needed to happen sooner rather than later, as Gates

[151] Lewis, "Managing New Style Warfare: An Interview with Keith Alexander"; Kaplan, *Dark Territory: The Secret History of Cyber War*, 182.

[152] Kaplan, *Dark Territory: The Secret History of Cyber War*, 183–84.

[153] Lewis, "Managing New Style Warfare: An Interview with Keith Alexander."

[154] Kaplan, *Dark Territory: The Secret History of Cyber War*, 181. Officials had also debated whether to use offensive tools to neutralize the *agent.btz* malware on non-military networks (including those in other countries). However, senior officials rejected this option: *agent.btz* appeared to be espionage and did not justify an aggressive response. Nakashima, "Cyber-Intruder Sparks Massive Federal Response - and Debate over Dealing with Threats."

witnessed bureaucratic dysfunction play out during the compromise and through the rest of Fall 2008.[155] Accordingly, Gates wrote a memo on November 11 that placed JTF-GNO under the operational command of General Alexander, effectively removing the Joint Task Force from DISA control.[156] This had *de facto* created what would later be formalized as U.S. Cyber Command.

By January of 2009, Secretary Gates pushed more aggressively to stand up Cyber Command with both President Bush and then President Obama. Both had agreed on the need for the new command. Buy-in from both the outgoing and the incoming presidents was crucial; however, another factor behind the timing of Gates' push was Alexander's rumored retirement from both the NSA and the Army. Gates knew Alexander was one of the few people who really understood cyber threats.[157] Hearing that Alexander had just attended a retirement briefing, Gates called Alexander to explain that he wanted Alexander to stay on as both Director of the NSA and Commander of Cyber Command: he would create the new command and promote Alexander from a three-star to a four-star general, thus extending his tenure at least three more years. As it turns out, Alexander's retirement was a false rumor—the briefing had been mandated since he had put it off multiple times already. Alexander agreed to Gates' proposition, and the wheels were put in motion for formally establishing Cyber Command.[158]

The transition to the Obama administration in early 2009 meant the official stand-up of Cyber Command would be delayed—major organizational changes tended not to take place

[155] Kaplan, *Dark Territory: The Secret History of Cyber War*, 184–85.

[156] Lewis, "Managing New Style Warfare: An Interview with Keith Alexander."

[157] Moreover, the CIA had recently predicted a major cyber-attack on the United States within the next two years, adding urgency to Gates' initiative. Kaplan, *Dark Territory: The Secret History of Cyber War*, 185.

[158] Lewis, "Managing New Style Warfare: An Interview with Keith Alexander"; Gates, *Duty: Memoirs of a Secretary at War*, 449–50; Kaplan, *Dark Territory: The Secret History of Cyber War*, 186.

during election years.[159] Ultimately, on June 23, 2009, Secretary Gates signed a memorandum that directed General Chilton of USSTRATCOM to establish U.S. Cyber Command (USCYBERCOM) as a sub-unified command subordinated to USSTRATCOM. Gates had planned to announce the new command in a speech the week before; however, the announcement was delayed a week and put in memo form to abate concerns from the CIA that the Department of Defense and the NSA would dominate the government's cyberspace efforts.[160] The memo formally recommended that General Alexander run the command while retaining his title of Director of the NSA. The purpose of U.S. Cyber Command would be "to better organized Defense operations in cyberspace, to ensure our freedom of access to cyberspace, and to oversee investments in people, resources, and technology to prevent disruptions of service to the military."[161] An implementation plan was subsequently issued in September of 2009.[162]

Despite a slow Congressional process, Alexander's appointment was approved the next year in 2010. By that time, several Department of Defense reviews—specifically, the Quadrennial Defense Review (QDR) and the Ballistic Missile Defense Review—hinted at the growing strategic importance of cyberspace. Both reviews indicated that the Department had been preparing to fight two conventional wars at the same time, not the two conflicts in which it was currently engaged in Iraq and Afghanistan. The QDR in particular had shown that more

[159] Department of Defense Historian interview with author.

[160] Ellen Nakashima, "Gates Establishes Cyber-Defense Command," *The Washington Post*, June 24, 2009, https://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303492.html.

[161] Gates, *Duty: Memoirs of a Secretary at War*, 449; Kaplan, *Dark Territory: The Secret History of Cyber War*, 186.

[162] United States Government Accountability Office, "Military Transformation: Additional Actions Needed by U.S. Strategic Command to Strengthen Implementation of Its Many Missions and New Organization," Report to the Subcommittee on Strategic Forces, Committee on Armed Services, House of Representatives (Washington, D.C.: United States Government Accountability Office, September 2006). That summer, the Department of Defense had begun drafting a set of rules of engagement and an execute order that would allow USSTRATCOM and USCYBERCOM to direct operations and defense of military networks worldwide. The order required hostile provocation directed at the U.S. that threatened imminent death, serious injury, or damage to national or economic security. .Nakashima, "Cyber-Intruder Sparks Massive Federal Response - and Debate over Dealing with Threats."

resources were needed for special operations, helicopters, drones, and intelligence/surveillance/reconnaissance (ISR).[163] Investing in the establishment of U.S. Cyber Command would be an important step in enhancing ISR capabilities in cyberspace.

On May 21, 2010, U.S. Cyber Command was officially established as a sub-unified combatant command with General Alexander in charge.[164] An announcement from U.S. Strategic Command stated that USCYBERCOM had reached initial operating capability (IOC). USSTRATCOM's announcement also specified the new command's mission, responsibilities, organizations, and relationship to other commands.[165] The command would start with a staff of roughly 750 personnel and an approximate budget of $155 million.[166] Four months later in September, General Chilton sent a classified memo recommending that U.S. Cyber Command be deemed fully operational.[167] The news that USCYBERCOM had reached full operating capability (FOC) became public on October 31 with the following service components: U.S. Army Cyber Command (ARCYBER), Air Forces Cyber (AFCYBER), Fleet Cyber Command (FLTCYBER), and the U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER).[168]

As USCYBERCOM worked towards full operating capacity, disputes between the Department of Defense and the CIA flared over which entity—the military or the CIA—should be the lead organization for conducting cyber operations against al-Qaeda targets. As with the

[163] United States Department of Defense, "Report of the 2010 Quadrennial Defense Review," Quadrennial Defense Review (Washington, D.C.: United States Government, February 2010), https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf.

[164] Secretary Gates had concordantly created a new civilian office to lead policy development and command oversight; Gates, *Duty: Memoirs of a Secretary at War*, 449–50.

[165] United States Strategic Command, "USCYBERCOM Announcement Message," May 21, 2010, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=2692108-Document-6.

[166] Nakashima, "Cyber-Intruder Sparks Massive Federal Response - and Debate over Dealing with Threats."

[167] It also summarizes the Cyber Command's six key missions, including one that is partially classified. Kevin P. Chilton, "Full Operational Capacity (FOC) of U.S. Cyber Command (USCYBERCOM)," Memorandum (United States Strategic Command, September 21, 2010), The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=2692110-Document-8.

[168] U.S. Cyber Command, "U.S. Cyber Command History."

CIA-Saudi website incident, the CIA maintained that these operations were covert action; the nascent Cyber Command pushed for greater authority, arguing that offensive cyber operations were part of the military mission to counter terrorism. The primary issue for senior policymakers and lawyers, however, was defining the battlefield. Most wanted to limit the scope of military computer network attacks to the war zones—the CIA was responsible for covert operations outside battle zones, and the State Department was concerned with the diplomatic backlash of military operations outside war zones. Yet, like with the CIA's inquiry after the takedown of the CIA-Saudi site, officials were unable to resolve the mission dispute, leaving the door open for both the CIA and the military to carry out offensive cyber operations against al-Qaeda.[169]

U.S. Cyber Command, Part II: Implementing a Unified Command

U.S. Cyber Command's relationship with USSTRATCOM was always an imperfect marriage. The cyber mission was not a logical fit under U.S. Strategic Command. As with the joint task force, the arrangement remained logistically difficult with USSTRATCOM located in Omaha, Nebraska and USCYBERCOM at Fort Meade in Maryland. The relationship between the two commands appeared to work the best when USSTRATCOM did not assert day-to-day control over U.S. Cyber Command. For both reasons, many in the military and the broader Department began to realize—just like McConnell, Alexander, and others had advocated—that Cyber Command would need to become a standalone, unified command.[170]

Continued Expansion, Setbacks, and a Near-Miss

Secretary Gates was among those who believed that Cyber Command would eventually be elevated to a unified command. However, he also knew that the "ten command" rule meant

[169] Ellen Nakashima, "Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield," *The Washington Post*, November 6, 2010, https://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html?wprss=rss_world.
[170] Lewis, "The Fifth Domain: An Interview with William Lynn."

that an existing combatant command first had to be eliminated. Gates' solution to this problem was to disestablish U.S. Joint Forces Command (USJFCOM), one of the unified combatant commands that was located in Norfolk, Virginia.[171] As U.S. Cyber Command was working towards full operating capability, Gates announced on August 9, 2010 that U.S. Joint Forces Command would be slated for disestablishment as a cost-saving measure for the Department.[172] Once completed, this move would make room for the elevation of USCYBERCOM.

However, any efforts to elevate Cyber Command would have to wait. February 2010 saw the initial leak of U.S diplomatic cables to Wikileaks, and in June the U.K.-based newspaper *The Guardian* reported that it had received classified cables that had been sent over SIPRNet. Then, in late November, at least five newspapers across the world released coverage of the leaked cables.[173] U.S. Cyber Command was tasked with assessing the operational and strategic impact of the leaks on cyber operations. A fusion cell established within USCYBERCOM released a classified evaluation on December 2, 2010 that indicated the leaks revealed extensive U.S. intelligence on the cyber operations of adversaries. The classified cables showed that the U.S. possessed knowledge of "specific adversary TTPs [tactics, techniques, and procedures], including malware, toolsets, IP addresses, and domains used in intrusion activity."[174] The report suggests that the leaks hampered the United States' ability to track and disrupt advanced

[171] Department of Defense Historian interview with author.

[172] Larry Shaughnessy, "Gates Proposes Cutting Joint Forces Command from Defense Budget," *CNN*, August 10, 2010, https://www.cnn.com/2010/POLITICS/08/09/gates.joint.forces/index.html.

[173] Lisa Lynch, "The Leak Heard Round the World? Cablegate in the Evolving Global Mediascape," in *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, ed. Benedetta Brevini, Arne Hintz, and Patrick McCurdy (Palgrave MacMillan, 2013), 56–77.

[174] United States Cyber Command Fusion Cell, "Situational Awareness Report 2010-SA-0025: WikiLeaks Release of Classified Documents from a Department of State Database" (United States Strategic Command, December 2, 2010), 3, The National Security Archive, https://nsarchive2.gwu.edu//dc.html?doc=6792855-National-Security-Archive-United-States.

persistent threats (APTs), as it expects adversaries to "modify their current infrastructure and intrusion techniques."[175]

Although the Wikileaks revelations delivered a set-back to U.S. Cyber Command, a window of opportunity to elevate USCYBERCOM emerged in late-2011 through 2012. During this period, several changes were made by senior-level leadership that facilitated the elevation debate.[176] In January 2011, President Obama approved Secretary Gates' recommendation to disestablish U.S. Joint Forces Command. On August 4, 2011, U.S. Joint Forces Command was officially disestablished, leaving nine unified combatant commands. This created the institutional space needed to upgrade U.S. Cyber Command to a unified command.[177]

Other changes facilitating a new unified command were occurring in the Department of Defense. Earlier that May, DOD had developed a list of offensive cyber tools to streamline USCYBERCOM's operations. This list entailed several conditions for utilizing cyber tools. For usage in war zones, the president could grant approval in advance; however, any usage outside war zones or during peacetime would require prior presidential approval. These developments reignited the debate between the CIA and DOD from the year before—whether disrupting a terrorist computer network or website was a traditional military activity or covert action.[178] Despite the lack of resolution, the military *de facto* gained the upper hand on July 1, when former CIA Director Leon Panetta was sworn in to replace Gates as Secretary of Defense.[179]

[175] United States Cyber Command Fusion Cell, 3.

[176] U.S. Subject Matter Expert #2 interview with author, interview by Blessing Jason, telephone, March 19, 2019.

[177] The decision to disestablish USJFCOM was also accompanied by the elimination of the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) on January 11, 2012. This cleared additional headquarters space for another unified command. Department of Defense Historian interview with author.

[178] Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," 627.

[179] Felicia Sonmez, "Leon Panetta, CIA Director, Unanimously Confirmed by Senate as Defense Secretary," *Washington Post*, June 21, 2011, https://www.washingtonpost.com/national/national-security/leon-panetta-cia-director-unanimously-confirmed-by-senate-as-defense-secretary/2011/06/21/AGajizeH_story.html; Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," 627.

Later that month, the Department officially recognized cyberspace as a warfighting domain with the release of the Department of Defense Strategy for Operating in Cyberspace.[180] The decision to recognize cyberspace as a military domain was actively debated in the administration. Ultimately, senior leadership saw this as a crucial step in developing doctrine as well as expanding military structures, training, and the technologies needed to operate in cyberspace and organizing DOD's overall efforts.[181]

Cyber Command was nearly elevated to a unified combatant command in October 2012. The Joint Chiefs of Staff had already approved the USCYBERCOM 2012 concept of organization that involved the creation of a Cyber Mission Force (CMF). The Cyber Mission Force would be comprised of 133 teams across three categories: Cyber Protection Teams that would augment and defend DOD's priority networks and systems; Cyber National Mission Force teams that would undertake and support wider national defense initiatives; and Cyber Combat Mission Force teams that would integrate with the other combatant commands and conduct computer network operations in support of those combatant commands. However, the CMF would not receive budgetary support until Fiscal Year 2014.[182] After the approval of the CMF—and in the wake of media reports on Operation Olympic Games, a suspected joint U.S.-Israel cover operation to degrade industrial control systems in an Iranian nuclear facility[183]—President Obama signed Presidential Policy Directive 20 (PPD-20). PPD-20 provided a more explicit

[180] United States Department of Defense, "Department of Defense Strategy for Operating in Cyberspace" (Washington, D.C.: United States Government, July 2011), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[181] Lewis, "The Fifth Domain: An Interview with William Lynn."

[182] U.S. Cyber Command, "U.S. Cyber Command History"; United States Government Accountability Office, "DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force" (Washington, D.C.: United States Government Accountability Office, March 2019), https://www.gao.gov/assets/700/697268.pdf.

[183] For an overview of Operation Olympic Games, see: Kaplan, *Dark Territory: The Secret History of Cyber War*, 203–20.

framework for conducting computer network operations; in particular, it established core principles and processes for conducting network attack operations.[184]

It was at this point that many in the Department of Defense and the White House joined General Alexander in thinking that U.S. Cyber Command should be elevated to a unified command. For at least three reasons, however, Secretary Panetta felt the discussion should be tabled and the decision to elevate be postponed. One was the underdevelopment of the Cyber Mission Force. The CMF was still essentially on the drawing board: the initiative had no money for implementation at the time and was an unproven concept.[185] Second, there was disagreement on the dual-hat arrangement with the NSA. For many, elevating USCYBERCOM meant the command was one step closer to an eventual split from the NSA. The administration could not reach a consensus on whether to dissolve the dual-hat arrange and, if separated from the NSA, how to proceed. This gridlock promoted the status quo, i.e. USCYBERCOM as a sub-unified command.[186] Finally, 2012 was an election year; Panetta did not want to turn the elevation of U.S. Cyber Command into a partisan issue and thus a campaign distraction.[187] As a result, U.S. Cyber Command remain subordinated to USSTRATCOM.

The ensuing two years were marked by continued expansion, additional setbacks, and a change in command of USCYBERCOM. Two events increased U.S. Cyber Command's strategic relevance. The first was the February 3, 2013 release of Joint Publication 3-12 (R), *Cyberspace Operations* by the Joint Chiefs of Staff. This document provided further guidance on the roles, responsibilities, planning and coordination processes for computer network operations as well as

[184] Herbert S. Lin and Amy B. Zegart, "Introduction," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2019), 2.
[185] Department of Defense Historian interview with author.
[186] U.S. Air Force/U.S. Cyber Command Consultant interview with author; Lewis, "Managing New Style Warfare: An Interview with Keith Alexander."
[187] Department of Defense Historian interview with author.

a foundation for further doctrinal development.[188] Outside of DOD, the release of a report by security company FireEye on February 19 publicly revealed a growing issue of concern for the Obama administration and General Alexander: Chinese espionage in cyberspace.[189] The White House saw the report as additional political capital to address cyber operations at a June 2013 summit planned with China's Xi Jinping. However, 48 hours prior to the June summit, *The Guardian* published a story on classified U.S. global surveillance initiatives that had been leaked by NSA contractor Edward Snowden. President Obama lost key leverage over the summit.[190] The Snowden leaks, coupled with a change in the Secretary of Defense that February (Panetta was replaced by Chuck Hagel), effectively stalled the expansion of U.S. Cyber Command, as it was doing damage-control for at least the next year.[191]

Moreover, the 16-day shutdown of the federal government in October 2013 significantly delayed the development of the Cyber Mission Force. The inability of the U.S. Senate to agree on a spending bill resulted in the postponement of 44 courses and a loss of approximately 278,000 total training hours for over 1,000 CMF personnel.[192] Eventually, USCYBERCOM was able to activate the Cyber National Mission Force Headquarters at Fort Meade on January 17, 2014, a key step in actualizing the 2012 proposal.[193] Despite funding delays and the continued fallout from the Snowden leaks, Cyber Command did receive support to continue developing the

[188] U.S. Military Joint Chiefs of Staff, "Joint Publication 3-12 (R), Cyberspace Operations," February 5, 2013, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=2692126-Document-18.

[189] Dan McWhorter, "Mandiant Exposes APT1 - One of China's Cyber Espionage Units and Releases 3,000 Inidcators" (Fireye, February 19, 2013), https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html.

[190] U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[191] Department of Defense Historian interview with author; U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[192] U.S. Cyber Command, "Cyber Mission Force Training and Cyber Flag Update," Briefing (United States Government, October 22, 2013), 21, https://nsarchive2.gwu.edu/dc.html?doc=5977841-National-Security-Archive-USCYBERCOM-Cyber, p. 21.

[193] U.S. Cyber Command, "U.S. Cyber Command History."

Cyber Mission Force. The Quadrennial Defense Review (QDR), delivered to Congress on March 4, 2014, identified the CMF as a top priority for U.S. presence in cyberspace.[194]

U.S. Cyber Command experienced its first official change of command on Friday March 28, 2014, when General Alexander retired from military service, thereby relinquishing command of both USCYBERCOM and stepping down as Director of the NSA. Three days later, that Monday, Admiral Michael Rogers assumed command of USCYBERCOM and took control of the NSA.[195] At the beginning of his tenure, Rogers continued to advocate for Cyber Command's elevation to a unified command.[196] Much of Rogers' efforts were directed at the continued development of the Cyber Mission Force. This included assigning the Cyber Combat Mission teams (via service components) to the unified combatant commands. Marine Corps Cyberspace Command (MARFORCYBER) would be assigned to U.S. Special Operations Command (USSOCOM); Army Cyber Command would be assigned to U.S. Central Command (USCENTCOM), U.S. Africa Command (USAFRICOM), and U.S. Northern Command (USNORTHCOM); Fleet Cyber Command (FLTCYBER) would support U.S. Pacific Command (USPACOM) and U.S. Southern Command (USSOUTHCOM); and Air Forces Cyber (AFCYBER) would be assigned to U.S. European Command (USEUCOM), U.S. Strategic Command (USSTRATCOM), and U.S. Transportation Command (USTRANSCOM).[197] Locating CMF teams within each combatant command mirrored the Special Operations Command model and allowed technical personnel to be assigned and rapidly deployed to

[194] United States Department of Defense, "Report of the 2014 Quadrennial Defense Review," Quadrennial Defense Review (Washington, D.C.: United States Government, March 4, 2014), 33, 41, https://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.
[195] U.S. Cyber Command, "U.S. Cyber Command History."
[196] U.S. Admiral (ret.) Michael Rogers interview with author.
[197] Department of Defense Historian interview with author; United States Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," October 24, 2016, https://www.defense.gov/Explore/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/.

accomplish specific objectives for the respective combatant command to which they were assigned.[198]

Admiral Rogers had made a three-fold argument for moving U.S. Cyber Command to a unified combatant command. First, because cyberspace would be foundational for future military operations, the Department of Defense needed mission expertise and insight at the level where budgeting, resourcing, strategy, and prioritization decisions are made, i.e. the unified combatant command level. Keeping USCYBERCOM as a sub-unified command meant that it did not have a seat at the table, and that would hurt overall military outcomes. Second, the cyber mission demanded "speed": target lists changed constantly and operational decisions required quicker decision-making than many kinetic operations in other domains (land, air, sea, space).[199] Admiral Rogers routinely emphasized the need for decision-making speed. Why did he have to go from Fort Meade in Maryland all the way to Omaha, Nebraska for approval from U.S. Strategic Command when he was 24 miles from the Pentagon, Capital Hill, and the White House?

Finally, he argued that the cyber mission was not a niche mission relegated to USCYBERCOM. It had to be integrated across all the operational elements of the Department and within the service structures, and a unified U.S. Cyber Command would be the vehicle to drive this integration. He drew an explicit comparison to the experience of the first U.S. Space Command (USSPACECOM), which was operational as a unified combatant command from 1985-2002. Rogers appealed to other commanders by acknowledging the dangers of an overly specialized and detached combatant command. USSPACECOM had no meaningful command or mission connection to the other combatant commands: combatant commanders rarely interacted

[198] Bing, "Command and Control: A Fight for the Future of Government Hacking."
[199] Former NSA Director of Information Warfare interview with author, interview by Jason Blessing, Washington, D.C., March 11, 2019.

with USSPACECOM, had little insight into what the command actually accomplished, and did not see how its mission provided benefits to their own mission sets. In contrast, A unified Cyber Command would be integrated into existing Department constructs to support other missions.[200]

Towards Proof of Concept: Joint Task Force-Ares and Operation Glowing Symphony

Unfortunately, other commanders thought that U.S. Cyber Command still lacked maturity.[201] Much of this belief was grounded in the fact that other commanders still did not understand how USCYBERCOM supported their own missions. At one point, Admiral Rogers had one of the service chiefs approach him and ask, "Mike, if you guys could do some cyber stuff, I wouldn't have to spend money on all these other capabilities, right?" Admiral Rogers responded no, cyber capabilities were not a replacement for traditional capabilities—instead, they provided commanders with a greater range of capabilities and decision options than they would have otherwise had.[202]

Progress towards a unified command would again be stalled with a change at the top of the Department, as Ash Carter was nominated by President Obama in December 2014 to replace Chuck Hagel as Secretary of Defense. Carter took control of the Department in February of 2015, and the transition between Secretaries effectively delayed the discussion of a unified U.S. Cyber Command.[203] Rogers, however, continued to push for elevation. For example, Kaplan (2016) suggests that testimony by Rogers before the Senate Armed Services Committee in March 19, 2015 provides insight into his strategy. When asked by Senator John McCain whether the current level of "cyber-deterrence" was inadequate, Rogers replied in the affirmative. Kaplan asserts that Rogers' logic was that a need for more cyber-deterrence meant more money and

[200] U.S. Admiral (ret.) Michael Rogers interview with author.

[201] Department of Defense Historian interview with author.

[202] U.S. Admiral (ret.) Michael Rogers interview with author.

[203] Department of Defense Historian interview with author.

more power for U.S. Cyber Command.[204] On the heels of the Department's new cyber strategy released in April,[205] Rogers released his vision for the continued build-out of USCYBERCOM on June 3, 2015. A major focus of this vision document was the integration of cyber tools to support larger joint force operations.[206]

Although the July 2015 data breaches of the U.S. Office of Personnel Management[207] and Russian information operations during the 2016 presidential election cycle[208] acted as lightning rods for the attention of senior leadership, two campaigns during the 2014-2016 period validated for military commanders the idea that U.S. Cyber Command should be elevated to a unified combatant command. The first was the Russian invasion of Crimea in March of 2014. Russian operations in Ukraine marked the first time that U.S. military officials saw significant tactical use of offensive cyber operations and the integration of network attacks with tactical electronic warfare (EW) and conventional operations.[209] These operations differed significantly from the distributed denial of service (DDOS) attacks in Estonia in 2007 and in Georgia in 2008[210] in that

[204] Kaplan, *Dark Territory: The Secret History of Cyber War*, 283.

[205] The strategy identified five broad strategic goals and implementation objectives. United States Department of Defense, "The DOD Cyber Strategy" (Washington, D.C.: United States Government, April 2015), https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

[206] U.S. Cyber Command, "Beyond the Build: Delivering Outcomes through Cyberspace - The Commander's Vision and Guidance for US Cyber Command" (Fort Meade, MD: United States Government, June 3, 2015), The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=2692135-Document-27.

[207] U.S. Air Force/U.S. Cyber Command Consultant interview with author; Jason Chaffetz, Mark Meadows, and Will Hurd, "The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation," Report from the Committee on Oversight and Government Reform (Washington, D.C.: U.S. House of Representatives (114th Congress), September 7, 2016), https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[208] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment (Washington, D.C.: United States Government, January 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[209] "Statement of Admiral Michael S. Rogers, Commander United States Cyber Command," Testimony (Washington, D.C.: U.S. Senate, May 9, 2017), The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3728886-Admiral-Michael-S-Rogers-Commander-United-States; U.S. Subject Matter Expert #2 interview with author.

[210] For an overview of these incidents, see: Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford and New York: Oxford University Press, 2015), 137–63.

the entailed attacks on the power grid and other physical systems and tracking the movement of enemy forces in real-time by compromising soldiers' mobile phones.[211] The second—and arguably more important—campaign was the Department of Defense's decision to utilize computer network operations in the fight against the Islamic State in Iraq and the Levant (ISIL) codenamed Operation Glowing Symphony.[212]

Dropping "Cyber Bombs" on ISIL. To combat the continued threat of ISIL in Iraq and Syria, the Department of Defense formally established the Combined Joint Task Force – Operation Inherent Resolve (CJTF-OIR), a multi-nation coalition, on October 17, 2014.[213] Within six months, on March 29, 2015, an operations order had been signed directing U.S. Cyber Command to support Operation Inherent Resolve via cooperation with U.S. Central Command. USCYBERCOM's main operational responsibilities would be to: provide information operations to support U.S. Central Command; conduct force protection and counter-command and control operations in support of Operation Inherent Resolve; provide mission support to enable cyberspace effects; conduct operations against U.S. Central Command's ISIL targets; and support any other USCENTCOM requirements.[214]

News of USCYBERCOM's role in Operation Inherent Resolve became public in February of 2016 after Secretary of Defense Carter's congressional testimony on progress. In a subsequent interview with *NPR*, Secretary Carter elaborated that part of the goal was to disrupt ISIL's communications and command and control. "We are using cyber tools, which is a major, new departure…These are attacks in the war zone, essentially using cyber as a weapon of war.

[211] U.S. Subject Matter Expert #2 interview with author.
[212] U.S. Subject Matter Expert #2 interview with author.Carter, interview
[213] Operation Inherent Resolve, "About CJTF-OIR," n.d., https://www.inherentresolve.mil/About-CJTF-OIR/.
[214] U.S. Cyber Command, "USCYBERCOM Operations Order (OPORD) 15-0055: Operations Order in Support of Operation Inherent Resolve," March 29, 2015, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=5751043-National-Security-Archive-COS-MEMO-11-FEB-19.

Just as you drop bombs, we are dropping cyber bombs."[215] An USCYBERCOM internal mission brief from April 12, 2016 provides more details; specifically, the command's concerns center on ISIL's ability to enable global terrorist networking through cyberspace, incite attacks via social media, distribute propaganda online, and dox select individuals.[216] In a subsequent testimony before the Senate Committee on Armed Service on April 28, Secretary Carter would confirm that, as USCYBERCOM's first major combat operation, this was the first real test of U.S. Cyber Command's capabilities ability to produce tangible effects on the battlefield.[217]

One week later, on May 5, Admiral Rogers ordered the creation of Joint Task Force – ARES (JTF-ARES) within U.S. Cyber Command to develop and use malware and other capabilities to degrade ISIL's online capacity. This included damaging and destroying ISIL's networks, computers, mobile phones, and other communications equipment. The order also provided JTF-ARES with instructions to coordinate with coalition partners. Two amending orders (May 5 and June 13) gave additional detail on the development of cyber capabilities to escalate the fight against ISIL but did not place any restrictions on the scope or reach of subsequent operations.[218] Command was delegated to General Paul Nakasone, a three-star general from Army Cyber Command (and future Commander of USCYBERCOM).[219]

[215] "In Fight Against ISIS, U.S. Adds Cyber Tools" (National Public Radio, February 28, 2016), https://www.npr.org/2016/02/28/468446138/in-fight-against-isis-u-s-adds-cyber-tools.
[216] U.S. Cyber Command, "Mission Analysis Brief: Cyber Support to Counter ISIL," Briefing (United States Government, April 12, 2016), 5, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4311638-United-States-Cyber-Command-Mission-Analysis.
[217] "HEARING TO RECEIVE TESTIMONY ON COUNTER-ISIL (ISLAMIC STATE OF IRAQ AND THE LEVANT) OPERATIONS AND MIDDLE EAST STRATEGY," Hearing (Washington, D.C.: U.S. Senate Committee on Armed Services, April 28, 2016), 38–45, https://www.armed-services.senate.gov/imo/media/doc/16-51_04-28-16.pdf.
[218] The original order with both subsequent orders can be found at: U.S. Cyber Command, "CYBERCOM FRAGORD 01 to TASKORD 16-0063 To Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space," May 5, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3678213-Document-07-USCYBERCOM-to-CDRUSACYBER-Subj#document/p23.
[219] Ellen Nakashima, "Incoming NSA Chief Has a Reputation for Winning 'All the Important Fights.' Russia Will Be His Biggest Test Yet," *The Washington Post*, April 1, 2018, https://www.washingtonpost.com/world/national-

JTF-ARES would be responsible for conducting Operation Glowing Symphony, a digital campaign against ISIL. Operational planning had begun in earnest in September 2016. The Task Force began to develop concepts of operation as early as September 12, as evidenced by an internal document. In it, JTF-ARES established operational goals and measures of performance and effectiveness. Moreover, the concepts of operation document portrays network attacks as a form of fire support.[220] An overview briefing of Operation Glowing Symphony was subsequently delivered on September 16.[221] Later, on October 7, USCYBERCOM briefed select individuals from the unified combatant commands, the Office of the Secretary of Defense, and other Department agencies on the means and ends of Operation Glowing Symphony.[222] While JTF-ARES planned Operation Glowing Symphony, USCYBERCOM met an important public goal. On October 21, 2016, all 133 Cyber Mission Force teams reached initial operating capability.[223] This was an important milestone in implementing the Department's Cyber Strategy, particularly given the intensive costs (and setbacks) to develop and train teams.[224]

Planning for Operation Glowing Symphony continued through October. While originally planned for execution in September, Operation Glowing Symphony was delayed due to objection from the CIA, as well as the Federal Bureau of Investigation (FBI) and the State Department.

security/incoming-nsa-chief-has-a-reputation-for-winning-all-the-important-fights-russia-will-be-his-biggest-test-yet/2018/03/31/ee943ef0-23d6-11e8-badd-7c9f29a55815_story.html.

[220] USCYBERCOM JTF-ARES, "United States Cyber Command Concept of Operations - OPERATION GLOWING SYMPHONY," September 13, 2016, 14–15, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638018-USCYBERCOM-JTF-ARES-United-States-Cyber-Command.

[221] USCYBERCOM JTF-ARES, "Operation GLOWING SYMPHONY Overview," current as of September 16, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638019-USCYBERCOM-JTF-ARES-Operation-GLOWING-SYMPHONY.

[222] USCYBERCOM JTF-ARES, "In Progress Review OP Glowing Symphony [Redacted]," October 7, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638020-USCYBERCOM-JTF-ARES-In-Progress-Review-OP.

[223] United States Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability."

[224] U.S. House of Representatives Committee on Armed Services, "Implementing the Department of Defense Cyber Strategy," September 30, 2015, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3114903-Document-09.

Resistance to the operation centered on notifying local governments of impending network attacks, which would have affected networks across approximately 35 countries. The CIA was particularly concerned with how unannounced network attacks would undermine cooperation with law enforcement, intelligence, and counterterrorism elements in those countries. CIA Director John Brennan, along with Secretary of State John Kerry, and Director of National Intelligence James Clapper, argued that giving notice—particularly to allies—was necessary to preserve these relationships. SECDEF Carter, Admiral Rogers, and General Joseph Dunford, Chairman of the Joint Chiefs of Staff, asserted that there would be no harmful collateral effects, and notice was not required under existing authority. Moreover, giving notice could result in a public leak of the operation that would alert targets and allow others to discover U.S. Cyber Command's capabilities.[225]

The National Security Council addressed the dispute for weeks, delaying the Operation's original timeline.[226] Finally, by early November, the JTF-ARES agreed to a notification framework for activities related to the operation.[227] On November 7, 2016, JTF-ARES issued a command and control checklist that required providing USCYBERCOM with operational updates every six hours with immediate updates required for issues of internal disagreement, changes in the parameters of the mission, or on the call for ceasefire by other combatant commands. At this point, technical/tactical and operational deconfliction had already been

[225] Ellen Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies," *The Washington Post*, May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.

[226] Nakashima.

[227] Notably, this appears to have included contacts for Israel and the Netherlands. United States Department of Defense, "Agreed Operation Glowing Symphony Notification Plan," November 4, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638021-Department-of-Defense-Agreed-Operation-Glowing. Ultimately, a total of 15 countries were notified, but actions were only taken on networks in roughly five or six countries. Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies."

completed.[228] The next day, Tuesday November 8, JTF-ARES was officially authorized to begin conducting Operation Glowing Symphony.[229] On Wednesday November 9, Admiral Rogers released the Operations Order to JTF-ARES and its service components, thereby turning the September 12 concepts of operation into actionable orders.[230] A briefing was subsequently held on Thursday November 10 to summarize Rogers' Operations Order.[231]

That same November, Operation Glowing Symphony started to product its first effects. The months prior had been focused on gaining access to ISIL networks and creating target lists. ISIL routinely used encrypted mobile applications, social media, and online magazine and video content; the group even had an entire information technology (IT) department. JTF-ARES operators sent phishing emails to plant malware, malware, spyware, and back doors to gain access and conduct reconnaissance. Using login credentials obtained through these methods, operators used administrator privileges to build target lists; they noticed that ISIL used roughly ten core accounts and a handful of servers around the world to manage online activities. The execution of Operation Glowing Symphony ensued in late November. JTF-ARES operators logged into ISIL accounts and deleted content and file, crashed servers, misconfigured networks, and changed passwords. ISIL was locked out of online accounts, and the group's online activities were effectively frozen. Once ISIL's main administrative accounts and distribution hubs had

[228] USCYBERCOM JTF-ARES, "C-2 Mission Checklist - Operation GLOWING SYMPHONY (V11)," November 7, 2016, 1, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638022-USCYBERCOM-JTF-ARES-C-2-Mission-Checklist.

[229] United States Strategic Command, "FRAGORD 06 to USSTRATCOM OPORD 8000-17: Authorization to Conduct Operation GLOWING SYMPHONY," November 8, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638023-USSTRATCOM-Subj-FRAGORD-06-to-USSTRATCOM-OPORD.

[230] U.S. Cyber Command, "USCYBERCOM OPORD 16-0188 OPERATION GLOWING SYMPHONY (OGS)," November 9, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638024-USCYBERCOM-Subject-USCYBERCOM-OPORD-16-0188.

[231] USCYBERCOM JTF-ARES, "JTF-ARES: Operation Glowing Symphony," November 10, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638025-USCYBERCOM-JTF-ARES-JTF-ARES-Operation-Glowing.

been compromised, JTF-ARES operators pivoted to target ISIL's morale by slowing network speeds, dropping connections, denying account access, and draining cellphone batteries. By May 2017, ISIL's online operations had been significantly degraded, and many servers remained down.[232]

Elevation to Unified Command: From Reactive to Persistent Force

Additional elements of the Department of Defense and the Intelligence Community would be notified of the existence of Operation Glowing Symphony on December 10, 2016, after the initial execution by JTF-ARES.[233] Prior to Operation Glowing Symphony many commanders and civilians in the Department had a fundamental misunderstanding of both ISIL's operations in cyberspace and USCYBERCOMS offensive capabilities. Glowing Symphony provided the "proof of concept" for cyber capabilities: the digital assault spurred a reconsideration of conflict in cyberspace and how USCYBERCOM could interface with the combatant commands operating in other domains.[234]

Operation Glowing Symphony subsequently served as a reference point for USCYBERCOM's effectiveness and maturity.[235] For the Department of Defense and the military, the operation was an overwhelming success: it proved that U.S. Cyber Command could integrate computer network operations into traditional military battle plans of the other combatant commands. The Intelligence Community reached a different conclusion about

[232] Dina Temple-Raston, "How the U.S. Hacked ISIS," *National Public Radio*, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

[233] U.S. Cyber Command, "USCYBERCOM GENADMIN 16-0210 OPERATION GLOWING SYMPHONY," December 10, 2016, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638026-USCYBERCOM-to-USSTRATCOM-USCENTCOM-and-The.

[234] U.S. Subject Matter Expert #2 interview with author; Department of Defense Historian interview with author.

[235] See, for example, Admiral Roger's May 9, 2017 statement before the Senate Armed Forces Committee: "Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, before the Senate Committee on Armed Services" (U.S. Senate Committee on Armed Services, May 9, 2017), 7–8, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3728886-Admiral-Michael-S-Rogers-Commander-United-States.

Operation Glowing Symphony. After roughly one month into the operation, the CIA assessed that the operation's effects were short-lived—ISIL would either restore online content or move content to new servers. The conflicting views of the operation's impact came from different definitions of success: USCYBERCOM and DOD focused on temporarily disrupting and distracting adversaries, while the Intelligence Community defined success in terms of enduring outcomes.[236]

Despite these differing assessments, Operation Glowing Symphony provided the military with the upper hand in the Title 10-Title 50 debate: cyber capabilities could not be held out of military operations as a separate intelligence capability.[237] Indeed, although the CIA would continue to play an important role in the cyber domain,[238] JTF-ARES offered a model for future operations. Specifically, the success of JTF-ARES and Operation Glowing Symphony influenced with creation of the Russia Small Group across U.S. Cyber Command and the NSA to counter Russian influence and cyber operations.[239] While the dual-hat structure with the NSA may have initially stunted USCYBERCOM's development—thereby benefitting the Intelligence

[236] Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies."

[237] Bing, "Command and Control: A Fight for the Future of Government Hacking."

[238] Zach Dorfman et al., "Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks," *Yahoo! News*, July 15, 2020, https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html.

[239] Dina Temple-Raston, "Task Force Takes on Russian Election Interference," *National Public Radio*, August 14, 2019, https://www.npr.org/2019/08/14/751048230/new-nsa-task-force-takes-on-russian-election-interference; Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *The Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html; Shannon Vavra, "NSA's Russian Cyberthreat Task Force Is Now Permanent," *Cyberscoop*, April 19, 2019, https://www.cyberscoop.com/nsa-russia-small-group-cyber-command/.

Community—Operation Glowing Symphony marked a turning point in the military's influence in interagency efforts in the cyber domain.[240]

Planning and executing the operation had reignited the discussion of elevation to a unified command as early as late-2015; this time, senior leadership in the Department and White House concluded that USCYBERCOM should indeed be elevated. However, the 2016 presidential election and impending transition in administration delayed elevation [241] for another year. Eventually, in late 2016, President Obama, Secretary Carter, and the Joint Chiefs of Staff recommended to Congress that USCYBERCOM be elevated to a unified combatant command. Congress subsequently authorized this elevation in December 2016 with the release of the FY2017 National Defense Authorization Act.[242]

The transition to the Trump administration in January of 2017 brought with it an assertive Secretary of Defense—retired Marine Corps general James Mattis—who was intimately familiar with DOD politics. Secretary Mattis supported elevating USCYBERCOM and revising the 2011 Unified Command Plan to make room for a new unified combatant command.[243] On August 18, 2017, the new Trump administration released an official statement directing the elevation of U.S. Cyber Command from a sub-unified to a fully unified combatant command.[244] This elevation

[240] "The NSA went into this thinking that they were going to be the top dog. Now they are paranoid that they may have eaten a massive tapeworm instead." Bing, "Command and Control: A Fight for the Future of Government Hacking."

[241] Department of Defense Historian interview with author. Operation Glowing Symphony was subsequently extended on July 1, 2017. See: U.S. Cyber Command, "USCYBERCOM GENADMIN 17-0093 EXTENSION OF OPERATION GLOWING SYMPHONY," July 1, 2017, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=4638027-USCYBERCOM-Subj-USCYBERCOM-GENADMIN-17-0093.

[242] United States Congress, "National Defense Authorization Act for Fiscal Year 2017," Pub. L. No. 114–328 (2016), Sec. 923, https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf.

[243] Department of Defense Historian interview with author.

[244] United States Government, "Statement by President Donald J. Trump on the Elevation of Cyber Command," August 18, 2017, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

represented a recognition of the growing importance of cyberspace to U.S. national security.[245] The importance of a unified U.S. Cyber Command would be further supported by the administration's growing strategic emphasis on a return to great power competition shown in the December 2017 *National Security Strategy*[246] and the January 2018 *National Defense Strategy*.[247]

U.S. Cyber Command's elevation to a unified command was also accompanied by a pivot in the command's strategic and operational thinking. Specifically, USCYBERCOM began changing from a reactive force—i.e., operations were primarily conducted in response to an adversary's action—to a force that would maintain a persistent operational presence in cyberspace. Much of this shift coincided with and was a result of planning and executing Operation Glowing Symphony. For example, a USCYBERCOM briefing from November 30, 2016 shows the roots of strategic change: in contrasting the dynamics of cyberspace with the nuclear strategic environment, the briefing concludes that deterrence in cyberspace is much more complex than nuclear deterrence. Because cyberspace is characterized by constant contact in a dynamically constructed terrain, initiative must be seized and retained through a strategy of persistence.[248] This strategic theme—persistence—would be echoed in a number of reports and testimonies on cyber deterrence throughout 2017.[249] USCYBERCOM's command vision, a

[245] "Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, before the Senate Committee on Armed Services," 8.

[246] United States Government, "National Security Strategy of the United States," December 2017, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=4421220-The-White-House-National-Security-Strategy-of.

[247] United States Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America," January 19, 2018, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=4421221-Defense-Department-Summary-of-the-2018-National.

[248] U.S. Cyber Command, "How Understanding Cyberspace as a Strategic Environment Should Drive Cyber Capabilities and Operations," November 30, 2016, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=6560991-National-Security-Archive-2-USCYBERCOM-How.

[249] For instance, see: United States Department of Defense Science Board, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence," February 2017, The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3515021-Document-07-Defense-Science-Task-Board-Final; Martin Libicki, "It Takes More Than Offensive Capability to Have an Effective Cyberdeterrence Posture:," Testimony (Washington, D.C.: U.S. House of Representatives Committee on Armed Services, March 1, 2017), The National

public document released on March 23, 2018, further codifies the thinking that the operating environment is one of constant contact and temporary advantage. Superiority is achieved through persistence, which broadly requires constantly maneuvering between defense and offense globally across an interconnected digital space "as close as possible to adversaries and their operations."[250]

On May 4, 2018, U.S. Cyber Command became operational as a unified combatant command. This occurred during the change of command: Admiral Rogers term as Commander of USCYBERCOM and Director of the NSA had ended, and the duties were transferred to Army General Paul Nakasone,[251] the commander responsible for leading JTF-ARES. Later that fall, the Department of Defense released its 2018 cyber strategy document, where the strategy of persistent engagement would be carried out by "defend[ing] forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[252]

Analysis and Conclusion

To what extent can organizational size, adoption-capacity, or organizational culture explain the evolution of the U.S. cyber force structure? The U.S. case offers support for my claim that organizational size is an overlooked factor shaping the implementation of cyber forces. However,

Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3515026-Document-12-Martin-C-Libicki-U-S-Naval-Academy; "Statement by Dr. Craig Fields and Dr. Jim Miller, Defense Science Board, Statement before the Armed Services Committee, United States Senate: Cyber Deterrence" (U.S. Senate Committee on Armed Services, March 2, 2017), The National Security Archive, https://nsarchive2.gwu.edu/dc.html?doc=3694484-Document-09-Dr-Craig-Fields-and-Dr-Jim-Miller.

[250] U.S. Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," March 23, 2018, The National Security Archive, https://nsarchive.gwu.edu/dc.html?doc=4421219-United-States-Cyber-Command-Achieve-and-Maintain.

[251] U.S. Cyber Command, "U.S. Cyber Command History."

[252] United States Department of Defense, "Summary: Department of Defense Cyber Strategy," 2018, 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

answering six questions provides insight into each theoretical framework's ability to explain implementation dynamics.

(1) Why did the U.S. introduce JTF-CND under DISA (a subordinated branch force structure) and subsequently give control over the task force to combatant commands (modifying force structure to subordinated joint)?

Accounts suggest that the ELIGIBLE RECEIVER exercise in 1997 was the driving factor behind the creation of JTF-CND. Although SOLAR SUNRISE—which many feared was linked to the growing tensions with Iraq—drove the formalization of JTF-CND,[253] the need for an institutional response was clearly identified in ELIGIBLE RECEIVER 1997. The exercise was part of a semi-annual series of exercises that the Joint Chiefs of Staff utilized in part to mitigate existing and future risks and threats.[254] This suggests that the initial impetus for introducing the task force came from the military's ability to invest in internal experimentation and new initiatives. Moreover, the lack of literal operating space and set up of trailers for the task force suggests that capacity was not a strong consideration for creating JTF-CND. Culture also struggles to explain why the task force was given to DISA. Although DISA may have been a better cultural fit for the mission than the Air Force, the DISA arrangement appears to have been a bargain to satisfy service interests concerned about mission-capture by the Air Force.

The shift of JTF-CND from DISA to USSPACECOM, which modified cyber force structure from subordinated branch to subordinated joint, does not appear to be the result of capacity or culture. The lack of interest in the mission on the part of other unified combatant commands does not provide positive evidence for a greater absorption capacity for USSPACECOM. Culture may have been an enabler: JTF-CND still fit within the broader

[253] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 122–35.
[254] Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 55.

military culture of jointness, and, being heavily populated by the Air Force, USSPACECOM may have been predisposed to take on a technologically centered mission. However, it is also possible that the mission remained defined in a limited way so that it did not infringe on the missions of the other commands; a broader mission scope for JTF-CND could have driven internal competition.

Verdict: Preliminary support for both organizational size and cultural explanations. Little support for adoption-capacity.

(2) Why did AFCYBER(P) fail?

A successful AFCYBER(P) would have further modified the U.S. cyber force structure, taking the U.S. from a subordinated joint to a sub-unified service construct. My theory of organizational size asserts that modification is the result of competing bureaucratic interests that exercise veto power over the organizational design of cyber forces. As such, this explanation suggests that AFCYBER(P) failed because implementers failed to placate competing interests by narrowly defining the cyber mission, linking their mission definition to existing interests, or by including others in the command structure. Adoption-capacity theory suggests that AFCYBER(P) failed because the broader military did not possess the capacity for the Air Force to absorb the entire cyber mission. According to this logic, AFCYBER(P) put increased demands on the Air Force that hampered the military’s capacity to conduct the ongoing campaigns in Iraq and Afghanistan. Finally, the cultural explanation suggests that, as a service-level initiative, AFCYBER(P) did not fit within the larger joint warfighting culture and was not aligned with how the rest of the military viewed computer network operations.

Evidence from the episode indicates that the broader military possessed the capacity for AFCYBER(P), i.e. the creation of AFCYBER(P) did not significantly degrade the military’s overall ability and capacity to conduct the wars in Afghanistan and Iraq. By and large, the Air Force had been sidelined in the two ground wars and relegated to providing ISR and drone capabilities.[255] Although Gates singles out the Air Force for a reluctance to develop greater ISR capabilities (citing AFCYBER(P) as a distraction), he does acknowledge that this was a military-wide problem. Gates would approve $2.6 billion worth of new ISR initiatives in August of 2008.[256] As such, the creation of AFCYBER(P) appears to have had a limited impact on overall military capacity to absorb the initiative. Interestingly, Gates pointed to the impact that AFCYBER(P) had on the Air Force's devaluation of nuclear mission, not the Air Force's performance in Iraq and Afghanistan. For Gates, combining the nuclear and cyber missions under the Eight Air Force greatly reduced the leadership's daily focus on the nuclear mission.[257]

Consistent with the expectations from my theory of organizational size, the primary reasons for the failure of AFCYBER(P) appear to be: (1) an overly broad definition of the command's mission, and (2) a failure to reduce veto players by appealing to common interests. First, Air Force Secretary Mike Wynne and those in the Eighth Air Force responsible for developing AFCYBER(P) never explicitly defined exactly what the new Air Force mission would include or exclude.[258] Moreover, Wynne's strategic justification for the new command rested on the eventual rise of peer-competitor states that would challenge the U.S. in cyberspace. However, with no actual peer competitor at the time and no connection to the ISR efforts in Iraq

[255] U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[256] Marshall Curtis Erwin, "Intelligence, Surveillance, and Reconnaisance (ISR) Acquisition: Issues for Congress" (Washington, D.C.: Congressional Reseach Service, April 16, 2013), 10, https://fas.org/sgp/crs/intel/R41284.pdf.

[257] Gates, *Duty: Memoirs of a Secretary at War*, 240–41, 244.

[258] The most refined version of the scope of the mission indicated that the goal was to establish "freedom to maneuver" in cyberspace. Michael Wynne, "Cyberspace as a Domain in Which the Air Force Flies and Fights" (C4ISR Integration Conference, Crystal City, VA, November 2, 2006), http://www.iwar.org.uk/iwar/resources/cybercommand/speech.htm.

and Afghanistan, AFCYBER(P) was hard to justify to the other services and combatant commands.[259]

As a result, the other combat services assumed that, despite public reassurances,[260] the Air Force sought to become the sole provider of cyber tools within the joint construct, i.e. the Air Force personnel would eventually replace other service personnel across combatant commands.[261] This fear was compounded by the fact that the Air Force gave responsibilities to the Eighth Air Force; this service component had been the dominant force in Strategic Air Command, which controlled two of the three nuclear strike capabilities prior to the creation of USSTRATCOM. The services saw AFCYBER(P) as an attempt to capture and dominate the cyber mission the same way the Air Force had dominated the nuclear mission before reorganizations in 1992.[262] The result was inter-service resistance to AFYCBER(P).[263] While the nuclear incident at Minot underlies the immediate collapse of AFCYBER(P), the lack of broader organizational support for the initiative rested on a failure to define and connect the mission to existing interests. Wynne remarked after the fact that a joint cyber command was the best possible option; it needed to be joint.[264]

This episode does lend some support for the cultural explanation via counterfactual. Although not within the joint warfighting construct, it is possible that AFCYBER(P) would have

[259] U.S. Air Force/U.S. Cyber Command Consultant interview with author; U.S. Admiral (ret.) Michael Rogers interview with author.

[260] "The operational wings will be doing electronic warfare, network attack, network defense and exploitation, and watching directed-energy weapon development and information operations. At the major command level, it involves mostly resources policy to support those operational units. That's no different than what the other 10 Air Force major commands do… The reason to stand up the command is to focus mass and energy at the resource problem. We have been doing this in pockets all over the Air Force for a long time; it really is to get it all organized under one command." CHIPS Magazine, "Interview with Air Force Major General William T. Lord, Air Force Cyberspace Command (Provisional) Commander."

[261] U.S. Admiral (ret.) Michael Rogers interview with author.

[262] Department of Defense Historian interview with author.

[263] U.S. Air Force/U.S. Cyber Command Consultant interview with author.

[264] U.S. Air Force/U.S. Cyber Command Consultant interview with author.

survived had it been aligned with ISR capabilities instead of the nuclear mission. The other military services viewed the cyber mission as just another form of combat support, and each of the services began incorporating cyber into their own ISR capability profiles.[265] Had the Air Force followed the broader cultural movement and placed AFCYBER(P) developments under control of Air Force Space Command (where it was eventually placed as a downgraded Numbered Air Force), it is possible that there would have been less resistance across the military.[266] While the evidence does not rule out this explanation, supporting evidence remains weak.

Verdict: Strong support for the theory of organizational size with weak support for the cultural explanation. No support for adoption-capacity logic.

(3) Why was a sub-unified joint force structure chosen for U.S. Cyber Command over alternatives?

There are three possible reasons why U.S. Cyber Command was initially created as a sub-unified joint command and not a unified command. First, adoption-capacity suggests that the military lacked the resources to convert the existing joint task force into a unified command. Second, the cultural explanation suggests that the joint approach was consistent with joint military culture—and the prior success of U.S. Special Operations Command—and the decision to create a sub-unified command rested on cultural constraints. Third, according to my theory of organizational size, the joint arrangement was the product of competing inter-organizational interests; a sub-unified command was the result of a lack of a "proof of concept" and not resource constraints.

[265] On the role of service sub-culture in this respect, see: Sarah P. White, "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine" (Dissertation, Cambridge, Massachusetts, Harvard University, 2019).

[266] Department of Defense Historian interview with author.

The evidence provides mixed support for organizational size, strong support for culture, and little support for adoption-capacity. In terms of culture, the joint approach remained consistent with military's approach to conducting warfare, and USSOCOM's success was referenced as a reason for creating a joint command for cyber. Moreover, the recent creation of USAFRICOM as the tenth unified combatant command created restraints that prevented the creation of USCYBERCOM as a unified command. The "ten-command rule" was a widely understood cultural reference point for decision-making. At the same time, the decision to continue a joint organizational model was characterized by explicit considerations of the competing interests within the military that would resist other organizational models like the creation of a new service. However, neither proof of mission maturity nor resource constraints were advanced for keeping USCYBERCOM as a sub-unified command. Indeed, the dual-hat arrangement with the NSA provided USCYBERCOM with a crucial boost in technical and human resources, without which the initiative may have stalled for years as USCYBERCOM would have had to duplicate what already existed in the NSA.[267] Instead, political constraints on a unified command appear to have stemmed from the implicit ten-command rule. As such, organizational size receives mixed support and adoption-capacity receives little support.

Verdict: Mixed support for organizational size. Strong support for cultural explanation and little support for adoption-capacity.

(4) Why was USCYBERCOM established in 2010 and not 2009?

In addition to the question of force structure, the timing of USCYBERCOM's creation provides an examination point for each explanation. Although there was sufficient buy-in and

[267] Former NSA Director of Information Warfare interview with author.

resourcing to establish USCYBERCOM in 2009 the wake of SIPRNet—and Gates had *de facto* created the command with the merger of JTF-GNO and JFCC-NW—the delay was primarily the product of a change in presidential administrations. The political change did not significantly alter the capacity to absorb USYBERCOM, create additional culture constraints, or change existing views on the cyber mission. Thus, there is no evidence to support any of the explanations.

Verdict: Evidence provides no support for organizational size, culture, or adoption-capacity.

(5) Why wasn't USCYBERCOM elevated between 2012 and 2013?

The non-elevation of USCYBERCOM between 2012 and 2013 show the limits of the cultural and adoption-capacity explanations. The disestablishment of U.S. Joint Forces Command in 2011 cleared a major cultural obstacle: it reduced the number of unified combatant commands from ten to nine, theoretically clearing the way for USCYBERCOM to be elevated. At the same time, the disestablishment of USJFCOM also represented a reduction in bureaucracy that theoretically increased the organizational capacity for the military to elevate USCYBERCOM. Moreover, the Snowden leaks provided a potential stimulus for elevation: the revelation of capabilities could have incentivized the elevation of USCYBERCOM to offset the loss of strategic advantage.

However, no such elevation occurred; for two reasons, many in the military believed that the command lacked maturity. On one hand, the command had not been established long enough to merit elevation: the Cyber Mission Force, the main focus of implementation efforts, was only in its initial developmental stages. On the other hand, many combatant commanders did not understand how cyber capabilities affected their own missions. This evidence supports the argument from my theory of organizational size that the likelihood of moving towards full implementation is increased by providing "proof of concept."

Verdict: Evidence provides support for organizational size. No support for culture or adoption-capacity explanations.

(6) Why was USCYBERCOM elevated to a unified combatant command?

The eventual elevation of USCYBERCOM to a unified command resulted from the success of JTF-ARES. Operation Glowing Symphony provided a concrete demonstration of how cyber capabilities could integrate with and support kinetic operations. This "proof of concept" fostered buy-in from military commanders and civilian officials and built support for elevation to a unified command. Moreover, because there were no major changes in military culture or organizational capacity, the elevation of USCYBERCOM casts additional doubt on the explanatory power of these competing frameworks.

Verdict: Strong support for organizational size. No support for culture or adoption-capacity.

Table 5.1 summarizes this discussion.

Table 5.1: Summary of Evidential Support for Alternative Explanations (United States)

	Explanation		
Episode	*Organizational Size*	*Culture*	*Adoption-Capacity*
Introduction/Modification of JTF-CND	***Supports***	***Supports***	Weakly Supports
Failure of AFCYBER(P)	***Strongly Supports***	Weakly Supports	No Support
USCYBERCOM initial force structure	Mixed Support	***Strongly Supports***	No Support
Creation of USCYBERCOM in 2010	No Support	No Support	No Support
Non-elevation of USCYBERCOM, 2012-2013	***Supports***	No Support	No Support
Elevation of USCYBERCOM	***Strongly Supports***	No Support	No Support

CHAPTER 6

The Dynamics of Change in a Small Military: Cyber Force Structure in Estonia

If we compare the United States or the U.K. or Canada to Estonia, Estonia is a village.[1]

- Dr. Jaak Aaviksoo
Fmr. Estonian Minister of Defense

Introduction

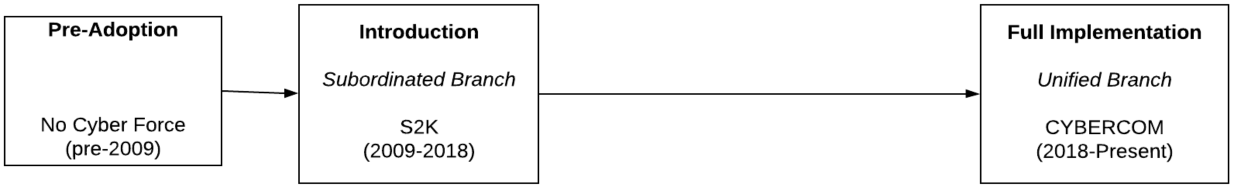
This chapter examines the cyber force implementation dynamics in a small military organization—the Estonian Defense Forces (EDF). Total military personnel for the Estonian Defense Forces peaked in 2003 with roughly 8,100 active duty personnel. From 2009 to 2017, the EDF has had an average size of approximately 5,900 active personnel.[2] This chapter details the creation of and changes in Estonia's cyber force structure. In doing so, it assesses the three competing theoretical frameworks advanced in Chapter 3: organizational size, adoption-capacity, and military culture. Using the operationalization from Chapter 4, Figure 6.1 summarizes the evolution of Estonia's cyber force structure according to implementation stage, the corresponding force structure, and the respective military institution.

This chapter contains four major sections. The first section provides background on Estonia's security environment post-2004 after joining both the European Union and the North Atlantic Treaty Organization. The second section details the chain of events from 2007 to 2009 that led to the delegation of cyber operations to the Estonian Defense Forces' (EDF) Staff and Signals Battalion. The third section examines the creation of the EDF's Cyber Command by

[1] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author, interview by Jason Blessing, Tallinn, Estonia, June 3, 2019.
[2] The World Bank, "World Development Indicators."

looking at efforts to implement a new unified branch from 2010 to 2018. Much of this section is dedicated to detailing the genesis of the new command and the hurdles that its advocates faced. Due to the relative dearth of public information on the establishment of Estonia's Cyber Command compared to the creation of U.S. Cyber Command, the second and third sections rely heavily on interview data. The chapter concludes by evaluating each theoretical explanation as applied to the case of Estonia.

Figure 6.1. The Evolution of Estonia's Cyber Force Structure: Implementation Stage, Force Structure, and Institution.



Background: Estonia's Changing Strategic Environment

Russia has been the most important factor in Estonia's strategic environment, particularly since the country's independence from Soviet rule in 1991.[3] In this regard, two decisions in 2004 represent an important analytical starting point for Estonia's contemporary strategic environment.[4] First, on May 1, 2004, Estonia officially entered the European Union, an important foundation for the future of Estonian foreign policy.[5] Second, Estonia joined the North

[3] Anders Wivel and Matthew Crandall, "Punching Above Their Weight, but Why? Explaining Denmark and Estonia in the Transatlantic Relationship," *Journal of Transatlantic Studies* 17 (2019): 410–11.

[4] Leonid A. Karabeshkin, "The Ongoing Transformation of the Estonian Defence Forces," in *Democratic Civil-Military Relations: Soldiering in 21st Century Europe*, ed. Sabine Mannitz (London and New York: Routledge, 2012), 128.

[5] Ministry of Foreign Affairs, "Estonia in the European Union" (Republic of Estonia, n.d.), https://vm.ee/en/estonia-european-union.

Atlantic Treaty Organization (NATO) in March of 2004 as part of NATO's second wave of post-Cold War expansion; membership was finalized in April of 2007.[6]

NATO membership was particularly impactful and had a dual effect on the strategic environment. Deepening ties with the Western Europe and the United States placed additional stress on official diplomatic relations between Estonia and Russia. Russian officials portrayed Estonia's membership as a hostile attempt to leave the Russian sphere of influence and part of NATO's increasing threat to Russian national security.[7] Estonia's strategic military posture also began to shift from a single focus on territorial defense to a posture that incorporated and relied more on the collective defense guarantees of NATO's Article 5.[8] This shift, which had begun prior to 2004 in anticipation of NATO membership, was accompanied by a desire to both support and contribute to allied security interests with military means. This manifested in decisions to participate in U.S.-led military coalitions in Afghanistan and Iraq.[9] At the same time, Estonia's participation in out-of-area missions and its integration in NATO's collective defense system provided an incentive for its small military force to contribute in a strategically meaningful way.[10]

Many in Estonia saw cyber-security as such an area where they could contribute. Cyber threats did not appear in prominent discussions within NATO: the alliance and its members were

[6] North Atlantic Treaty Organization, "Member Countries" (North Atlantic Treaty Organization, March 24, 2020), https://www.nato.int/cps/en/natohq/topics_52044.htm#:~:text=Cold%20War%20enlargement-,Bulgaria%2C%20Estonia%2C%20Latvia%2C%20Lithuania%2C%20Romania%2C%20Slovakia%20and,of%20enlargement%20in%20NATO%20history.

[7] Hiski Haukkala, "A Close Encounter of the Worst Kind? The Logic of Situated Actors and the Statue Crisis between Estonia and Russia," *Journal of Baltic Studies* 40, no. 2 (2009): 207–10; Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 143.

[8] Karabeshkin, "The Ongoing Transformation of the Estonian Defence Forces," 133.

[9] Wivel and Crandall, "Punching Above Their Weight, but Why? Explaining Denmark and Estonia in the Transatlantic Relationship," 408–9.

[10] Karabeshkin, "The Ongoing Transformation of the Estonian Defence Forces," 134; Wivel and Crandall, "Punching Above Their Weight, but Why? Explaining Denmark and Estonia in the Transatlantic Relationship," 408–9.

preeminently occupied with the wars in Iraq and Afghanistan.[11] For Estonia, NATO membership coincided with the culmination of a host of domestic digital initiatives. The Estonian government invested heavily in the development of information technologies throughout the 1990s and early 2000s. In the drive to become an international leader in information technologies, Estonia's state and private infrastructure became heavily dependent on the Internet.[12] More than any other country in the world, Estonia's critical infrastructure had become cyber-dependent; from routine government forms and banking to military command posts, connectivity to the Internet was an essential part of a functioning state.[13] Much of this was directed towards a political goal: Estonian officials wanted to rapidly break free from the Soviet legacy and to globalize through technology.[14] In an attempt to capitalize on the country's reputation for technological progress and tie it to its membership in NATO, Estonian officials proposed opening a cyber-focused institution within NATO's "Centers of Excellence" scheme.[15] Planning and preparatory

[11] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[12] By 2007, almost the entire country was covered by free wireless internet connections. All government services were available online, and nearly 98 percent of all private financial transactions occurred online. Estonian electronic innovations for everyday life included: providing all Estonian schools with an internet connection; electronic identification cards for citizens; the ability to electronically pay taxes from a mobile phone; the ability to pay for parking meters from a mobile phone; online tracking for parents of their child's school performance. The founding of international communications giant Skype in 2003 only served to accelerate Estonia's reputation for connectedness. Moreover, Estonia pioneered e-voting; in 2005, the country was the first worldwide to introduce electronic voting for their parliamentary elections. See: Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; "Estonia Hit by 'Moscow Cyber War,'" *BBC News*, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm; Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia, and Kyrgyzstan," *European Scientific Journal* 3 (February 2014): 238; Patrick Howell O'Neill, "The Cyberattack That Changed the World," *The Daily Dot*, May 20, 2016, https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/; Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9, no. 1–2 (Winter/Spring 2008), http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia; Sam Shead, "Estonia Is So Scared of a Russian Cyberattack That It's Opening a Data Centre in the UK," *Business Insider*, July 25, 2016, http://www.businessinsider.com/estonia-is-so-scared-of-a-russian-cyberattack-that-its-opening-a-data-centre-in-the-uk-2016-7; Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations" (Cooperative Cyber Defence Centre of Exellence, 2010), 16–18, https://ccdcoe.org/publications/books/legalconsiderations.pdf.

[13] Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 25–27.

[14] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[15] For more on the purpose and operations of current Centers, see: North Atlantic Treaty Organization, "Centres of Excellence" (North Atlantic Treaty Organization, January 24, 2019), https://www.nato.int/cps/en/natohq/topics_68372.htm.

development for this center took place under the Estonian Ministry of Defense (MOD). However, NATO allies were unmoved by the proposal for a cyber center—that is, until late in 2007.[16]

Adapting the Staff and Signals Battalion into a Cyber Force

Despite the push to establish a cyber-focused NATO center of excellence, no real thought had been given to the role of the Estonian Defense Forces in cyberspace.[17] More broadly, Estonia had no government-level cyber-strategy prior to 2008.[18] However, the catalyst for change occurred in May of 2007 after the Estonian government's decision to relocate the "Bronze Soldier," a World War-II memorial in the main square of Tallinn commemorating the Soviet Union's defeat of the Nazis. Although a night of protests occurred, the primary backlash took place online in the form of a three-week onslaught of distributed denial of service (DDOS) attacks. Although not perceived as a distinctly military issue, the attacks facilitated the eventual adaption of the EDF's Staff and Signals Battalion into Estonia's first military arm for cyberspace.

The 2007 Bronze Soldier Episode

The decision in 2007 to relocate the Bronze Soldier of Tallinn was the latest in a string of government initiatives to de-Sovietize Estonia. For many Estonians, Russian and Soviet monuments were symbols that glorified Soviet occupation and distorted history. For the sizeable ethnic Russian minority in Estonia (approximately 26 percent of the population in 2007), visiting

[16] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Former Estonian Ministry of Defense Official #1 interview with author, interview by Jason Blessing, Tallinn, Estonia, June 13, 2019.

[17] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[18] Jamie Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom" (Book Chapter, Oxford, 2016), 24, https://www.politics.ox.ac.uk/materials/publications/15664/strategies-of-cyber-crisis-management.pdf. The government did, however, maintain an emergency response team for smaller-scale cyber crises and computer-related disasters. The Estonian Computer Emergency Response Team (CERT-EE) was established in 2006 to identify potential security threats, handle any security incidents within Estonian networks, and detect and analyze the spread of malware and other security concerns across computers on the Estonian network. Collier, 7.

the Bronze Soldier memorial on May 9 was an important way to celebrate Russia's WWII Victory Day. For the Russian government, statues such as the Bronze Solder were symbols of national pride that represented the glory and strength of Russia's military might.[19] In the lead-up to the general parliamentary election held in March 2007, the removal of the statue had been part of the Reform Party's election platform. After the party's surprising victory and the election of Andrus Ansip as Prime Minister, the decision to relocate the statue received support from a conservative government coalition—one that excluded the moderate Centre Party and instead included the Pro Patria and Res Publica Union, a conservative nationalist party.[20]

The Ministry of Defense had been tasked with handling the physical relocation of the statue, and the date for relocation was set for April 27. That night, in response, protests and riots erupted in the streets of Tallinn.[21] The protests were accompanied by a string of cyber incidents that night that targeted the government and critical infrastructure in the private sector. While the protests only lasted one night, the cyber-attacks continued for almost a month, occurring in three waves: ping-flooding attacks to overload web traffic in the first wave from April 27 to April 29; a wave of targeted botnet distributed denial of services (DDOS) attacks from April 30 to May 11 in the second phase (including the heaviest attack on May 9, Russia's WWII victory day); and a third wave of botnet DDOS attacks occurring from May 11 to May 18.[22] On the government

[19] Alexander Astrov, "States of Sovereignty," *Russian Politics and Law* 47, no. 5 (2009): 66–79; Martin Ehala, "The Bronze Soldier: Identity and Threat Maintenance in Estonia," *Journal of Baltic Studies* 40, no. 1 (2009): 139–58; Marko Lehti, Matti Jutila, and Markku Jokisipila, "Never-Ending Second World War: Public Performances of National Dignity and the Drama of the Bronze Soldier," *Journal of Baltic Studies* 39, no. 4 (2008): 393–418; David J. Smith, "'Woe from Stones': Commemoration, Identity Politics and Estonia's War of Monuments," *Journal of Baltic Studies* 39, no. 4 (2008): 419–30.
[20] Karsten Bruggemann and Andres Kasekamp, "The Politics of History and the 'War of Monuments' in Estonia," *Nationalities Papers* 36, no. 3 (2008): 434–36.
[21] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.
[22] The first phase was carried out by ethnic Russian "script kiddies"; these relatively unsophisticated hackers ran coordinated script from Russian-language hacker websites with internet protocol (IP) addresses originating from Russia. The more devastating DDoS phases were carried out by Russian hackers via botnet servers. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007,

side, the ping and DDOS attacks targeted the servers used by the Estonian parliament, websites of the President and Prime Minister's respective parties, and the institutions in control of Estonian Internet infrastructure. In the private sector, attacks targeted two of the largest financial firms, three news organizations, and several communications firms.[23] Although some form of digital retaliation for relocation had been anticipated, the scope of the cyber incidents had surprised government officials.[24]

Ministry of Defense Takes the Lead. Officials in the Ministry of Defense first identified issues with their computer networks in the early hours of April 28. As Lauri Almann (Estonia's permanent Undersecretary of Defense at the time) has recalled: "We were sitting in the government situation room, and suddenly in walks our chief [public relations] person, who says, 'We are unable to put our press releases out' on government Web sites. We didn't understand the seriousness of the problem until he said, 'We are under cyberattack.'"[25] Later that morning, Minister of Defense Jaak Aaviksoo could not access the Reform Party's website; moreover, he noticed that websites for the leading Estonia news outlets, including the *Posttimees*, were not

https://www.wired.com/2007/08/ff-estonia/. Tikk, Kaska, and Vihul, "International Cyber Incidents: Legal Considerations," 20.

[23] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review* 18, no. 2 (2008), http://www.iar-gwu.org/node/65; "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia; Ruus, "Cyber War I: Estonia Attacked from Russia."

[24] Russian-language forums had been monitored in the weeks leading up to the statue's removal by a task force formed prior to the March 2007 parliamentary elections. The task force—comprised of experts from internet service providers (ISPs), election authorities, police, and national intelligence services—assessed the likelihood of cyber incidents prior to the removal of the Bronze Soldier. By mid-April, it was clear that commenters on these Russian sites were calling for digital attacks on Estonian infrastructure: DDOS attacks were referenced frequently, and the task force notified officials within the Ministry of Defense and the Ministry of the Interior. Likewise, international network security communities identified the potential for cyber incidents based on Russian-language forums monitored for Russia-based cyber-crime, malware, underground economic operations, and espionage. In particular, European IT experts shared their judgements with their counterparts in the Estonian government prior to the removal of the Bronze Soldier. Andreas Schmidt, "The Estonian Cyberattacks" (Book Chapter, Delft University of Technology, 2013), 5–7, http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf.

[25] Wyatt Kash, "Lessons from the Cyberattacks on Estonia," *Government Computer News*, June 13, 2008, https://gcn.com/Articles/2008/06/13/Lauri-Almann--Lessons-from-the-cyberattacks-on-Estonia.aspx?Page=1.

functional.[26] Across the Ministry of Defense and the wider government, officials realized that computer network operations could constitute a nation security threat; these network attacks were not the same as a computer virus or an account hack. Minister Aaviksoo was subsequently briefed on the wider outages and concluded that these network attacks were serious, systematic, and coordinated, and had signs of Russian government involvement[27] despite any concrete links to the Kremlin.[28]

Both internally and externally, Minister Aaviksoo declared the networks attacks a national security threat, likening them to a naval blockade—preventing connectivity to the Internet and functionality across networks was like shutting down ports to the sea.[29] This analogy spread throughout the administration and had become the dominant domestic public narrative by April 30.[30] However, by framing the network attacks as blockade and signaling Russian

[26] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Davis, "Hackers Take Down the Most Wired Country in Europe."

[27] "If your webpage is defaced with Cyrillic letters, it's most probably not the French." Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author. Placing initial blame on the Russian government was based on the IP address evidence, the verbal threats made by Russian government leaders and the Russian media in the days leading up to the removal of the Bronze Soldier, and on Russia's encouragement of rioting in the streets of Tallinn. Emails coordinating attacks were also uncovered; some attacks were set to launch at 12:00 noon. However, the attacks occurred at 11:00 AM, an hour earlier: coordination had actually been planned according to Moscow time, an hour ahead of Tallin's clocks. Kari Alenius, "An Exceptional War That Ended in Victory for Estonia or an Ordinary E-Disturbance?: Estonian Narratives of the Cyber-Attacks in 2007" (European Conference on Information Warfare and Security, Laval, France, 2012), 20–23

[28] Eventually, part of the DDOS assault was identified as originating from a botnet server that Russian security forces had used to attack an opposition political party weeks earlier; the forensics of both the Russian opposition party hack and the Estonia attacks indicated likely Russian FSB involvement. Davis, "Hackers Take Down the Most Wired Country in Europe," 20. Many had also speculated that discussions on the Russian-language hacking forums were sophisticated efforts by the Russian FSB to conceal their actions by socially engineering the appearance of cyber-mob dynamics. Mischa Hansel, "Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks," Journal of International Relations and Development, 2016, 14–16.

[29] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 54.

[30] Alenius, "An Exceptional War That Ended in Victory for Estonia or an Ordinary E-Disturbance?: Estonian Narratives of the Cyber-Attacks in 2007," 19–20. Schmidt, "The Estonian Cyberattacks," 23. Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington Post*, May 19, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html. Interestingly, three days prior to the expected cyber-backlash, the Estonian government had planned a press release regarding the anticipated cyberattacks from Russian-language hacker sites. The administration's goal was to create media attention that would push the EU to call for Russian government intervention and prevention of cyberattacks within their borders (whether or not they were directly responsible). However, diplomatic pressures from within the EU—

culpability,[31] discussions soon emerged over whether Estonia could invoke NATO's collective defense provision. Many across the government, including speaker of parliament Ene Ergma, had believed the network attacks were attempts by the Kremlin to probe NATO's network defenses and readiness.[32] However, after extensive consultation with NATO allies, Defense Minister Aaviksoo announced that there was no basis for triggering Article 5:

> At present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country…Not a single NATO defence minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future.[33]

Although Article 5 was off the table, the Ministry of Defense still coordinated extensively with NATO, the European Union, and others such as the United States, Israel, Finland, Germany, Slovenia, and Sweden. Each entity sent computer emergency response teams (CERTs) to observe and assist the Estonian CERT (CERT-EE), which was operating temporarily under the Ministry of Defense.[34] With international assistance,

particularly from German Chancellor Angela Merkel, who had an upcoming meeting with Russian President Vladimir Putin—persuaded Estonia not to release the statement Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs* 9, no. 1 (Winter 2008): 122–23.

[31] The President and the Foreign Minister delayed blaming the Russian government on the international stage until several days into the attack. This delay may have been strategic: jumping the gun and accusing Russia too early in the crisis could have undermined the Estonian government's credibility in asserting blame—a move that would have complicated the provision of foreign technical assistance On May 1, Estonian Foreign Minister Urmas Paet asserted Russian responsibility for the attack, declaring that several IP addresses came directly from Russian President Putin's office and that government actors were behind the attacks Hansel, "Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks," 12–14; O'Neill, "The Cyberattack That Changed the World.". This message was publicly echoed by speaker of the parliament Ene Ergma, commander of the Estonian armed forces Ants Laaneots, and former Prime Minister and Charmain of the Pro Patria and Res Publica Union Party Mart Laar. Alenius, "An Exceptional War That Ended in Victory for Estonia or an Ordinary E-Disturbance?: Estonian Narratives of the Cyber-Attacks in 2007," 20, 22–23.

[32] Davis, "Hackers Take Down the Most Wired Country in Europe"; O'Neill, "The Cyberattack That Changed the World."

[33] Quoted in "Russia Accused of Unleashing Cyberwar to Disable Estonia." See also: Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations" (Cooperative Cyber Defence Centre of Exellence, 2010), 25–26, https://ccdcoe.org/publications/books/legalconsiderations.pdf.

[34] Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," 54. "Estonia Hit by 'Moscow Cyber War'"; "Russia Accused of Unleashing Cyberwar to Disable Estonia." Tikk, Kaska, and Vihul,

CERT-EE was able to implement a three-pronged strategy: (1) increase Estonia's server capacity to handle the overload of internet traffic from botnets servers; (2) distinguish authentic from the "zombie" traffic responsible for the DDOS to block illegitimate server traffic; and (3) locate and neutralize the bots and zombies used for the attacks.[35] Working around the clock, CERT-EE and its international partners managed to increase bandwidth by May 10 and continued to hunt down botnet servers until approximately May 23.[36]

Sidelining the Military. One of the main insights that emerged from the Ministry of Defense—and subsequently, the rest of the government—was that there was no designated entity responsible for cyber-security or cyber-defense. CERT-EE had become the *de facto* hub for technical coordination, but there were no structures or rules in place for political coordination. Instead, there was a loose network of experts across the government and private sector on which the Ministry of Defense was forced to rely.[37] The Staff and Signals Battalion, a support unit within the EDF tasked with ensuring the availability and functionality of EDF strategic communications and information technology,[38] was the only military entity that possessed such expertise. However, personnel from the Staff and Signals Battalion were largely sidelined during the network attacks and were only brought in as consultants. Only civilian infrastructure had been targeted; no damage had been done to military networks, and the attacks never reached

"International Cyber Incidents: Legal Considerations," 24. Andreas Schmidt, "The Estonian Cyberattacks" (Book Chapter, Delft University of Technology, 2013), 13, http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf.

[35] Ruus, "Cyber War I: Estonia Attacked from Russia"; Tikk, Kaska, and Vihul, "International Cyber Incidents: Legal Considerations," 24. The third prong of the strategy capability and authority beyond that of country-level and NATO CERTs. On the role of "the Vetted", see: Davis, "Hackers Take Down the Most Wired Country in Europe"; O'Neill, "The Cyberattack That Changed the World"; Ruus, "Cyber War I: Estonia Attacked from Russia."

[36] For overviews of CERT-EE's international coordination and the local "beer and sauna" protocol, see: Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 8; Ruus, "Cyber War I: Estonia Attacked from Russia"; Schmidt, "The Estonian Cyberattacks," 23. Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," 124.

[37] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[38] Osula, "National Cyber Security Organisation: Estonia," 10.

defense processes. As a result, there was a clear understanding that the network attacks were not primarily a military defense issue. First and foremost, the network attacks were a civilian political issue.[39]

Moreover, aside from acting as a coordinating body for international assistance, the Ministry of Defense actively looked to downplay its role to avoid the perception that the Defense Forces would intervene in domestic affairs. The Ministry of Defense had been responsible for the relocation of the Bronze Soldier and had taken the lead in coordinating the response to the cyber incidents. As a result, a perception emerged that the Ministry of Defense was responsible for dealing with network attacks more broadly and that the Ministry and the EDF had very strong postures in cyberspace. Neither was true; as such, it fell to the Ministry to draw back and severely limit EDF involvement. According to Minister Aaviksoo, this latter part was particularly important in relation to both the night of protests and the online assault:

> In the Soviet days, if there was something going wrong, the Kremlin would send troops in the streets. We were so sensitive about something like that happening…They never fight their own people. They never show themselves in the streets. And for [the network attacks], you don't centralize, you don't mix things up. There must be a clear distinction line between civil and military.[40]

Despite the lack of direct involvement, the EDF and the Ministry of Defense clearly understood the military implications of the network attacks.[41] Yet, the Ministry pushed to prioritize civilian initiatives over the development of military capabilities. Prior to 2007, most civilian agencies viewed cyber-security as an issue purely for "the IT people"—it simply was not on the radar for most agencies. After the network attacks, however, there was a sense of urgency

[39] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Former Estonian Ministry of Defense Official #1 interview with author.

[40] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[41] Estonian Cyber Command Official interview with author, interview by Jason Blessing, Tallinn, Estonia, June 14, 2019.

to incorporate cyber-security into governmental processes. As such, the Ministry of Defense could not realistically justify diverting resources from much-needed civilian initiatives to expand the Staff and Signals Battalion. Therefore, Minister Aaviksoo tried to prioritize three shorter-term goals. First, the Ministry would begin drafting a comprehensive national cyber-security strategy in conjunction with the Ministry of Economic Affairs and Communications. Second, the Ministry of Defense would work with NATO to establish a cyber center of excellence in Tallinn. The debate over invoking Article 5 had brought cyber threats front and center for Estonia's allies; Minister Aaviksoo saw a window of opportunity for the previously proposed center to materialize. Finally, the Ministry would begin discussions over how to supplement the military's cyber capacity through new reserve initiatives.[42]

Civilian Priority, Limited Military Resources

Within a year, both a national cyber-security strategy and the cyber center of excellence were established. Both developments were direct consequences of the inadequacies exposed during the Bronze Soldier episode.[43] The Ministry of Defense released the first *National Cyber Security Strategy* in May of 2008. The strategy stressed a whole-of-nation approach: organization, technical, and regulatory information security measures were to be implemented across the ministries of Defense, Education and Research, Justice, Economic Affairs and Communications, International Affairs, and Foreign Affairs.[44] Although stating that cyber-security research and development were necessarily intertwined with national defense, military affairs were not directly acknowledged in the strategy. The role of the EDF was only

[42] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Estonian Cyber Command Official interview with author.

[43] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Former Estonian Ministry of Defense Official #3 interview with author, interview by Jason Blessing, Tallinn, Estonia, May 24, 2019.

[44] An initial implementation plan was adopted in May 2009 and progress has subsequently been assessed annually. Tikk, Kaska, and Vihul, "International Cyber Incidents: Legal Considerations," 29–31.

acknowledged as (1) a supporter of efforts by a new NATO cyber center of excellence and (2) as a partner in a new Master's course on cyber-security with Tallinn Technical University.[45]

Despite the lack of public attention, civilian and military leadership within the Ministry of Defense began to expand the Staff and Signals Battalion's responsibilities to explicitly include cyber operations. The Battalion was the only viable option for developing a military capability. The Ministry of Defense had to build on the small pool of existing expertise: the Staff and Signals Battalion had the only functionally-related competence within the military.[46] EDF leadership at the joint staff level and the service level were in consensus over delegating the emerging cyber role to the Staff and Signals Battalion. Given the limited human and financial capital at the EDF's disposal, creating a new and separate military arm for cyberspace was simply not feasible.[47]

Some within the Defense Forces (and a few civilian politicians), however, favored a much stronger posture and pushed for the development of independent cyber capabilities. The Staff and Signals Battalion had taken a backseat during the 2007 network attacks, and several military commanders felt compelled to show that the military had a plan and could deliver solutions to cyber threats. Moreover, these commanders argued that developing cyber capabilities would aid Estonia's integration into NATO—the country could cement its place in the alliance by providing cyber expertise to its partners.[48]

On two accounts, however, these ambitions were quashed. On one hand, the Joint Staff and Chief of Defense (CHOD) General Ants Laaneots, the commander of the EDF, did not support building independent cyber capabilities. Despite the government-wide impact of the

[45] Ministry of Defense, "Cyber Security Strategy" (Republic of Estonia, May 2008), 16–17.
[46] Estonian Cyber Command Official interview with author.
[47] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.
[48] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

2007 DDOS attacks, top military officials remained committed to building the EDF's capacity for territorial defense. The military lacked the resource base to carve out distinct cyber capabilities; the leadership's interests centered on basic capabilities for countering potential Russian aggression. Dedicating resources to cyber capabilities, staffing, and training, would also hamper the EDF's ability to integrate into NATO structures.[49] On the other hand, advocates encountered resistance from the civilian leadership in the Ministry of Defense. As Minister of Defense has reflected:

> I was also skeptical about this development simply because, if you employ 4,000 people [in the military] and have a conscription system…you are so involved in building that very basic capability that it's not wise to take the best military brains and put them in a niche area that is not giving you back what you what you expect.[50]

The mix of strategic imperatives and resource constraints effectively shut down discussions over and independent entity for cyber capabilities in the military.

The launch of the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) on May 14, 2008 further constrained the EDF's ability to implement any new internal cyber initiatives. The CCDCOE was the realization of Estonia's 2004 proposal to NATO; it was set up to organize academics and military practitioners for complex technical cyber-defense exercises and to function as NATO's own cyber think-tank.[51] Civilian and military specialists from across Estonia were needed to staff the CCDCOE. As a result, military personnel from the Staff and Signals Battalion were needed for the Estonian contingent of the CCDCOE. In this way, the CCDCOE absorbed part of the military's human capital, stretching an already-thin resource base

[49] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Former Estonian Ministry of Defense Official #1 interview with author.

[50] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[51] NATO Cooperative Cyber Defence Centre of Excellence, "About Us," *CCDCOE: NATO Cooperative Cyber Defence Centre of Excellence* (blog), n.d., https://ccdcoe.org/about-us.html; Former Estonian Ministry of Defense Official #3 interview with author.

for cyber to its limits.[52] This intensified the EDF's reliance on public universities to develop a pipeline of cyber-defense talent; more than ever, the EDF lacked the resources to build greater cyber expertise in-house.[53]

By June 19, 2008, any possible window that may have existed for an independent cyber force had closed as the Riigikogu (the Estonian Parliament) passed the Defense Forces Organization Act. The Act, which helped finalize the country's post-independence military-related legal construction,[54] officially delegated cyber-related duties to the Staff and Signals Battalion and formalized its relationship to the NATO CCDCOE. The Act went into force on January 1, 2009.[55] More tellingly, in the 2009-2012 period after the Act was passed, no cyber force initiative ever came close to appearing on the agenda of the Riigikogu's National Defense Committee, the legislative committee responsible for handling all military-related issues.[56]

Conceptualizing and Implementing a Unified Cyber Branch

From late 2009 through 2013, the Ministry of Defense continued to prioritize civilian dimensions of cyber-security over the development of the military's cyber capabilities. Cyber-security would not even officially be recognized as a military issue until the release of the second *National Cyber Security Strategy* in 2013. As a result, no serious proposals emerged to create an entity outside of the Staff and Signals Battalion to handle cyber operations. The Ministry did, however, work during this period to increase the military's latent capacity—albeit, indirectly—by establishing a pool of reserve talent to supplement both civilian and military efforts in

[52] Former Estonian Ministry of Defense Official #1 interview with author; Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.
[53] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.
[54] Karabeshkin, "The Ongoing Transformation of the Estonian Defence Forces."
[55] Riigikogu, "Estonian Defence Forces Organisation Act," Pub. L. No. RT I 2008, 35, 213, § 57 (2009), https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530102013067/consolide.
[56] Former Estonian Ministry of Defense Official #2 interview with author, interview by Jason Blessing, Tallinn, Estonia, June 11, 2019.

cyberspace. The turning point came in 2014: structural changes within the Ministry of Defense provided the opportunity to reassess both civilian and military approaches to the cyber domain. Against this backdrop, the initial visions for Cyber Command emerged and were eventually realized in 2018.

Human Capital Constraints, 2010-2013

Strategic documents released in early 2010 gave no attention to the Estonian Defense Forces' approach cyberspace. The *Estonian Long Term Defence Development Plan 2009-2018*, released by the Ministry of Defense in late January of 2010, only acknowledged the CCDCOE as the key mechanism for increasing Estonia's commitment to NATO (and, conversely, the alliances commitment to Estonian defense). More specifically, the document stated that it was "vital to fully develop NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) into an organisation that will bring together competence on cyber security and that will help NATO and Allies to develop military capabilities in this field."[57] Later, in May, the Riigikogu released the *Nation Security Concept of Estonia*. While coordinated cyber-attacks were referenced as a potentially significant national security threat, the discussion in the document was limited to cyber-crime and online extremism[58] with no explicit mention of a military dimension.

Despite the lack of recognition in high-level documents, the Ministry of Defense focused on addressing the military's human capital problem in a way that supported the government's priority on civilian initiatives. Specifically, the Ministry emphasized the development of the reservist Cyber Defense Unit (eventually renamed the Cyber Defense League). The idea for a

[57] Ministry of Defense, "Estonian Long Term Defence Development Plan" (Republic of Estonia, January 22, 2009), 17, https://www.ecfr.eu/page/-/Estonie_-_2009_-_Estonia_long_term_development_plan_2009_2018.pdf.
[58] Republic of Estonia, "National Security Concept of Estonia," May 12, 2010, 6, 8, 17.

cyber component of the Estonian Defense League (EDL)—the country's military reserve system—had arisen in September of 2007 as a result of the fallout from the Bronze Soldier Incident.[59] By 2008, an informal cooperation network emerged within the Estonian Defense League, and the Ministry of Defense formed a working group to formalize this network. The first *de facto* cyber units of the EDL were established in April 2009, and these units were legally codified by the Riigikogu in late January 2011.[60] The 2011 defense strategy's discussion of the role of the Estonian Defense League underscored the importance of the Cyber Defense Unit to military cyber-defense. The EDL was explicitly tasked with developing cyber-defense capabilities to help the Ministry coordinate broader national cyber-security efforts.[61]

The Estonian Defense League's increased cyber capacity provided a crucial pool of civilian talent from which the military could draw, particularly as the Ministry of Defense stepped out of the role as leading coordinator for cyber issues.[62] In early 2011, the responsibility for cyber-security policy coordination was transferred from the Ministry of Defense to the Ministry of Economic Affairs and Communication.[63] This shift was meant to emphasize domestic cyber issues over national security and thereby increase government-wide awareness. Initially, the Ministry of Defense was the only ministry that possessed the resources to coordinate cyber issues across the government; other ministries had limited and fragmented approaches to cyber threats. Long-term, this move was intended to reduce the strain on the

[59] Defense Minister Aaviksoo, with a background in the Estonian educational system, had supported the idea as proposed by Ulo Jaaksoo, a member of the Estonian Academy of Science and CEO of the company Cybernetica AS. Estonian Cyber Command Official interview with author.

[60] Kadri Kaska, Anna-Maria Osula, and Jan Stinissen, "The Cyber Defence Unit of the Estonian Defence League: Legal, Policy, and Organisational Analysis" (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013), 8.

[61] Ministry of Defense, "National Defence Strategy: Estonia" (Republic of Estonia, 2011), 13, https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

[62] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[63] Osula, "National Cyber Security Organisation: Estonia," 7.

Ministry of Defense's resources and allow it to focus more on national security and military defense issues.[64] In the short-term, however, it meant that military approaches to cyberspace would continue to pay deference to civilian priorities. As such, establishing the Cyber Defense League was the only viable way to build military capacity for the cyber mission by linking it with the broader civilian emphasis.[65]

While the Staff and Signals Battalion had officially been tasked with the cyber mission in January of 2009, references to military cyber-defense only occurred at the strategic policy levels after 2013. Although the parliamentary elections of March 2011 brought in new leadership to the Ministry of Defense with Mart Laar, the Ministry was largely marked by continuity. After suffering a stroke in February of 2012, Laar resigned; before Urmas Reinsalu was eventually tapped to replace him, Laar's duties were carried out by Jaak Aaviksoo, who had been appointed Minster of Education and Research after the 2011 elections.[66] Within the Ministry of Defense, discussions centered on framing the EDF's approach to cyber operations—whether the Ministry would state the EDF's intention to develop a strategy of active defense and offensive cyber capabilities or state EDF intentions in a broader manner. An internal paper even emerged during this period advocating for the Estonian proposal of a NATO-level cyber command; this would have required an expansion of the effort currently under the Staff and Signals Battalion.[67]

Although there were people across the Ministry and military willing to discuss more robust strategic and institutional approaches for the EDF—particularly those involved with

[64] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author.

[65] Estonian Cyber Command Official interview with author; Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author. Collier, "Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom," 9–10; Schmidt, "The Estonian Cyberattacks," 24.

[66] "Defense Minister Mart Laar Resigns after Stroke," *ERR*, May 6, 2012, https://news.err.ee/104235/defense-minister-mart-laar-resigns-after-stroke.

[67] Former Estonian Ministry of Defense Official #2 interview with author; Former Estonian Ministry of Defense Official #3 interview with author.

creating the Cyber Defense League—they were not linked in any formal, structural way. As a result, many of these internal discussions went nowhere.[68] Eventually, the Ministry decided that issues related to active defense and offensive capabilities were still too sensitive to state in public documents, particularly given the implications such a statement might have across NATO.[69] The 2013 defense development plan did not comment on the EDF's role in cyberspace. Instead, it linked the creation of the Estonian Defense League's cyber units to Estonia's contribution to the growth of the CCDCOE.[70]

Structural Changes, Strategic Development, and the Idea of Cyber Command, 2014-2015

Shortly after the release of the 2013 defense development plan, the Ministry of Defense took an important step to consolidate civilian and military cyber expertise. On January 31, 2014, Minister of Defense Urmas Reinsalu approved the creation of the Cyber Policy Department within the Ministry. The new department was tasked with coordinating the Ministry's cyber-related initiatives, developing policy proposals, and acting as a point of contact for the rest of the government.[71] Within a month, the Cyber Policy Department was active and the Ministry began looking for an official to head the department.[72] By June, the Ministry had selected Mihkel Tikk to lead the Cyber Policy Department. Tikk, who took over the Department in July and had been

[68] Former Estonian Ministry of Defense Official #3 interview with author.

[69] Former Estonian Ministry of Defense Official #2 interview with author.

[70] Ministry of Defense, "National Defence Development Plan 2013-2022" (Republic of Estonia, 2013), https://www.kaitseministeerium.ee//riigikaitse2022/riigikaitse-arengukava/index-en.html.

[71] Ministry of Defense, "Käskkirjaga nr 34: Küberpoliitika osakonna põhimäärus [Directive No. 34: Statutes of the Cyber Policy Department]" (Republic of Estonia, January 31, 2014), https://www.kaitseministeerium.ee//sites/default/files/elfinder/article_files/kuberpoliitika_osakond.pdf.

[72] Teelemari Loonet, "Kaitseministeeriumis Alustas Tööd Küberpoliitika Osakond [Cyber Policy Department Begins Work in Ministry of Defense]," *Postimees*, February 4, 2014, https://www.postimees.ee/2684832/kaitseministeeriumis-alustas-tood-kuberpoliitika-osakond.

one of the founders of the Cyber Defense League within the Estonian Defense League,[73] would be indispensable in the eventual creation of Cyber Command.[74]

The reorganization of previous Ministry efforts into the Cyber Policy Department resulted in two important realizations. The first was that, despite having the common goal of streamlining and enhancing the Ministry's efforts in cyberspace, there were major differences in civilian and military mindsets about how to reach that goal. Shortly after Tikk took the reins, the Cyber Policy Department consolidated information and communication technology (ICT) services—not cyber capabilities, but purely service-layer consolidation. Those from the EDF asserted that the Ministry's ICT services should be streamlined to support warfighting. Conversely, civilians in the Ministry argued that ICT consolidation should prioritize peacetime functions to better integrate and coordinate with other ministries. Prior to the creation of the Cyber Policy Department, these discussions were confined to their respective camps with little crossover. Civilian MOD personnel rarely went out into the field, on missions, or even to military exercises to understand how ICT could support warfighting. Similarly, EDF personnel rarely went to the Ministry to partake in the broader strategic discussions on the role of ICT for cross-governmental and international strategic relations. The Cyber Policy Department brought these two blocs together to identify common goals and overlapping responsibilities.[75]

The second realization was that existing arrangements—both civilian and military—were decentralized and wildly inefficient considering resource limitations. At the civilian level, almost every suborganization and department within the Ministry of Defense had its own chief

[73] Marek Kuul, "Kaitseministeeriumi Küberpoliitika Osakonda Hakkab Juhtima Mihkel Tikk [Mihkel Tikk Will Head the Cyber Policy Department of the Ministry of Defense]," *ERR*, June 13, 2014, https://www.err.ee/514725/kaitseministeeriumi-kuberpoliitika-osakonda-hakkab-juhtima-mihkel-tikk.

[74] Estonian Cyber Command Official interview with author.

[75] Estonian Cyber Command Official interview with author; Former Estonian Ministry of Defense Official #2 interview with author.

information officer, chief information security officer, or chief technology officer. Tikk and MOD leadership recognized that centralizing these efforts would not only streamline defense processes related to the cyber domain but would also save money.[76] Within the EDF, although the Staff and Signals Battalion was responsible for military network defense, each of the services—the Army, Navy, and Air Force—and Special Operations Command had their own technical teams and subcommands to support their respective operations. Over time, this institutional setup had become operationally inefficient and ineffective. As a result, the creation of the Cyber Policy Department spurred an examination of how the Estonian Defense Forces could better organize its efforts in the cyber domain.[77]

The Initial Vision for Cyber Command. Discussions within the Cyber Policy Department over consolidating the cyber elements of the EDF grew in earnest as the department collaborated in the development of the second National Cyber Strategy. The strategy—heavily influenced by the CCDCOE[78]—was released in September of 2014 and was the first strategic document to publicly acknowledge the EDF's role in cyberspace. Although a limited acknowledgement, it did specify the military's intent to develop cyber capabilities for the purposes of collective defense under NATO.[79]

This new public-facing outward stance reflected the Ministry of Defense's internal debates over developing a more robust EDF posture in cyberspace. The Ministry of Defense's

[76] Estonian Cyber Command Official interview with author.

[77] Estonian Cyber Command Official interview with author; Former Estonian Ministry of Defense Official #2 interview with author.

[78] NATO Cooperative Cyber Defence Centre of Excellence, "Centre Contributed to New Estonian Cyber Security Strategy," December 29, 2014, https://ccdcoe.org/news/2014/centre-contributed-to-the-new-estonian-cyber-security-strategy/.

[79] Ministry of Economic Affairs and Communication, "National Cyber Security Strategy for 2014-2014" (Republic of Estonia, September 2014), 10, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf; Former Estonian Ministry of Defense Official #2 interview with author; Former Estonian Ministry of Defense Official #1 interview with author. This strategy was also accompanied by an implementation plan for the 2014-2017 period that remains classified. Osula, "National Cyber Security Organisation: Estonia," 7.

Permanent Secretary, Mikk Marran, had reached out to Tikk during this period about gaining support from Riho Terras, the Chief of the Defense Forces (CHOD) since December 2011, for restructuring the EDF.[80] Terras needed no convincing, however. He favored the development of cyber capabilities and was one of the drivers behind the proposal to establish a NATO-level cyber range training facility in Estonia; he had even offered the alliance use of the Staff and Signals Battalion's cyber range in June of 2014.[81] Instead, Tikk responded that the CHOD did not have time to discuss the dynamics of a reorganization. Rather, the key to gaining support for reorganization was to convince everyone around him—the Joint Staff and the service chiefs—that a new command was necessary. That way, when Terras consulted the Joint Staff and the services towards a final decision, everyone would be on the same page and would recommend reorganization.[82]

A potential reorganization of the EDF's cyber capabilities coalesced around three main arguments. First, growing needs for high-level coordination for countering network attacks demanded a more comprehensive institution within the military. Consolidating the EDF's existing efforts into a new system or organization would facilitate coordination both internally within the Estonian ecosystem and externally with NATO allies. In this regard, the current arrangement under the Staff and Signals Battalion proved inadequate.[83] Second, and relatedly, the Staff and Signals Battalion lacked the resources to be effective on a larger scale. In particular, the Battalion lacked a sufficient workforce, and the residual talent in the military was dispersed

[80] Estonian Cyber Command Official interview with author.
[81] Estonian Cyber Command Official interview with author; Former Estonian Ministry of Defense Official #1 interview with author; Estonian Defence Forces, "Terras: NATO Kavandab Eestisse Küberharjutusvälja Loomist [Terras: NATO Plans to Create a Cyber Training Range in Estonia]," June 12, 2014, https://mil.ee/uudised/terras-nato-kavandab-eestisse-kuberharjutusvalja-loomist/. The Cyber Range had been developed under the Staff and Signals Battalion since 2012; Osula, "National Cyber Security Organisation: Estonia," 10.
[82] Estonian Cyber Command Official interview with author.
[83] Estonian Cyber Command Official interview with author.

across the combat services. A new organization that was higher in the chain of command could consolidate existing talent and would be more likely to attract governmental resources to recruit and train new cyber operators.[84]

Finally, reorganizing the military's cyber efforts offered an opportunity to reduce the bureaucratic hurdles related to command and control. The increasing operational speed in cyberspace required a shorter chain of command than was currently in place. For a directive from the Cyber Policy Department to reach military elements, it had to go through multiple levels of bureaucracy: the Cyber Policy Department was under the Minister of Defense, the Command, Control, Communications, and Computers Directorate (the J-6 Directorate, responsible for cyber planning) was located under the Chief of Staff of the Military, and the Staff and Signals Battalion was directly under the command of the Chief of Defense. Moving across lines of command risked losing coordination at either the strategic, strategic supporting, or operational levels. Centralizing these efforts would both increase operational speed and create the possibly for some issues to reach higher political levels to respond more swiftly to attacks.[85] The general conclusion was that a new cyber-focused command should be created within the Estonian Defense Forces. Instead of building capabilities and then creating an independent command, many in the Cyber Policy Department believed that by defining a clear organizational end-state—a new military command—it would be easier to build support around an initiative.[86]

Designing a Cyber Command. Heading into 2015, the Cyber Policy Department began working on an internal cyber policy plan for the Ministry of Defense. As part of this effort, the Department created a roadmap for consolidating the EDF's cyber efforts into a new cyber

[84] Estonian Cyber Command Official interview with author; Former Estonian Ministry of Defense Official #2 interview with author.
[85] Estonian Cyber Command Official interview with author.
[86] Estonian Cyber Command Official interview with author.

command. Much of this stage of planning was dedicated to gathering like-minded civilians and military commanders. In particular, the Cyber Policy Department engaged with the head of the Joint Staff's J-6 Directorate, the commander of the Staff and Signals Battalion, and their incoming replacements, all of whom supported the creation of a cyber-specific command of some kind. The key was to create a command plan that everyone would understand and support, and this became the team that would define that plan.[87]

The main challenge was to convince military leadership—primarily the Chief of Defense, the Joint Staff, and to a lesser degree, the service commanders—that creating a new command was not an overwhelming risk, i.e. that it would not detract from the military's primary goal of developing the Army's capabilities for Baltic defense.[88] Although CHOD Terras had continually supported the growth of cyber initiatives in the EDF, much of the top military leadership still maintained a mindset of "computers versus bullets."[89] Many feared that their resources—budgetary, personnel, and technological—would be reassigned to cyber operations and military support functions. As a result, the working group, operating out of the Cyber Policy Department, identified areas where the EDF could invest in cyber capabilities moving forward without compromising other military priorities. Moreover, the working group pitched the new command as a cost-saving measure.[90]

In terms of organizing the command, the creation of a new unified branch emerged from the working group as the only feasible force structure. The new cyber command would be modeled in part after the Estonian Special Operations Force, an independent branch of the

[87] Estonian Cyber Command Official interview with author.

[88] Former Estonian Ministry of Defense Official #1 interview with author; Estonian Cyber Command Official interview with author.

[89] Former Estonian Ministry of Defense Official #2 interview with author; Estonian Cyber Command Official interview with author.

[90] Estonian Cyber Command Official interview with author.

military that stood apart from the combat service ecosystem. The Special Operations Force offered a useful heuristic: it had a non-traditional mission set that did not fit into how the services defined their own missions and it operated directly under the Chief of Defense.[91] A joint-service construct had little appeal—the Staff and Signals Battalion was already providing communications and signals support for the services, particularly for the Air Force and Navy. These services had only a marginal stake in developing the cyber domain;[92] for example, without its own fighter jets, the Air Force was more concerned with renting fighter jets from NATO allies for training personnel.[93] As such, it made no sense to utilize a joint-force model: "We are not as big as the U.S., where every service and every subcommand can have their own huge IT department. It just didn't make sense."[94]

Moreover, the Army, by far the largest and most influential service, had no opposition to the branch model as long as the new cyber commander's power remained checked.[95] A service-level construct was also not feasible: the EDF simply lacked enough people to form a fourth service,[96] and the Army had no real base of expertise or desire around which to build a sub-unified service command.[97] As a result, the working group settled on the creation of a new unified branch: it represented the best way to support the services equally while maintaining the freedom to develop future capabilities and talent through the reserve system.[98]

[91] Former Estonian Ministry of Defense Official #1 interview with author.
[92] Estonian Cyber Command Official interview with author.
[93] Former Estonian Ministry of Defense Official #3 interview with author.
[94] Estonian Cyber Command Official interview with author.
[95] Estonian Cyber Command Official interview with author.
[96] Former Estonian Ministry of Defense Official #2 interview with author.
[97] Former Estonian Ministry of Defense Official #1 interview with author.
[98] Estonian Cyber Command Official interview with author.

Finalizing the Plan for Cyber Command and Initial Operating Capability, 2016-2018

Surprisingly, resistance within the EDF to the command proposal turned out to be quite low. Instead, most of the opposition came from the middle-management level within the Ministry of Defense. A major element of the Cyber Command proposal was to relocate the Ministry's IT service provision under the new command. Civilian operators faced a culture shock: they would be moved from a purely civilian-IT work environment to one where they operated alongside and in conjunction with military elements. Middle management feared that this consolidation would reduce the Ministry's service levels.[99]

A key factor in getting these three constituencies—EDF leadership, civilian IT operators, and Ministry middle management—on the same page was Mihkel Tikk's professional background. Tikk had been selected as head of the Cyber Policy Department because of his extensive experience in the IT sectors of the government, as an officer in the Estonian Defense League, and in the private sector. With this background, Tikk was able to recognize the differences in each camp's argument; they were all talking about the same issues and goals but with different semantics that prevented finding common ground. Moreover, much of the planning and organizational designing to date had been focused at the operational level. As a result, EDF leadership, military cyber operators, and civilian IT providers focused on the implications of a new command on their respective operational environments. Tikk's approach, then, was to frame the cyber command proposal in terms of common strategic ends. By defining the new command's purpose in broader strategic terms, Tikk explained how a cyber command would support existing defense and military policy and other end goals as laid out by the MOD. Crucially, Tikk had cultivated trust as a translator across these groups—because of his

[99] Estonian Cyber Command Official interview with author.

background and his personal connections, each group saw him as "one of their own."[100] As a result of Tikk's efforts, Chief of Defense Terras became convinced of the need to establish a new branch, and that a cyber command could be his legacy in the EDF.[101]

International Dimensions. Several international dynamics helped build additional support for a new cyber command. On the one hand, leadership at the CCDCOE—particularly the director, Sven Sakkov, who had previously worked in the Ministry of Defense—had been advocating for an Estonian cyber command. The development of a cyber command would keep Estonia relevant as the primary engine of the CCDCOE, particularly as NATO was moving closer to acknowledging cyberspace as an official military domain.[102] On the other hand, the alliance's move towards recognizing cyberspace as an operational domain raised geopolitical concerns that incentivized a new command. Interoperability with allied forces was certainly a concern,[103] and the Staff and Signals Battalion was not seen as a particularly strong point of contact for international coordination.[104] However, the main concern vis-à-vis NATO was Estonia's security dividend from the alliance. Specifically, the Ministry of Defense and the EDF did not want NATO to provide military assistance for the "wrong problems," i.e. sending allied support to combat hybrid threats (including cyber operations) instead of providing hard capabilities (air policing capabilities and troop rotations) to bolster territorial defense efforts.

Therefore, part of the appeal of a cyber command was as a signal to NATO: the new command represented a robust response to threats from cyberspace, so the alliance should continue to aid the EDF's deficiencies in traditional military capabilities.[105] In the lead-up to

[100] Estonian Cyber Command Official interview with author.
[101] Former Estonian Ministry of Defense Official #1 interview with author.
[102] Former Estonian Ministry of Defense Official #1 interview with author.
[103] Former Estonian Ministry of Defense Official #3 interview with author.
[104] Former Estonian Ministry of Defense Official #2 interview with author.
[105] Estonian Cyber Command Official interview with author; Former Estonian Ministry of Defense Official #2 interview with author.

NATO's recognition of cyberspace, the working group within the Cyber Policy Department consulted extensively with NATO allies about developing a command. Consultations with allies, particularly with the United States and the United Kingdom, over cyber issues had been occurring since the 2007 network attacks.[106] In the 2015-2016 period, the Cyber Policy Department explicitly narrowed conversations with allies to assess the different organizational models for cyber forces emerging across NATO members. Some of these consultations extended to non-NATO nations.[107]

NATO formally recognized cyberspace as a military warfighting domain in June of 2016.[108] Defense ministers across the alliance reaffirmed the applicability of collective defense to the domain at the NATO Warsaw Summit that July. This was the culmination of efforts that had begun in 2014 during the Wales Summit, when the alliance stated the applicability of international law to cyberspace.[109] Although not the primary driver behind Estonia's plans to create a new cyber command, NATO's recognition of cyberspace acted as an accelerant to finalize the proposal.[110]

An Open Window and Initial Operating Capability. NATO's 2016 declaration coincided with the opening of a policy planning window within the Ministry of Defense. The Ministry had begun crafting its new defense development plan, with the previous 2008 plan set to expire in 2018.[111] Throughout the formulation of the new development plan, it became clear that the cyber

[106] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Former Estonian Ministry of Defense Official #2 interview with author.

[107] Estonian Cyber Command Official interview with author. At the request of the interviewee, the names of specific NATO and non-NATO states that were consulted have been excluded.

[108] Julian E. Barnes, "NATO Recognizes Cyberspace as New Frontier in Defense," *The Wall Street Journal*, June 14, 2016, https://www.wsj.com/articles/nato-to-recognize-cyberspace-as-new-frontier-in-defense-1465908566.

[109] Tomas Minarik, "NATO Recognizes Cyberspace as a 'Domain of Operations' at Warsaw Summit" (NATO CCD COE Publications, July 2016), https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

[110] Estonian Cyber Command Official interview with author.

[111] Former Estonian Ministry of Defense Official #1 interview with author.

command proposal would materialize. CHOD Terras was a particularly strong proponent of creating a cyber command at this point: his incoming replacement, Major General Martin Herem, was a seen as a "tank guy." Major General Herem looked to dedicate even more attention to the development of the Army's capabilities; as such, this represented the best opportunity for Terras to move forward with creating a cyber command.[112] Moreover, Hannes Hanso, Minister of Defense from September 2015 to November 2016, had left the Ministry to become Chairman of the National Defense Committee of the Riigikogu; this presented a prime opportunity to cement legislative support around the new command.[113] As a result, the development plan, released by the Ministry of Defense in early 2017, announced that the EDF would officially establish a new cyber command. The decision was framed as a direct consequence of NATO's decision to recognize cyberspace as a military domain at the 2016 Warsaw summit.[114]

Three other events gave greater weight to this decision. First, in February 2017, the CCDCOE released the second, updated version of its *Tallinn Manual*, the most comprehensive analysis on the application of existing international law to cyberspace.[115] Second, Estonia rotated into a six-month occupancy of the presidency of the Council of the European Union; a major pillar of the country's agenda was technological innovation.[116] In September 2017, the Estonian Ministry of Defense hosted an EU conference for defense ministers and featured the first high-

[112] Former Estonian Ministry of Defense Official #1 interview with author.

[113] Former Estonian Ministry of Defense Official #2 interview with author.

[114] Ministry of Defense, "National Defence Development Plan 2017-2026" (Republic of Estonia, 2017), https://www.kaitseministeerium.ee/riigikaitse2026/arengukava/eng/.

[115] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

[116] Former Estonian Ministry of Defense Official #1 interview with author. For a collection of documents related to the Estonian agenda for the presidency, see: Ministry of Education and Research, "Estonian Presidency of the Council of the European Union 2017" (Republic of Estonia, 2017), https://www.hm.ee/en/activities/european-union/estonian-presidency-council-european-union-2017#:~:text=Estonia%20was%20holding%20hold%20its,than%20500%20million%20EU%20citizens.

level cyber tabletop exercise.[117] Finally, in January of 2018, the CCDCOE was tapped by NATO to lead the alliance's cyber-defense training and education efforts.[118] This provided the final push for the creation of an Estonian cyber command across the rest of the government.[119]

On June 21, 2018, parliament passed a statute revising the organization of the military, and in doing so formally established Cyber Command as a unified branch of the EDF. The units under the new command included: the Staff and Signals Battalion; an information communication technology center; the Strategic Communications Centers; the Headquarters and Support Company; and the Cyber and Information Operations Center.[120] The command remained geographically dispersed with units located in both Tallinn and Tartu;[121] defining new reporting structures in the command became the initial priority. With Terras leaving the CHOD position in December, Cyber Command (under command of Colonel Andres Hairk, former commander of the Staff and Signals Battalion) pushed to achieve initial operating capability by August 2018 and established the goal of reaching 300 personnel (compared U.S. Cyber Command's approximately 6,200 personnel in late 2018[122]) and full operating capacity by 2023.[123]

Analysis and Conclusion

To what extent can organizational size, adoption-capacity, or organizational culture explain the development of Estonia's cyber force structure? The Estonian case offers support for my claim

[117] European Union Agency for Cybersecurity, "European Defence Ministers Meet for Cyber Exercise Support by ENISA," September 8, 2017, https://www.enisa.europa.eu/news/enisa-news/european-defence-ministers-meet-for-cyber-exercise-supported-by-enisa.

[118] Grace Johansson, "NATO CCDCOE Coordinates NATO Cyber Education and Training," *SC Media*, February 8, 2018, https://www.scmagazineuk.com/nato-ccdcoe-coordinates-nato-cyber-education-training/article/1473351.

[119] Former Estonian Ministry of Defense Official #1 interview with author.

[120] Riigikogu, "Kaitseväe Põhimäärus [Statutes of the Defence Forces]," Pub. L. No. RT I, 28.06.2018, 8, 45 (2018), https://www.riigiteataja.ee/akt/128062018008.

[121] Former Estonian Ministry of Defense Official #1 interview with author.

[122] "Statement of Genernal Paul M. Nakasone, Command United States Cyber Command before the Senate Committee on Armed Services," Testimony (Washington, D.C.: U.S. Senate Committee on Armed Services, February 14, 2016), 1, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

[123] Estonian Cyber Command Official interview with author.

that organizational size is the primary factor shaping the implementation of cyber forces. Answering three questions provides more detailed insight into the comparative explanatory power of each theoretical framework.

(1) Why was Estonia's initial cyber force structure limited to the Staff and Signals Battalion?

Evidence from the 2007-2009 period indicates that the Bronze Soldier network attacks spurred discussions for institutional reform across the government, including within the Estonian Defense Forces. The decision to limit initial cyber force structure to a subordinated branch—in the form of the Staff and Signals Battalion—can be attributed to three potential causes. First, the cultural explanation would suggest that force structure decisions were constrained by a military culture of restraint in domestic affairs that developed in the years after independence from the Soviet Union. Defense Minister Aaviksoo's recollections lend credibility to this explanation: there was an explicit decision not to involve the military in civilian efforts to combat the 2007 DDOS attacks, and a similar logic was advanced for delaying new military initiatives for cyberspace: civilian efforts to protect domestic networks were prioritized over broad changes to the military's posture. This explanation, however, is undermined by the desire of many in the Staff and Signals Battalion to implement a more robust military posture.

This episode provides support for both my theory of organizational size and adoption-capacity theory. Consistent with my expectations for organizational size, risk aversion played a major role in determining the initial subordinated branch cyber force structure. Minister Aaviksoo explicitly acknowledged that, creating new military structures were seen as too risky. Unlike investments in the CCDCOE and the Cyber Defense League, investing a new command for the military had a low return. It was akin to putting all the military eggs in one basket: the limited size and resource base of the military meant that the military did not possess the risk tolerance to create a new military command while simultaneously building territorial defense capacity and integrating into NATO. Because the experience of 2007 had acted as a stimulus for government-wide action, the lack of risk tolerance meant that the existing Staff and Signals Battalion was the only option for creating a cyber force structure.

However, this evidence is also consistent with the expectations of adoption-capacity. The 2007 network attacks provided systemic-level motivation to address a novel security area and possessed an existing—albeit limited—capacity to absorb cyber operations into the Staff and Signals Battalion. Evidence from 2008 to 2010 suggests that capacity limited a more large-scale institutional response by (1) the need for the Staff and Signals Battalion to simultaneously staff the CCDCOE and (2) the inability of the Ministry of Defense to dedicate resources to both civilian and military initiatives.

Verdict: Support for both organizational size and adoption-capacity. Little support for the cultural explanation.

(2) Why was a unified branch force structure chosen for Cyber Command?

The Estonian military is dominated by the Army: it is the largest branch, represents the largest faction of the Joint Staff, and the Chief of Defense has traditionally come from the Army. As such, it has traditionally exhibited lower levels of jointness compared to other militaries in NATO.[124] Therefore, cultural logics would suggest that as initiatives for the cyber domain gain support, the cyber mission would naturally be incorporated into Army structures as a form of territorial defense. Yet, Army leadership and those in the Joint Staff expressed no interest in taking over the cyber mission. A lack of substantial jointness could have enabled the creation an

[124] Estonian Cyber Command Official interview with author; Former Estonian Ministry of Defense Official #1 interview with author.

independent service, this option was ultimately discarded. This indicates a lack of support for cultural explanations.

Consistent with the expectations of my theory, the size of the Estonian Defense Forces prevented a deviation from the branch model. The limited personnel pool for the military as a whole —evidenced by Estonia's continued reliance on conscription—forced each service to focus on their primary missions in the land, sea, and air domains. As a result, there was no interservice competition over the cyber mission: the services had no interest in expanding their mission sets when they were still struggling to fulfill their primary purposes. Internal power games were over resources that were not related to the cyber domain.[125] Because the services had no real footprint in the cyber domain, they had no preference over organizational design. In fact, the services actually supported the development of offensive cyber capabilities under a branch model.[126] Organizational size also impacted the decision against pursuing a new cyber service: the EDF lacked enough cyber-specific personnel to build a new service. As such, reorganizing talent from across the EDF within the existing branch construct remained the only viable option. This evidence also supports the main claim from adoption-capacity theory. The EDF lacked the capacity—particularly in terms of human capital—to undertake a joint or service construct.

Verdict: Strong support for both organizational size and adoption-capacity; no support for the cultural explanation.

(3) Why wasn't Cyber Command established in prior to 2018?

Interviews consistently point to the 2007 network attacks as the "proof of concept" behind the push to establish Cyber Command.[127] Why, then, did this proof of concept not

[125] Estonian Cyber Command Official interview with author.

[126] Estonian Cyber Command Official interview with author.

[127] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Former Estonian Ministry of Defense Official #1 interview with author; Former Estonian Ministry of Defense Official #2 interview with author; Former

translate into the creation of Cyber Command prior to 2018? There is no evidence that military culture played a role. Adoption-capacity logic suggests that two external demonstration events identified by interviewees should have spurred the creation of Cyber Command in the years before 2018. The first was the creation of U.S. Cyber Command in 2010; the second was the 2012 revelations surrounding Operation Olympic Games that targeted an Iranian nuclear facility.

Although civilian and military officials in the Ministry of Defense discussed the impacts of both events, neither event incentivized decisionmakers to create Cyber Command within the EDF. While the operation against Iran spurred the CCDCOE to think more seriously about legal implications of cyber incidents, leadership within the Estonian MOD continued to emphasize NATO's defense planning for the Baltics.[128] Instead, the creation of Cyber Command hinged on three things: the establishment of the Cyber Policy Department, gaining support from MOD leadership, and getting buy-in from the leadership in the EDF. Although the creation of the Cyber Policy Department reduced bureaucratic complexity and increased organizational capital in the Ministry of Defense, it did not directly change the organizational capacity of the military. Therefore, evidence only weakly supports adoption-capacity.

Moreover, the security environment was dominated by Russia: Estonia had been one of the states in the eastern flank of NATO trying to push Russian aggression onto the alliance's agenda since the early 2000s (success would only occur after the 2014 Russian invasion into Crimea).[129] A concern with provoking Russia, coupled with the limited number of cyber operators in the Staff and Signals Battalion, provided few opportunities for linking operational

Estonian Ministry of Defense Official #3 interview with author; Estonian Cyber Command Official interview with author.

[128] Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author; Former Estonian Ministry of Defense Official #1 interview with author.

[129] Former Estonian Ministry of Defense Official #1 interview with author.

effects of cyber capabilities to broader military interests. As a result, military-wide knowledge of operational effects was derived from the 2007 network attacks. With over ten years between the 2007 attack and the 2018 creation of Cyber Command, ***interpersonal connections and trust*** were the main factors linking the operational and strategic payoffs of Cyber Command to existing military interests. In this way, organizational size facilitated the link between the future effects of Cyber Command and the interests of MOD and EDF leadership. Mihkel Tikk was instrumental in this regard—his personal connections across the EDF, Ministry of Defense leadership, and civilian IT operators were crucial in building a broad coalition of support for Cyber Command. In such a small organization, building trust among personal ties for the creation of a new military command proved indispensable.[130] This provides support for the theory of organizational size.

Verdict: Support for organizational size, weak support for adoption-capacity, and no support for military culture.

Table 6.1 summarizes the evidential support for each explanation.

[130] Estonian Cyber Command Official interview with author; Former Estonian Ministry of Defense Official #1 interview with author.

Table 6.1: Summary of Evidential Support for Alternative Explanations (Estonia)

	Explanation		
Episode	*Organizational Size*	*Culture*	*Adoption-Capacity*
Delegation to Staff and Signals Battalion	***Supports***	Weakly Supports	***Supports***
Decision to Utilize Branch Model	***Strongly Supports***	No Support	***Strongly Supports***
Creation of Cyber Command in 2018	***Supports***	No Support	Weakly Supports

CHAPTER 7

Conclusion

Overview

This dissertation provides a conceptual and theoretical framework for understanding and explaining the variation in cyber force implementation dynamics across militaries. In doing so, this project provides two much needed contributions to the international security literature on cyber conflict. First, this project advances a novel typology for categorizing cyber force structure and identifies nine distinct arrangements: Subordinated Branch, Subordinated Service, Subordinated Joint, Sub-Unified Branch, Sub-Unified Service, Sub-Unified Joint, Unified Branch, Unified Service, and Unified Joint. Second, I create the first comprehensive database on cyber forces worldwide that catalogues changes in cyber forces structures over time.

This dissertation has argued that the implementation of cyber forces—as well as choices and changes in cyber force structure—is shaped by organizational size. The size of a military helps mitigate the implementation tension between building an operationally effective cyber force and integrating it into the broader defense bureaucracy. Implementers in large militaries are more likely to initially prioritize bureaucratic integration, while those in smaller militaries are more likely to prioritize operational concerns. Despite a greater risk tolerance and the availability (relative to smaller organizations) of human and financial capital to build an operationally effective cyber force, larger militaries entail a greater number of competing interests that can lay claim to the cyber mission. As such, implementers in larger militaries are more predisposed to ensure the bureaucratic integration and organizational survival of cyber forces before prioritizing mission-building. Conversely, implementers in smaller militaries are more likely to focus directly on mission-building. Implementers face a smaller pool of bureaucratic competitors; however, smaller militaries possess a smaller resource base and lack the risk tolerance of larger militaries. Accordingly, implementers are more likely to vigorously make a case for operational effectiveness to justify the additional strain on financial and human capital caused by building a more bureaucratic cyber force. In this way, organizational size shapes implementation priorities and influences implementation pathways and the changes in cyber force structure.

Summarizing and Evaluating the Findings

Chapter 2 established the variation in cyber force structures both across militaries and within militaries over time to show that principle diffusion has occurred. The quantitative analysis in Chapter 4 and the case studies of the United States (Chapter 5) and Estonia (Chapter 6) provide empirical support for my theoretical claims. Table 7.1 recaps each of my five hypotheses and summarizes the support from both quantitative and qualitative analysis.

Hypothesis 1 stated that the relationship between military size and the risk of completing the implementation is curvilinear. The quantitative analysis in Chapter 4 provided support for this hypothesis: smaller militaries are at a greater risk of fully implementing cyber forces over time than larger organizations. In effect, smaller organizations have a reduced median process duration time compared to larger military organizations. This finding is bolstered by the case studies: once started, the implementation process for the U.S. spanned 19 years (1998-2017) and entailed moving between four stages (Introduction, Modification, Expansion, and Full Implementation); conversely, Estonia's implementation length was only nine years (2009-2018) and only involved two stages (Introduction and Full Implementation).

Hypothesis 2 postulated that, due to a greater tolerance for risk, large militaries were more likely to transition into Introduction than smaller militaries. This hypothesized relationship between size and the probability of transitioning into Introduction over time found support in the quantitative analysis. Evidence from the case studies provide additional support for this hypothesis by linking size to the introduction of a cyber force through risk tolerance. In the case of the United States, internal experimentation via wargaming (in the form of the 1997 ELIGIBLE RECEIVER exercise) identified the need for a cyber-specific force to address computer network operations. As a large organization, the U.S. military was able to use internal wargaming to identify an area of risk that had not yet emerged as strategically salient and subsequently establish Joint Task Force – Computer Network Defense as a response. Conversely, Estonia's military relied on external stimuli (the 2007 network attacks) to justify the delegation of cyber responsibilities to the Staff and Signals Battalion. Estonia provided no evidence of internal experimentation efforts related to the cyber domain: the military simply lacked resources and maintained its focus on building traditional military capabilities. The inability to absorb a cyber force also delayed the creation of a formal role for the Staff and Signals Battalion as civilian initiatives were prioritized.

Both quantitative and qualitative analysis support Hypothesis 3—that large militaries are more likely to transition into Modification than smaller militaries. With regards to the case studies, size shaped the dynamics of Modification of the U.S. cyber force structure while it deterred Modification in the Estonian case. As a large military, the United States exhibited redundancy across the services: each military service had developed their own footprint in the cyber domain. As such, each service had an interest in retaining its share of the cyber mission. This simultaneously incentivized the transition from a branch model to a joint model (with the relocation of JTF-CND from DISA to USSPACECOM) and counterbalanced the attempted standup of AFCYBER(P) as the Air Force sought to secure a greater share of the cyber mission.

Table 7.1. Summary of Support for Hypotheses Derived from Theory of Organizational Size

Hypotheses	**Quantitative Analysis**	**Qualitative Analysis**
H1: The relationship between military size and the risk of completing the implementation process is curvilinear.	Supports	Supports
H2: Larger militaries are more likely to transition into Introduction than smaller militaries.	Supports	Supports
H3: Cyber forces in larger militaries are more likely to transition into Modification than those in smaller militaries.	Supports	Supports
H4: Cyber forces in larger militaries are more likely to transition into Expansion than those in smaller militaries.	Supports	Supports
H5: Cyber forces in larger militaries are more likely to transition into Full Implementation than those in smaller militaries.	Does Not Support	Supports (Qualified)

Conversely, Estonia’s military exhibited practically no redundancy: size restricted the services’ ability to expand operations outside their core missions. As a result, the services had no substantial stake or interest in the cyber mission. With fewer interests vying for the cyber mission, there was no need to alter the existing branch model under the Staff and Signals Battalion.

Hypothesis 4 also receives support from both quantitative and qualitative analysis. Simulations from Chapter 4 show that after roughly 15 years of occupying the Introduction stage, large militaries are much more likely to transition into Expansion than smaller militaries.

The case studies also provide evidence that size influenced expansion. As a larger organization, the U.S. was able to marshal the resources needed to expand the joint-force approach; an important dimension was dual-hatting the commander of U.S. Cyber Command as the Director of the National Security Agency. By formally merging authority, the military was able to access the NSA's human and technological capital to create USCYBERCOM. The Estonian Defense Forces had no such existing resource pool to access, and efforts to develop human capital were focused on building latent military capacity in the reserves. As such, transitioning to Expansion made no sense for the EDF given resource constraints, and debates focused on potential unified force structures.

Hypothesis 5 predicts that larger militaries are more likely to transition into Full Implementation than smaller militaries. This hypothesis receives no support from quantitative analysis. The multistate model in Chapter 4 shows that larger militaries are no more likely than smaller militaries to transition from Introduction to Full Implementation, and smaller militaries are actually more likely to transition from Pre-Adoption to Full Implementation than large militaries over time. Qualitative analysis provides qualified support for this hypothesis. Both the U.S. and Estonia reached Full Implementation by creating a unified cyber force structure, and the justification for both transitions rested on "proof of concept" that linked the operational effects of computer network operations to common strategic interests across the military. However, the proof of concept for U.S. Cyber Command—Operation Glowing Symphony—came in the form of an offensive operation. For Estonia, proof of concept came from defensive operations during the 2007 network attacks, prior to the formation of any cyber force. Although proof of concept drove Full Implementation in both militaries, size limited the circumstances under which proof of concept could occur. As a more loosely coupled organization, effective proof of concept in the

U.S. needed to be proximate and direct: the impacts of Operation Glowing Symphony bore directly on the operations conducted in conjunction with other military commands. In the case of Estonia, proof of concept was temporally distanced from the creation of EDF Cyber Command. However, the tighter coupling of the Estonian Defense Forces meant that the temporally distant proof of concept could be linked to existing strategic interests through trust and personal connections. As such, the cases studies provide qualified support for Hypothesis 5.

From the quantitative and qualitative analyses carried out in this dissertation, two distinct implementation pathways emerge. For the U.S., a large military, implementing cyber forces required prioritizing bureaucratic fit over developing the cyber mission: organizational redundancy meant that multiple competing interests had to be satisfied before dedicating greater resources to the cyber mission. Moreover, changes to cyber force structure occurred incrementally, and reaching a unified joint command rested on providing direct proof of concept to other military commands. In the case of Estonia, a small military, implementers were able to prioritize building organizational capacity to carry out the cyber mission. With no competition over the cyber mission, implementers could focus more on creating an effective organization that justified the strain on existing resources. Consolidation emerged as a solution to resource constraints, and the creation of the EDF Cyber Command relied on trust and personal relationships to link proof of concept to existing strategic interests. As such, several conceptual steps of the implementation process were bypassed.

Alternative Explanations

In each case study, assessments of both the adoption-capacity and organizational culture explanations highlight the importance of theorizing organizational size. The ultimately incomplete account provided by each alternative explanation shows that while organizational size is not the only (or even the most important) variable, the implementation of cyber forces cannot be explained without considering the effects of organizational size.

Adoption-capacity provides a consistent and compelling explanation for the case of Estonia. The evidence surrounding the delegation of cyber responsibilities to the Staff and Signals Battalion, the selection of a unified branch force structure, and the timing of Cyber Command's establishment provides support for adoption capacity. However, on its own, the adoption-capacity explanation struggles to account for several events covered in the case study of the United States. Adoption-capacity does provide some insight into the introduction and modification of Joint Task Force – Computer Network Defense, but it receives no support from the evidence in the rest of the case. Adoption-capacity cannot adequately explain the failure of Air Force Cyber Command (Provisional), the initial selection of a sub-unified joint force structure for U.S. Cyber Command, the non-elevation of USCYBERCOM between 2012 and 2013, or the subsequent elevation in 2018. As such, the combined insights from both the U.S. and Estonian cases show the complementary and contingent nature of adoption-capacity and the theory of organizational size. Both cases suggest that size is an important enabling and constraining factor and that adoption-capacity dynamics may take on greater causal priority in smaller organizations than in larger organizations. Even so, organizational culture still exhibits independent effects on the implementation process.

Evaluating military organizational culture as an explanation across each case also evidences the need to consider organizational size. Cultural logics receive strong support in the U.S. case from the evidence relating to the introduction and modification of JTF-CND and the initial force structure selection for USCYBERCOM. However, an account based solely on organization culture only weakly explains the failure of AFCYBER(P) and struggles to explain much of the rest of the U.S. case. In the case of Estonia, the cultural explanation receives weak support from evidence surrounding the delegation of the cyber mission to the Staff and Signals Battalion. The evidence does not support a cultural explanation of the selection of organizational model and the timing of Cyber Command's creation. As with adoption-capacity, explanations resting on organizational culture show that size is an important variable that has the potential to shape when and how organizational cultural factors matter.

Implications for the Study of the Diffusion of Military Innovations

In addition to the contributions to the literature on cyber conflict, this argument and its supporting evidence make three contributions to studies of the diffusion of military innovations. First, it shows how organizational characteristics mitigate diffusion pressures by constraining or enabling innovation and implementation. In this study, military size played an important role in shaping not only the initial decisions to adopt a cyber force but also the intermediate decisions over modification and expansion and the decision to implement a unified command. As a result, size influenced the range of choices faced by implementers. The analysis in this dissertation suggests that the structural characteristics of military organizations—such as size—can influence the types of changes and innovation likely to occur.

Second, this dissertation advances a stage-based framework for theorizing the adoption of an international innovation by incorporating implementation dynamics. The framework characterizes adoption and implementation as a dynamic process comprised of five stages: pre-adoption, introduction, modification, expansion, and full implementation. As such, this framework can account for the ways in which innovations change throughout diffusion processes. When innovations diffuse as concrete models, variations occur as militaries introduce the innovation into their particular ecosystems: select components or instruments of the innovation can be introduced or the innovation can be reinvented altogether. Conversely, when innovations diffuse as broader principles—as is the case with cyber forces—implementers enjoy a greater range of agency. This framework is able to capture the ways in which innovations can and do change in distinct ways after adoption during implementation. Stage-based theorizing can also provide unique insight into the emergence of competing innovation models over time in the international system. The same factor that influences adoption may exert a different effect on implementation decisions. As leading states change an innovation model during implementation, another model can emerge for laggards to adopt.

Third, this dissertation emphasizes the importance of matching the appropriate methods to stage-based theorizing. Specifically, I introduce multistate survival modeling to assess the stage-specific effects of organizational size. Multistate models provide a flexible option for statistically modeling the likelihood of transitioning between stages over time. It also allows for covariate effects to vary according to transition; this is particularly important for testing hypotheses related to both adoption and implementation.

Extensions of the Study

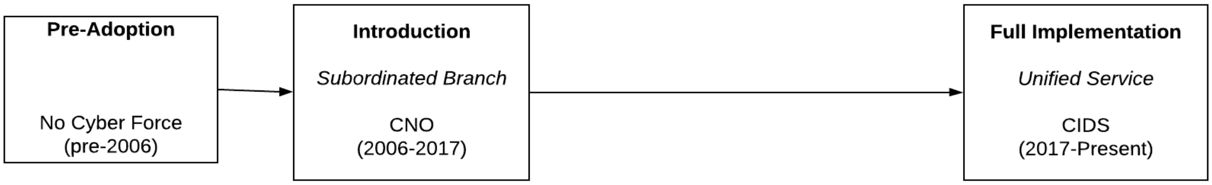
There are two major extensions to this dissertation that merit discussion. The first is the inclusion of additional case studies to assess the implementation of cyber forces in other militaries. The second extension of this study entails examining the adoption and implementation of other innovations. This section provides a brief discussion of both extensions.

Extending Qualitative Analysis: A Preliminary Assessment of Germany's Cyber Force Structure

The German military—the Bundeswehr—provides an exemplar of a non-extreme case of a medium-sized military. The Bundeswehr has averaged roughly 182,000 active duty personnel from 2011 to 2017: much larger than the Estonian Defense Forces (approximately 6,000) yet much smaller than the United States military (approximately 1.5 million) during this period.[1] In fact, the Bundeswehr represents the statistical mean of military size in terms of personnel in the Dataset on Cyber Force Structures. As such, it presents an important extension of my theory of organizational size to assess the operational-bureaucratic tradeoff during implementation.

Figure 7.1 shows the development of Germany's cyber force structure according to implementation stage, force structure, and the specific military institution. Germany created its first cyber force in December of 2006 as a subordinated branch. The Department of Computer Network Operations (CNO), established under the Strategic Reconnaissance Command of the Joint Support Service, was tasked with conducting cyber operations for military intelligence purposes. In April 2017, the Bundeswehr completed a major consolidation of its existing cyber efforts with the creation of the Cyber and Information Domain Service (CIDS).[2]

Figure 7.1. The Development of Germany's Cyber Force Structure: Implementation Stage, Force Structure, and Institution.



[1] The World Bank, "World Development Indicators."

[2] Bundeswehr, "Organisation: Kommando Streitkraftebasis," n.d., https://www.bundeswehr.de/de/organisation/streitkraeftebasis; Bundeswehr, "Organisation: Kommando Cyber- Und Informationsraum," n.d., https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum#Z7_694IG2S0MG6200ANOPUS4Q2021; Von John Goetz, Marcel Rosenbach, and Alexander Szandar, "National Defense in Cyberspace," *Der Spiegel*, February 11, 2009, https://www.spiegel.de/international/germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html; Isabel Skierka, "Bundeswehr: Cyber Security, the German Way," *Observer Research Fourndation*, October 20, 2016, https://www.orfonline.org/expert-speak/bundeswehr-cyber-security-the-german-way/.

This brief overview of Germany examines the factors behind the creation of the Cyber and Information Domain Service as a new unified service in the Bundeswehr.

The Impetus for Change and Proof of Concept. Preliminary evidence indicates that the 2013 Snowden leaks prompted an initial reconsideration of the Bundeswehr's cyber capabilities. For leadership of the Strategic Reconnaissance Command, the Snowden leaks revealed a major gap between German and U.S. capabilities related to signals intelligence and cyberspace. For leadership in the Ministry of Defense, the strategic importance of cyber capabilities was solidified by the 2014 Russian invasion in Crimea.[3] However, no serious consideration was given to changing the Bundeswehr's cyber force structure until 2015.

Two events would align civilian leadership in parliament (the Bundestag) and the Ministry of Defense with military leadership in the Bundeswehr to pursue reorganization. The first was the May 2015 compromise of Bundestag networks. Russian-based hackers had infiltrated Bundestag networks and attempted to install software on the computers of staff and members of parliament; this software would have provided hackers with permanent access to these computers for intelligence collection. Subsequent forensics would link the hacking group to the Russian government.[4] Similar to the case of Estonia, this spurred a reconsideration of government-wide initiatives related to cyberspace. However, the Bundestag compromise did not act as the proof of concept for military purposes. The Department of Computer Network Operations would provide proof of concept in 2015. Similar to the U.S. case, the CNO Department conducted an offensive operation, attacking Afghan mobile networks as part of the

[3] U.S. Army Major embedded in German Cyber and Information Domain Service interview with author, interview by Jason Blessing, telephone, August 20, 2019.

[4] "Russia 'Was Behind German Parliament Hack,'" *BBC News*, May 13, 2016, https://www.bbc.com/news/technology-36284447.

effort to release a German citizen kidnapped in Afghanistan.[5] Following these events, on September 17, 2015, Defense Minister Ursula von der Leyen ordered the establishment of a new cyber department within the Ministry and stated the intention to create a new organization within the Bundeswehr for the cyber domain.[6]

Resources, Interests, and New Force Structure. The stand-up of both the new cyber agency and a new military organization occurred concurrently: Minister von der Leyen delivered the order to officially set up the Ministry's new cyber agency on November 1, 2015, and a separate committee for the military initiative held its first round table on November 2. More formalized instructions were given to the committee on November 11; and on November 23, 2015, the steering committee officially began to work towards the creation of a new command by surveying the existing strategic landscape, cataloguing existing units, personnel, and deficiencies across the Bundeswehr, and developing justifications and responsibilities for a new organization.[7] The steering committee's final stage of analysis lasted through the end of 2015 and into early 2016. This stage included defining the factors and criteria for measuring the successful stand-up of a new command. Notably, the steering committee consulted extensively with experts in Silicon Valley and military personnel from both the U.S. and Israel.[8]

Debates over force structures emphasized both the need to elevate cyber operations to a higher level and the need to consolidate the Bundeswehr's existing piecemeal approach to the

[5] Justyna Gotkowska, "The Cyber and Information Space: A New Formation in the Bundeswehr" (Osrodek Studiow Wschodnich, April 12, 2017), https://www.osw.waw.pl/en/publikacje/analyses/2017-04-12/cyber-and-information-space-a-new-formation-bundeswehr; U.S. Army Major embedded in German Cyber and Information Domain Service interview with author.

[6] Ursula von der Leyen, "Tagesbefehl [Daily Command]," September 7, 2015.

[7] German Ministry of Defense, "Abschlussbericht Aufbaustab Cyber- Und Infromationsraum [Final Report from the Cyber and Information Domain Steering Committee]" (Berlin, Germany, April 2016), 9, http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf.

[8] German Ministry of Defense, "Abschlussbericht Aufbaustab Cyber- Und Infromationsraum [Final Report from the Cyber and Information Domain Steering Committee]," 11–42.

cyber domain. Strategic Reconnaissance Command was headed by a two-star general; elevating the issue and attracting more resources required a four-star general. At the same time, the CNO Department was the main organization for conducting computer network operations, the German Army, Navy, and Air Force each had their own cyber and information technology-focused units. Like the U.S., the Bundeswehr exhibited a certain degree of redundancy: each service had a stake in the cyber mission. However, the size of the Bundeswehr also limited competition over the cyber mission. Unlike special forces in the Bundeswehr, only a marginal number of service personnel staffed cyber/IT units; each service's stake in the cyber mission was low. [9] Most personnel resided in the Joint Support Service, and in total, the Bundeswehr had roughly 14,500 active personnel available for reorganization.[10]. As such, a joint-service arrangement was not necessary to coordinate combat service initiatives. Instead, an independent service construct emerged as the primary organizational model for cyber force structure. In this sense, the Joint Support Service acted as an important precedent for consolidating talent that supported combat operations.[11]

The committee released its final report on organizing a new service on April 25, 2016, roughly one week after Minister von der Leyen approved strategic guidance for the Ministry's cyber agency.[12] On the heels of the report, Minister von der Leyen publicly announced the plan to create a new service in the Bundeswehr.[13] Part of the motivation to announce the Bundeswehr's reorganization in late April related to NATO's pending recognition of the cyber

[9] U.S. Army Major embedded in German Cyber and Information Domain Service interview with author.

[10] Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr," *Connections: The Quarterly Journal* 19, no. 1 (2020): 13.

[11] On the creation of the Joint Support Service, see: Manfred Engelhardt, "Jointness in the Bundeswehr," in *German Defence Politics*, ed. Ira Wiesner, 1st ed., vol. 30, Bundeswehr Academy for Information and Communication Series (Germany: Nomos, 2013), 163–80.

[12] German Ministry of Defense, "Abschlussbericht Aufbaustab Cyber- Und Infromationsraum [Final Report from the Cyber and Information Domain Steering Committee]," 11.

[13] Skierka, "Bundeswehr: Cyber Security, the German Way."

domain. On one hand, Chancellor Merkel and Minister von der Leyen wanted Germany to be a leading state within NATO regarding cyber issues. On the other hand, German leadership wanted to be seen as a military innovator within the EU; announcing the intent to create a cyber service prior to NATO's domain recognition would lend credibility to the Bundeswehr.[14] After NATO's June 2016 recognition, Germany released its own formalized strategic views on cyberspace with its July 2016 White Paper and the subsequent 2016 *National Cyber Security Strategy*. The White Paper devoted significant attention to the cyber domain in the context of the military.[15] By April of 2017, the Cyber and Information Domain Service reached initial operating capability.[16]

Analysis in Brief. This brief discussion provides support for extending the theory of organizational size to additional cases. The Bundeswehr has had more resources available at its disposal than the Estonian Defense Forces and exhibited more redundancy in the cyber mission across the services than the EDF. However, the Bundeswehr lacks a resource base comparable to that of the United States: the Bundeswehr has been frequently cited as a military facing constant political and resource constraints.[17] As such, the theory of organizational size predicts a less severe tradeoff between bureaucratic integration and building operational effectiveness.

[14] U.S. Army Major embedded in German Cyber and Information Domain Service interview with author.

[15] The Federal Government of Germany, "White Paper 2016 on German Security Policy and the Future of the Bundeswehr" (The Federal Government of Germany, July 13, 2016), https://www.dsn.gob.es/sites/dsn/files/2016_German_WhitePaper_SecurityPolicy_13jul2016.pdf.

[16] For an overview of each of the CIDS subordinate units and their responsibilities, see: Deutscher Bundestag, "Antwort Der Bundesregierung: Auf Die Kleine Anfrage Der Abgeordneten Sevim Dağdelen, Christine Buchholz, Annette Groth, Weiterer Abgeordneter Und Der Fraktion DIE LINKE – Drucksache 18/11688 – Strukturen Des Organisationsbereichs Cyber- Und Informationsraum Der Bundeswehr in Nordrhein-Westfalen [Answer from the Federal Governmetn to the Request from Sevim Dagdelen, Christine Buchholz, Annette Groth, Another MP, and the DIE LINKE Parliamentary Group in Drucksache 18/11668 on the Organizational Structures of the Cyber and Information Domain Service of the Bundeswehr in North Rhine-Westpahilia," Printed Matter (Berlin, Germany, May 9, 2017), http://dipbt.bundestag.de/doc/btd/18/122/1812277.pdf.

[17] Tom Dyson, *The Politics of German Defence and Security: Policy Leadership and Military Reform in the Post-Cold War Era* (New York: Berghahn Books, 2007); Dyson, "Convergence and Divergence in Post-Cold War British, French, and German Military Reforms: Between International Structure and Executive Autonomy"; Tom Dyson, "The Challenge of Creating an Adaptive Bundeswehr," *German Politics*, 2019, 1–18; Tom Dyson, "Unpacking Military Emulation: Absorptive Capacity and German Counterinsurgency Doctrine during ISAF," *European Security* 29, no. 1 (2020): 33–54.

Although each service had a presence in the cyber domain, resources in the Bundeswehr appear to be more tightly coupled across the military than in the U.S. military. The services thus remained focused on their primary missions and retained relatively low interest in the cyber mission. The service presence in the cyber domain also provided more personnel for consolidation than the case of Estonia. As a result, service footprints in the cyber domain led to a reconsideration of the organizational model, but a lack of considerable competition among the services enabled a transition into a unified cyber force structure. Moreover, the recent experience of creating the Joint Support Service served as a useful model for bureaucratic integration. These dynamics, coupled with a pool of cyber personnel across the Bundeswehr, enabled implementers to pursue and independent service structure.

Application to Other Military Innovations

The conceptual typology and framework advanced in this dissertation can also be extended to assess the diffusion and implementation of military innovations other than cyber forces. Two examples serve to illustrate the utility of the framework. The spread of air forces provides a natural extension. Although most states have eventually developed an independent service, many air forces initially emerged subordinated to another combat service.[18] The French case illustrates this dynamic. France introduced its first major air branch—the Aeronautics Service (Service Aéronautique)—in 1909 as a unit under the French Army. In 1922, the Aeronautics Service was expanded to a Major Command within the Army; by 1934, France had elevated this command to an independent air force as a unified service.[19]

[18] James Hasik, "Mimetic and Normative Isomorphism in the Establishment and Maintenance of Independent Air Forces," *Defense & Security Analysis* 32, no. 3 (2016): 256–63.

[19] Pascal Vennesson, "Institution and Airpower: The Making of the French Air Force," *Journal of Strategic Studies* 18, no. 1 (1995): 36–67.

The development of special operations forces across militaries provides another example. In Norway, special operations forces were consolidated in 2014 into the Norwegian Special Operations Forces Command (NORSOF), a standalone branch apart from other service structures. Prior to 2014, both the Army and Navy had their own respective special forces commands: the Armed Forces Special Command (FSK) under the Army, active since at least 1982; and the Navy Special Operations Command (MJK), active first as the Frogmen unit under the Navy in 1953 and later as the major command post-1968.[20] Norway's special forces force structure has thus progressed as follows: no force pre-1953; a subordinated service force structure from 1953 to 1982; a subordinated joint service arrangement of *ad hoc* interservice coordination from 1982 to 2014; and a unified branch from 2014 to the present. Similar force structure developments have occurred in other countries such as Poland[21] and Estonia.[22] Figure 7.2 visually summarizes the extension of my framework to the French air force structure and Norway's special operations force structure.

It remains to be seen whether my theory of organizational size is also generalizable to other innovative military restructurings. However, anecdotal evidence provides initial support for the theory's generalizability. For example, the formation of U.S. Strategic Command (USSTRATCOM) in 1991 to control strategic nuclear forces was partially a product of clashes between the U.S. Air Force and the U.S. Navy over service-level preferences. Starting in 1946, U.S. air forces (initially the Army Air Force and then the subsequent U.S. Air Force) had advocated for a single, unified command to control all nuclear forces. Navy leadership refused to

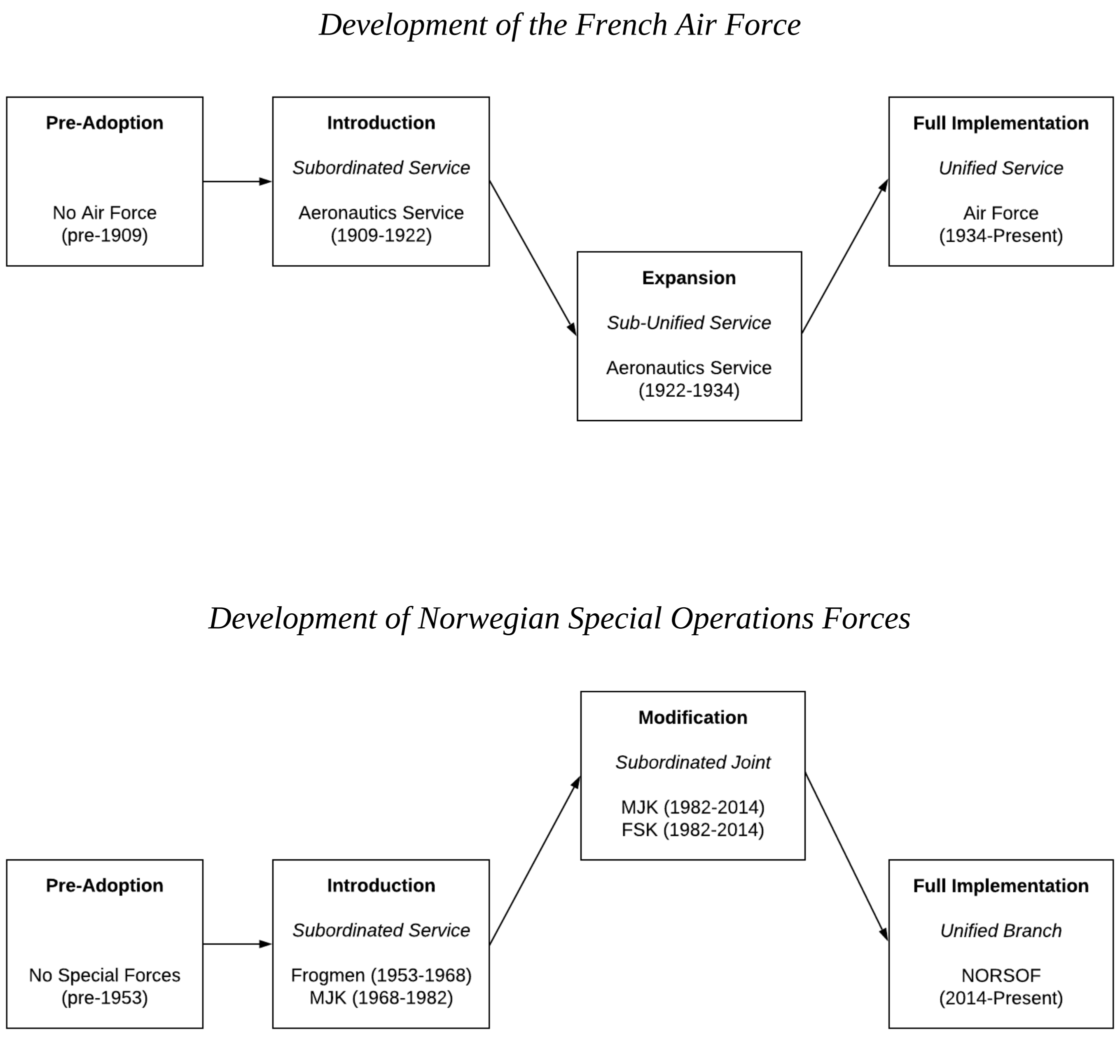
[20] Tommy Olsen and Marius Thormodsen, "Forging Norwegian Special Operation Forces" (Monterey, California, Naval Postgraduate School, 2014); Petter Hellesen, "Counterinsurgency and Its Implications for the Norwegian Special Operations Forces" (Naval Postgraduate School, 2008), 53–56

[21] Kjetil Mellingen, "Strategic Utilization of Norwegian Special Operations Forces" (Monterey, California, Naval Postgraduate School, 2010), 88.

[22] Rene Toomse, "Small States' Special Operations Forces in Preemptive Strategic Development Operations: Proposed Doctrine for Estonian Special Operations Forces," *Special Operations Journal* 1, no. 1 (2015): 44–61.

allow their forces to be absorbed by another service, arguing that nuclear-equipped submarines must coordinate with other naval forces and should therefore remain under the control of the Navy. Despite compromises made in 1960 to create the Joint Strategic Target Planning Staff, the Air Force and Navy retained independent control over their respective nuclear forces.

Figure 7.2. Extensions of the Framework and Typology to Additional Military Innovations



Development of the French Air Force

Development of Norwegian Special Operations Forces

A joint, unified command only became possible with the emergence of arms control agreements and the end of the Cold War: service parochialism declined as the strategic nuclear arsenal became less important.[23] Even after its creation, USSTRATCOM struggled with adequate staffing and the coordination and interoperability of service components due to interservice tensions.[24] The example of USSTRATCOM lends initial support to the theorized dynamics of large militaries. Returning the example of Norwegian Special Forces provides additional support for the theory's application to other innovations. Existing accounts suggest that, while mergers of the Armed Forces Special Command (FSK) and the Navy Special Operations Command (MJK) had been discussed since the late 1990s, reorganizations failed due to differing mission definitions. The main conflicts occurred between these respective commands, not between the larger services. The separate operations of the two commands represented an inefficient use of resources, particularly during deployments in Afghanistan. The consolidation of these two commands under a new branch was seen as a way to increase both readiness and combat power, thereby reducing the strain on military resources.[25] These dynamics mirror the developments of Estonia's cyber force structure and offer anecdotal support for extending the theory of organizational size to other military innovations.

Limitations of this Dissertation

Although this dissertation makes substantial contributions to both the cyber conflict literature and the literature on military diffusion, the present study has several limitations. First, although the quantitative analysis in Chapter 4 spans both democratic and non-democratic regimes, the

[23] Drea et al., "History of the Unified Command Plan: 1946-2012," 2–3, 64–65.
[24] United States Government Accountability Office, "Military Transformation: Additional Actions Needed by U.S. Strategic Command to Strengthen Implementation of Its Many Missions and New Organization," Report to the Subcommittee on Strategic Forces, Committee on Armed Services, House of Representatives (Washington, D.C.: U.S. GAO, September 2006).
[25] Olsen and Thormodsen, "Forging Norwegian Special Operation Forces," 15–20.

case studies focus only on democratic, NATO-member states. As a result, qualitative analysis only explores causal mechanisms in the context of democratic states. Recent analysis on Russian cyber force structure appears to support the generalizability of the theory of organizational size. The size of the Russian military has enabled both the Main Intelligence Directorate (GRU) and the Federal Security Service (FSB) to develop relatively independent and redundant capabilities. Moreover, competition between these two camps has prevented changes to cyber force structure. This appears to provide support for this dissertation's claim that large organizations must prioritize bureaucratic integration—i.e. reconciling any new force structure initiatives with GRU and FSB interests—before creating new or elevating existing cyber forces.[26] At the same time, the case of China presents a challenge for my theoretical claims. As one of the largest militaries in the world, the Chinese People's Liberation Army (PLA) underwent sweeping reforms in 2016; as part of these reforms, cyber and information-related efforts from across the military were consolidated under the new Strategic Support Force. This unified service replaced the previous cyber force structure under the General Staff Fourth Department (4/PLA), the military intelligence department of the PLA. As such, the theoretical framework advanced in this dissertation must be extended to assess implementation in non-democratic contexts.

Second, the case studies in this dissertation limit analysis to NATO member countries. As such, my theory of organizational size may be of limited applicability to militaries in democratic states outside of NATO. The development of Brazil's cyber force structure does provide some credibility to the framework outside of NATO: cyber force structure has been limited to subordinated and sub-unified service structures under the Army. The initial cyber force was

[26] Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in *20/20 Vision: The Next Decade*, ed. T. Jancarkova et al. (2020 12th International Conference on Cyber Conflict, Tallinn, Estonia: NATO CCD COE Publications, 2020), 129–55.

introduced in late 2008 in response to internal assessments instead of external imperatives, lending support to claims of risk tolerance in large militaries. Moreover, the most recent arrangement, Defense Cyber Command, integrates capabilities across the services but remains under the Army chain of command.[27] Any expansion would require a modification in organizational model to a formal joint-service structure. However, the case of Israel raises concern about how well the theory travels. Despite being a small military, the failure of a proposed merger between Unit 8200 (the military intelligence unit traditionally responsible for cyber operations) and the Command, Control, Communications, Computers, and Intelligence (C4I) Directorate of the Israeli Defense Forces exhibited implementation dynamics predicted for larger militaries. The merger failed because both stakeholders had entrenched interests and were unwilling to compromise over the new force structure. As such, preliminary case details suggest that successful initiatives for cyber force structure must account for bureaucratic integration prior to developing greater operational capacity.[28] This too merits an exploration of the framework's generalizability.

Two final caveats are in order. This project does not explicitly address *why* militaries pursue cyber forces. An assessment of motivation lies outside the scope of this study. Instead, this dissertation assumes that, when given the opportunity, states will attempt to implement cyber forces. This may account for the potential complementary nature between my theory and adoption-capacity: adoption-capacity can provide a foundation for pursuit based on competition, while my theory of organizational size explicates and refines implementation hurdles. Finally,

[27] Brazilian Air Force, "Oficiais-Generais de Aeronautica e Da Marinha Assumem Cargo No Exercito [General Officers of the Air Force and Navy Assume Positions under the Army]," April 25, 2017, https://www.fab.mil.br/noticias/mostra/29951/INTEROPERABILIDADE%20-%20Oficiais-Generais%20da%20Aeron%C3%A1utica%20e%20da%20Marinha%20assumem%20cargo%20no%20Ex%C3%A9rcito.

[28] "IDF Scraps Plans for a Unified Cyber Command," *Israel Defense*, May 15, 2017, https://www.israeldefense.co.il/en/node/29613.

the Dataset on Cyber Force Structures used for quantitative analysis in this dissertation only covers a 19-year time frame. As more data become available in the coming years, this dataset should be expanded and used for continued assessment of variation in institutional structures. While current trends indicate that institutional isomorphism and the emergence of a dominant force structure model appear unlikely, more data must be collected to test these conjectures.

Directions for Future Research

This dissertation provides a conceptual and theoretical springboard for future investigations into cyber forces and cyber force structures. Three directions appear fruitful for future research. First and foremost, the theoretical explanation advanced in this dissertation must be evaluated with evidence from other cases. Although my theoretical framework provides important insight into two democratic NATO-member states, further research is needed to evaluate whether this theory travels to (1) non-NATO states and (2) non-democratic states.

Second, future work should examine the effect of force structure on the behavior of cyber forces. Existing studies on cyber conflict have not yet explored the structural dimensions of behavior. As one recent review of the literature has highlighted: "[f]ew articles—if any—focus on how organizational structure…causes certain outcomes in cyber conflict."[29] On one hand, cyber force structure can shed light on how states approach the cyber domain and conceptualize the co-deployment of computer network operations with kinetic force in battlefield settings.[30] On the other hand, the new military structures hold strong implications for conflict escalation

[29] Gorwa and Smeets, "Cyber Conflict in Political Science: A Review of Methods and Literature."

[30] On Russian integration with kinetic operations in Ukraine, see: Kostyuk and Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?"

between states.[31] The study of cyber force structures is a crucial missing link in arguments about cyber-arms racing[32] and strategy and self-restraint among states in cyberspace.[33]

Finally, future research should look to theorize how cyber forces coordinate with their civilian intelligence counterparts. Structural arrangements—such as force structure—are bound to play an important role in determining operational and strategic responsibilities; the dual-hat arrangement between U.S. Cyber Command and the National Security Agency provides a clear example of a relationship bound by force structure. Yet, while this dissertation serves to identify the key stakeholders for cyber force implementation, it remains silent as to the types of cooperation likely to emerge between the military and civilian intelligence agencies. Subsequent work must therefore investigate this issue.

Broader Academic Implications

This dissertation holds three broader implications for international security scholars. First, this project provides a much-overlooked institutional dimension for scholars focused on military revolutions—specifically, the Information Technology Revolution in Military Affairs (IT-RMA). While cyber forces in and of themselves do not constitute a military revolution, the spread of cyber forces certainly reflects the integration of information technologies into military operations and structures with which IT-RMA scholars are concerned.[34] Most analyses and commentary on

[31] Timothy J. Junio, "The Politics and Strategy of Cyber Conflict" (Dissertation, Philadelphia, University of Pennsylvania, 2013); Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca and London: Cornell University Press, 1984), 15–16.

[32] Craig and Valeriano, "Conceptualising Cyber Arms Races"; Craig and Valeriano, "Reacting to Cyber Threats: Protection and Security in the Digital Age."

[33] Maness and Valeriano, "The Impact of Cyber Conflict on International Interactions"; Jacob Mauslein, "Three Essays on International Cyber Threats: Target Nation Characteristics, International Rivalry, and Asymmetric Information Exchange" (Dissertation, Manhattan, KS, Kansas State University, 2014); Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51, no. 3 (2014): 347–60; Valeriano and Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*.

[34] See, for example: Emily O. Goldman and Thomas G. Mahnken, eds., *The Information Revolution in Military Affairs in Asia* (New York and London: Palgrave MacMillan, 2004); Dima Adamsky and Kjell Inge Bjerga, "Introduction to the Information-Technology Revolution in Military Affairs," *Journal of Strategic Studies* 33, no. 4

military revolutions have tended to focus on the technological dimensions at the expense of organizational dynamics and personnel issues.[35] The typology and framework advanced in this dissertation provide one approach for deriving indicators to assess the evolution of IT-RMA elements as states implement innovations into their own military organizations.

Second, this dissertation carries implications for studying how states respond to emerging technological threats and opportunities. Examining how states to create military institutions for cyber-security is vital for understanding how states react to rapidly evolving technologies and ultimately transform the international environment. On one hand, this dissertation pushes back against claims of institutional isomorphism:[36] although militaries may emulate the practices of others, emulation does not require the creation of identical institutional arrangements. In the case of cyber forces, evidence from both quantitative and qualitative analysis in this dissertation shows that militaries can utilize the same innovation principle but implement qualitatively different force structures. On the other hand, the lack of institutional homogeneity sheds light on the ways in which states and their militaries shape technology through institutionalization and, in doing so, reshape the nature of interactions between states over time.[37]

Finally, by studying how military organizations change, this study can contribute to ongoing discussions about the nature of institutional reproduction and change over time. Evidence from both case studies show an interplay between functionalist and power-distribution

(2010): 463–68; Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*.

[35] Eliot A. Cohen, "Change and Transformation in Military Affairs," *Journal of Strategic Studies* 27, no. 3 (2004): 395–407.

[36] For a discussion on the dynamics of isomorphism. Paul J. DiMaggio and Walter W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* 48, no. 2 (1983): 147–60.

[37] For a comprehensive look at how international dynamics can be reshaped, see: Herrera, *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*.

mechanisms of institutional reproduction and change.[38] The dissertation has argued that the creation and persistence of cyber forces are driven by the tension between emerging functional needs for militaries (the operational imperative) and the distribution of power and preferences among military stakeholders (the bureaucratic imperative). Therefore, decisions over initial cyber force structures made at critical junctures—those short periods of time where actors choices can affect and subsequently restrict the range of future decisions through path dependence[39]—are not completely self-reinforcing and may "lock in" the range of potential force structures in the future in only a limited way.[40] Instead, military size provides the broader context against which military sub-organizations, such as cyber forces, are reproduced through the interactions of changing strategic environments and prevailing internal interests.

At the same time, the analysis advanced in this dissertation suggests that, because of the interplay between functional needs and power-distributional concerns in militaries, neither functionalist nor power distributional explanations provide a compelling logic of institutional change. The evidence from the cases studies thus appear to support accounts of institutional change that rest on "layering" and "conversion." In short, this dissertation's findings suggest that innovation and implementation in large militaries are more likely to reflect a process of institutional layering, while innovation and implementation in smaller militaries are likely to resemble institutional conversion. Institutional layering involves the creation and negotiation of new institutional arrangements on top of preexisting structures.[41] This is seen clearly in the U.S.

[38] For an overview of these two competing causal accounts, see: James Mahoney, "Path Dependence in Historical Sociology," *Theory and Society* 29 (2000): 516; Kathleen Thelen, "How Institutions Evolve: Insights from Comparative Historical Analysis," in *Comparative Historical Analysis in the Social Sciences*, ed. James Mahoney and Dietrich Rueschemeyer (Cambridge University Press, 2003), 214–22.

[39] Giovanni Capoccia and R. Daniel Kelemen, "The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism," *World Politics* 59, no. 3 (April 2007): 348.

[40] On the self-reinforcement processes of institutions, see: Mahoney, "Path Dependence in Historical Sociology," 512–26.

[41] Thelen, "How Institutions Evolve: Insights from Comparative Historical Analysis," 226–28.

case: functional imperatives incentivized the development of cyber forces, but existing service claims over the cyber mission acted as constraints. The subsequent deliberations over and changes in force structure reflected layering: over time, the scale of command for U.S. Cyber Command was renegotiated to a unified command, but this occurred within a joint-service framework to preserve existing service-interest structure. Conversely, institutional conversion entails the redirection of existing institutions to take on new roles or functions.[42] This process appears to have occurred in the case of Estonia. Unlike the U.S. the combat services of the Estonian Defense Forces had no real interest in retaining the cyber mission; however, a limited resource base restricted implementation prospects. Thus, the EDF repurposed existing efforts via consolidation instead of layering: cyber units and personnel were removed from the services and merged with the Staff and Signals Battalion to create a new cyber force structure.

Policy Implications

Several policy implications flow from this dissertation's analysis of cyber force implementation. First, the typology of cyber force structures advanced in this dissertation is an important step towards identifying jurisdictional and operational overlaps and fault lines among cyber force stakeholders.[43] When left unaddressed, bureaucratic overlaps—between military elements, but also between the military and civilian intelligence agencies—can lead to two problems. On one hand, the elevation of cyber forces can alter distributional relationships; this can spur competition over defense budgets both within the military and in relation to civilian intelligence. Competition between cyber forces and intelligence agencies carries several implications for strategic efforts in the cyber domain. In-fighting risks conflict escalation through subpar strategic

[42] Thelen, 228–30.

[43] On the impact of bureaucratic overlap on the formulation and effectiveness of defense policy, see: B. J. Archuleta, "Rediscovering Defense Policy: A Public Policy Call to Arms," *Policy Studies Journal* 44, no. 1 (2016): S66.

assessment and coordination result from: inefficient resource usages; duplicated efforts; the lack of a common definition of security; and the withholding of information to control over decision processes.[44] On the other hand, the strategic elevation of cyber forces brings to the forefront tensions between network exploitation and network attack. In the case of the U.S., the civilian National Security Agency emphasizes exploitation for intelligence collection, while USCYBERCOM is geared more towards achieving effects through network attack. The U.S. dual-hat arrangement has been an attempt to alleviate this tension. Where commanders are not given discretion to determine the tradeoff, military commanders may be more willing to accept escalatory risks to show competency. In a domain of relatively ambiguous signaling dynamics,[45] this spells trouble for conflict escalation.

A second set of policy consequences arises for NATO. The creation of cyber forces among member states may be an attempt to close the ongoing gap in military transformation.[46] Evidence from the Estonian case study—and the preliminary extension to Germany in this chapter—suggests that the alliance can function to reduce the political costs of creating and implementing cyber forces. In both instances, consultation with NATO allies provided additional information regarding the relative payoff of organizational models and the strategic dimensions of the cyber domain. The creation of cyber forces across the alliance will certainly help to formalize and facilitate interoperability and intelligence-sharing (to a certain degree) in the cyber domain. Consultation also provides the opportunity for leading alliance members, such as the U.S., to help shape allied doctrine.[47]

[44] On how these elements play out in traditional military domains, see: Risa Brooks, *Shaping Strategy: The Civil-Military Politics of Strategic Assessment* (Princeton, New Jersey: Princeton University Press, 2008).

[45] Valeriano, Jensen, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*.

[46] On the gap in military innovation in NATO, see: Terriff, Osinga, and Farrell, *A Transformation Gap? American Innovations and European Military Change*.

[47] On the role of norms in shaping doctrine, see: Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies and Norms in U.S. Cyberwar Doctrine," *Journal of Cybersecurity* 3, no. 1 (2017): 7–17.

However, the worldwide development of cyber forces leads to a third, more discouraging implication. While institutional isomorphism may not occur in relation to cyber forces, that does not preclude the emulation of practices in the cyber domain.[48] In this regard, U.S. Cyber Command's "defend forward" strategy and its operational construct of "persistent engagement" have set a troublesome precedent. As a fairly overt statement of USCYBERCOM's intent to operate in the "grey zone" of cyberspace to protect "blue zones" (i.e., your own networks), the strategy reveals a contradiction: there is no grey zone. As soon as you leave your own networks, you are entering into someone else's network.[49] The issue then becomes: as other cyber forces develop greater capabilities, who will be the next to "defend forward"? Should behavioral practices follow the institutional patterns identified in this dissertation, both allies and adversaries of the U.S. should be expected to develop their own versions of forward defense and persistent engagement, thus creating greater threats to U.S. network security.

A final policy implication emerges from this study related to broader military innovation. Although not the driving factor behind changes in cyber force structure, continuity in civilian defense leadership appears to have been an enabling factor in both the U.S. and Estonian cases. The creation of U.S. Cyber Command would likely have been delayed by at least six months to one year had Secretary Gates not been asked to remain in his position as Defense Secretary as the Obama administration replaced the Bush administration. Similarly, in the case of Estonia, Minister Aaviksoo's *de facto* retention of defense responsibilities as Education Minister in the wake of Mart Laar's stroke in 2012 created a continuity in leadership that sustained initial debates over the EDF's strategic role in cyberspace. This suggests that continuity in civilian

[48] For a comprehensive overview on the emulation of military practices, see: Elman, "The Logic of Emulation: The Diffusion of Military Practices in the International System."
[49] Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*.

defense leadership can facilitate the emergence of innovations—leadership appears more likely to undertake new initiatives when they have some degree of job security.

Appendix 1

Details on the Dataset on Cyber Force Structures (DCFS)

Description of the Dataset

The Dataset on Cyber Force Structures catalogues the evolution of cyber forces and force structures for all United Nations (UN) members with an active military force from 2000 to 2018. For those states with a cyber force, the DCFS captures both the organizational model utilized and the scale of command. Three states enter the dataset after 2000: Timor Leste in September 2002 after its independence and subsequent membership to the UN; Montenegro in June 2006 after independence and formal UN membership; and South Sudan in July 2011 after independence and admission to the UN.

An active military force is a necessary precondition for inclusion into the dataset: there can be no cyber force without an active military. As such, the DCFS surveys 172 UN-member states and excludes the 21 member states that do not maintain an active military force. UN-members without an active military include: Andorra, Costa Rica, Dominica, Grenada, Iceland, Kiribati, Liechtenstein, Marshall Islands, Mauritius, the Federated States of Micronesia, Monaco, Nauru, Palau, Panama, Saint Lucia, Saint Vincent and the Grenadines, Samoa, the Solomon Islands, Tuvalu, and Vanuatu.

Several cyber force initiatives from UN-member states are excluded from the dataset due to lack of adequate information for full coding according to the procedures described below. A list of these exclusions are as follows: the Bolivian Army’s Cyber Center; Cuba’s Cyber Command; Ethiopia’s Cyber Security and Space Force; the Mongolian Armed Forces Cyber Center; New Zealand’s Cyber Support Center; Pakistan’s capabilities writ large; Russia’s new

Information Warfare Branch; the United Arab Emirates' Military Cyber Command; and the modernization initiatives announced by Armenia, Georgia, and Morocco.

Finally, the DCFS does not include information on non-UN members that meet the criteria for cyber forces. For example, although Taiwan established an Information, Communications, and Electronic Warfare Command in 2017,[50] this initiative is excluded from the dataset. Subsequent expansions of the dataset will look to include both additional years and non-UN members.

Dataset Sources

The Dataset on Cyber Force Structures uses five types of resources to code country cyber forces over time. The sources are:

Official government publications. Official government publications utilized for coding include: national cyber-security strategies; national defense strategies; national cyber-defense strategies; implementation plans related to national strategies; defense white papers; government web pages; executive and legislative decrees; and government press releases and announcements. Many of these primary documents are available in English. Where official English language versions are not available, native-language versions were translated to English using Google Translate.

Reports produced by think tanks or international organizations. Reports produced by think thanks and international bodies are drawn from six main sources: initiatives of the United Nations Institute for Disarmament Research (UNIDIR); the International Telecommunication Union(ITU); the Potomac Institute's Cyber Readiness Index series; analyses from the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE); the European Union Agency for

[50] "Chapter Six: Asia."

Cybersecurity (ENISA); and think tanks such as the Center for Strategic and International Studies, Estonia's International Centre for Defense and Security, the Center for Security Studies at ETH Zurich, and the International Institute from Strategic Studies which produces *The Military Balance*. While most sources provide primary government documents and case-study analyses, it is worth noting that several UNIDIR sources catalogue broader national cyber-defense initiatives and are not limited to just the military. Accordingly these UNIDIR resources—*Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization*, *The Cyber Index* published in 2013, and the UNIDIR Cyber Policy Portal (https://cyberpolicyportal.org/en/) provided crucial starting points for research and coding.

Peer-reviewed academic works. In addition to the academic works cited in this dissertation, research and coding have relied on journal articles and books containing country-specific case studies on military reforms, national intelligence communities, and cyber-specific initiatives where available.

News articles from international and regional media outlets. Information from news and magazine outlets have been collected through LexisNexis from sources such as the Associated Press, Reuters, the Wall Street Journal, Wired Magazine, and region-specific publications such as the Diplomat (East and South-East Asia) and Dialogo Americas (Central and South America).

Interviews conducted with former policymakers, military officials, industry members, and subject matter experts. Extensive interviews have been conducted with elites in the United States (including several former military officials and one former cyber commander) and Estonia (including former Ministry of Defense policymakers, NATO CCDCOE officials, and current officials in Cyber Command). Initial interviews have also been conducted with contacts in

Germany, Switzerland, the Netherlands, and Singapore. These interviews have been used not only to obtain or confirm country-specific initiatives, but also to refine the criteria and conceptual categories for the typology presented in this dissertation.

Cyber Force Coding Procedures

Several major coding rules have been applied to these resources to ascertain both the existence of cyber forces and their force structures according to the conceptual categories of my typology. Each observation must meet the following criteria to be included in the dataset:

1) Each observation must contain the following descriptive information:

    - Name of the UN-member state to which the organization corresponds;
    - An organizational name that appears in the military hierarchy/order of battle (and, where applicable, and organizational acronym);
    - An operational start date (month and year) that indicates when cyber forces achieve initial operating capability;
    - An operational end date (month and year) indicating when an organization is dissolved or disbanded based expansion of the initial organization into a new entity, reorganization and consolidation with other organizations to create a new entity, or replacement with new initiatives that create greater changes to the military hierarchy;
    - The entity to which the organization directly reports in the military hierarchy;
    - Organizational location in either the combat or combat support chain of command;
    - The number of combat services included in the organization; and
    - Confirmation of CNO authority.
    - Where possible, the primary functional role of the organization (logistics, intelligence, combat) is noted.

2) An official government source must identify the organization and its CNO responsibilities. These government sources must be confirmed through at least two other non-government resources, regardless of resource type.

3) Where official government sources are unavailable or do not provide enough information for rule #1, information on cyber forces must be derived from at least three different types of resources listed above.

4) Cyber force subsystem location is coded based on the function of its immediate parent organization. For example, Germany's Department of Information and Computer Network Operations (2006-2017) was subordinated to the Strategic Reconnaissance Command in the Joint Support Service and is thus coded as a combat support organization (and thus a branch model). Where there is no parent organization (i.e. a unified command), subsystem location is determined by whether the organization is incorporated into combat service chains of command or stands as an independent non-service force.

5) When multiple organizations within a country are given CNO responsibilities, cyber forces are coded based on placement in the military hierarchy—those organizations higher in the chain of command that retain operational responsibilities are designated as the primary cyber force. For example, Denmark's primary cyber force from 2009-2012 was the Army 3rd Electronic Warfare Company; however, because the Offensive Cyber Warfare Unit (established 2012) under the Defense Intelligence Service had fewer links in the chain of command to the Danish Defense Command (the joint command) and the Minister of Defense, the Cyber Warfare Unit replace the 3rd Electronic Warfare Company as the primary cyber force despite the continued operation of the 3rd EW Company.

6) Organizational Model is based on (1) subsystem location and (2) the number of combat services that maintain cyber forces. Cyber forces located in the combat support subsystem maintain a Branch Model. Cyber forces in the combat subsystem have either a Service model (1 combat service) or a Joint model (2+ combat services with cyber forces). Joint organizational models occur when either (1) combat services are formally linked by a single supra-command, or (2) multiple combat services maintain their own independent cyber forces. When multiple combat services maintain cyber forces, but each of these forces report to only one of the combat services, countries are coded as having a single-service model instead of a joint structure.

7) Scale of Command is determined by immediate parent organizations and reporting structures. A Unified Command has no parent organization and reports directly to Chiefs/Ministers/Secretaries of Defense. Unified Commands are joint unified combatant commands, independent combat services, or independent branch commands. Sub-Unified Commands report to Unified Commands: they include joint combatant commands that are

not unified; Major Commands under individual combat services; and Major Commands reporting to an independent branch command. Finally, Subordinated Commands report to Sub-Unified commands (and, in rare cases, directly to Unified Commands as task forces). Subordinated command structures appear as task forces, joint component units to a unified or sub-unified combatant command, individual units reporting to a Major Command within a combat service, or functional support units reporting to branch commands.

Appendix 2

Robustness Checks for Statistical Models in Chapter 4

Robustness Checks: Unimputed Data

Table A1: Stratified Cox Model of the Entire Implementation Process, Robustness Check Using Unimputed Data

Variables	B/(SE)
Log Total Military Personnel	2.318* (1.02)
Log Total Military Personnel Squared	-0.074† (0.045)
Log Military Spending (USD mil) per 1000 Soldiers	0.178 (0.167)
Government Expertise	2.221† (1.200)
Government Expertise Squared	-0.212† (0.109)
Latent Cyber Capacity	4.687*** (1.178)
Latent Cyber Capacity Squared	-0.401** (0.135)
Regime	2.418*** (0.727)
Total Active Conflicts	0.296 (0.402)
Intensity of Strategic Environment	-0.158 (0.240)
Diffusion	13.770** (5.242)
Diffusion x Time	-0.088** (0.032)

Note: *p ≤ .05. **p ≤ .01. ***p ≤ .001. †p ≤ .10. Standard errors reported in parentheses. N = 61,052. Failures= 80. Log likelihood = -617.2566.

Table A2. Multistate Model of the Implementation Process, Robustness Check Using Unimputed Data

Covariates	P → F	P → I	I → M	I → E	I → F	M → E	M → F	E → F
Log Total Military Personnel	0.940 (0.718)	0.851*** (0.136)	0. 927† (0.492)	0.362 (0.290)	0. 170 (0.301)	0.362 (0.290)	0.678 (1.133)	0.678 (1.133)
Log Military Spending per 1000 Soldiers (USD mil)	0.846 (0.727)	0. 431* (0.187)	3.362* (1.383)	1.607* (0.741)	0.260 (0.580)	1.607* (0.741)	-0.805 (2.116)	-0.805 (2.116)
Government Expertise	0.467 (1.055)	-0.244 (0. 210)	-0.602 (0.647)	-0.491 (0.402)	-0.150 (0.425)	-0.491 (0.402)	-0.328 (1.834)	-0.328 (1.834)
Latent Cyber Capacity	-0.126 (1.851)	1.189*** (0.256)	-2.111 (1.915)	-0.145 (0.778)	1.492*** (0.399)	-0.145 (0.778)	0.535 (1.856)	0.535 (1.856)
Regime	3.393*** (0.779)	3.393*** (0.779)	3.393*** (0.779)	3.393*** (0.779)	3.393*** (0.779)	3.393*** (0.779)	3.393*** (0.779)	3.393*** (0.779)
Total Active Conflicts	0.126 (0.421)	0.126 (0.421)	0.126 (0.421)	0.126 (0.421)	0.126 (0.421)	0.126 (0.421)	0.126 (0.421)	0.126 (0.421)
Intensity of Strategic Environment	-0.052 (0.253)	-0.052 (0.253)	-0.052 (0.253)	-0.052 (0.253)	-0.052 (0.253)	-0.052 (0.253)	-0.052 (0.253)	-0.052 (0.253)
Diffusion	-14.572 (16.199)	51.136*** (13.862)	8.286* (4.021)	3.448 (2.831)	4.807 (3.876)	3.448 (2.831)	-3.573 (6.107)	-3.573 (6.107)
Diffusion x Time	-	-0.432*** (0.099)	-	-	-	-	-	-

Note: *p ≤ .05. **p ≤ .01. ***p ≤ .001. †p ≤ .10. Standard errors reported in parentheses.
N = 61,052. Failures= 80. Log likelihood = -587.43719.

Robustness Checks: Stratified Cox Models with Imputed Data

In addition to using an alternative measure for military spending, the robustness checks in Table 4.13 utilize two additional measures not discussed in the primary text of the chapter. Additional control variables are as follows:

Military Professionalism. Professionalization of the armed forces may impact the military's capacity to adopt and implement innovations. To capture the potential effects of professionalism on the implementation process, I utilize two measures: an ordinal measure assessing the extent to which appointment decisions in the armed forces are made based on personal/political connections or on skills and merit; and an ordinal measure assessing the extent to which members of the armed forces are salaried employees (conscripts are excluded). Both measures are drawn from the Varieties of Democracy Project.

Economic Development. In addition to the latent cyber capacity index, it is also possible that latent cyber capabilities rest on the development of a country's broader economic base. To account for this potential confounder, I operationalize economic development as gross domestic product (GDP) in constant 2010 U.S. dollars. This measure is logged to facilitate comparability

Across all models M1-M3, the relationship between organizational size and the implementation process holds, supporting the conclusions in the main text. Statistically significant relationships persist regardless of whether size is conceptualized in terms of military personnel (M1) or in terms of spending (M2 and M3) when controlling for other factors. In fact, these robustness checks enhance the findings in the main text: the significance levels of spending as a measure of size suggest that the personnel measure utilized in the main text is the more conservative measure for organizational size.

Table A3: Stratified Cox Models of the Implementation Process, Robustness Checks Using Imputed Data.

Covariates	M1	M2	M3
Log Total Military Personnel	2.516*	0.332*	0.328†
	(1.124)	(0.140)	(0.169)
Log Total Military Personnel Squared	-0.101* (0.049)		
Log Total Military Spending (USD mil)	0.290† (0.160)	2.059*** (0.594)	2.442*** (0.674)
Log Total Military Spending Squared (USD mil)		-0.108*** (0.034)	-0.130*** (0.037)
Military Professionalism (Appointments)	-0.052 (0.171)		-0.261 (0.165)
Military Professionalism II (Salaried)	0.148 (0.169)		0.233 (0.169)
Military Influence	-0.984		-1.728
	(1.539)		(1.582)
Government Expertise	2.266*	1.627	1.458
	(1.051)	(1.034)	(1.045)
Government Expertise Squared	-0.207*	-0.159†	-0.138
	(0.090)	(0.089)	(0.090)
Latent Cyber Capacity	3.462***	3.691***	3.781***
	(0.943)	(0.844)	(0.909)
Latent Cyber Capacity Squared	-0.255**	-0.267**	-0.272**
	(0.099)	(0.089)	(0.093)
Log GDP per capita	-0.125		-0.106
	(0.232)		(0.228)
Regime		2.732***	
		(0. 661)	
Regime II	0.233***		0.281***
	(0.070)		(0.073)
Total Active Conflicts	0.567	0.433	0.535
	(0.345)	(0.313)	(0.334)
Intensity of Strategic Environment	-0.304 (0.207)	-0.197 (0.193)	-0.248 (0.202)
Diffusion	13.437**	11.333*	12.711**
	(5.090)	(4.746)	(4.789)
Diffusion x Time	-.078**	-0.066*	-0.071*
	(0.030)	(4.746)	(0.028)

Note: *p ≤ .05. **p ≤ .01. ***p ≤ .001. †p ≤ .10. Standard errors reported in parentheses. N = 72,006. Failures=89. Imputations = 5.

Bibliography

8th Air Force/J-GSOC. “8th Air Force,” August 3, 2010. https://www.8af.af.mil/About-Us/Fact-Sheets/Display/Article/333781/8th-air-force/.

Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford, California: Stanford University Press, 2010.

Adamsky, Dima, and Kjell Inge Bjerga. “Introduction.” In *Contemporary Military Innovation: Between Anticipation and Adaptation*, edited by Dima Adamsky and Kjell Inge Bjerga, 1–6. London and New York: Routledge, 2012.

———. “Introduction to the Information-Technology Revolution in Military Affairs.” *Journal of Strategic Studies* 33, no. 4 (2010): 463–68.

Aiken, Michael, and Jerald Hage. “The Organic Organization and Innovation.” *Sociology* 5 (1971): 63–82.

Albuquerque, Adriana Lins de, and Jakob Hedenskog. “Moldova: A Defence Sector Reform Assessment.” Stockholm, Sweden: Swedish Defence Research Agency, December 2016. https://www.foi.se/rest-api/report/FOI-R--4350--SE.

Alenius, Kari. “An Exceptional War That Ended in Victory for Estonia or an Ordinary E-Disturbance?: Estonian Narratives of the Cyber-Attacks in 2007,” 18–24. Laval, France, 2012.

Allison, Graham, and Morton Halperin. “Bureaucratic Politics: A Paradigm and Some Policy Implications.” *World Politics* 24, no. 1 (1972): 40–79.

Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little Brown, 1971.

Ambler, G., S. Seaman, and R. Z. Omar. “An Evaluation of Penalised Survival Methods for Developing Prognostic Models with Rare Events.” *Statistics in Medicine* 31 (2012): 1150–61.

Applegate, Scott D. “Leveraging Cyber Militias as a Force Multiplier in Cyber Operations.” Fairfax, VA: Center for Secure Information Systems, George Mason University, 2012.

Archuleta, B. J. “Rediscovering Defense Policy: A Public Policy Call to Arms.” *Policy Studies Journal* 44, no. 1 (2016): S50–69.

Arel-Bundock, Vincent, and Krzysztof J. Pelc. “When Can Multiple Imputation Improve Regression Estimates?” *Poltical Analysis* 26 (2018): 240–45.

Ari, Baris. "Uncrossing the Rubicon: Transitions from Violent Civil Conflict to Peace." Dissertation, University of Essex, 2018.

Arias-Aranda, D., B. Minguela-Rata, and A. Rodriguez-Duarte. "Innovation and Firm Size: An Empirical Study for Spanish Engineering Consulting Companies." *European Journal of Innovation Management* 4, no. 3 (2001): 133–42.

Arquilla, J., and D. Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141–65.

Astrov, Alexander. "States of Sovereignty." *Russian Politics and Law* 47, no. 5 (2009): 66–79.

Avant, Deborah D. "The Institutional Sources of Military Doctrine: Hegemons in Peripheral Wars." *International Studies Quarterly* 37, no. 4 (1993): 409–30.

Axe, David. "Air Force Establishes 'Reduced' Cyber-War Command." *WIRED*, August 18, 2009. https://www.wired.com/2009/08/air-force-establishes-new-reduced-cyber-war-command/.

Baezner, Marie. "Study on the Use of Reserve Forces in Military Cybersecurity: A Comparative Study of Selected Countries." Zurich, Switzerland: Center for Security Studies, ETH Zurich, March 4, 2020. https://doi.org/10.3929/ethz-b-000413590.

Baldridge, J. Victor, and Robert A. Burnham. "Organizational Innovation: Industrial, Organizational, and Environmental Impact." *Administrative Science Quarterly* 20 (1975): 165–76.

Barnes, Julian E. "NATO Recognizes Cyberspace as New Frontier in Defense." *The Wall Street Journal*, June 14, 2016. https://www.wsj.com/articles/nato-to-recognize-cyberspace-as-new-frontier-in-defense-1465908566.

Barrie, Christopher. "The Process of Revolutionary Protest: Development and Democracy in the Tunisian Revolution of 2010-2011." Working Paper, August 28, 2018.

Beach, Derek, and Rasmus Brun Pedersen. *Process-Tracing Methods: Foundations and Guidelines*. Ann Arbor: The University of Michigan Press, 2013.

Bennett, Andrew, and Jeffrey T. Checkel. "Process Tracing: From Philosophical Roots to Best Practices." In *Process Tracing: From Metaphor to Analytic Tool*, edited by Andrew Bennett and Jeffrey T. Checkel, 3–37. Cambridge, United Kingdom: Cambridge University Press, 2015.

Berry, Francis Stokes, and William D. Berry. "Innovation and Diffusion Models in Policy Research." In *Theories of the Policy Process*, edited by Paul A. Sabatier and Chris Weible, 3rd Edition., 307–59. Boulder, CO: Westview Press, 2014.

———. “State Lottery Adoptions as Policy Innovations: An Event History Analysis.” *American Political Science Review* 84, no. 2 (1990): 395–415.

Biddle, Stephen. *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton and Oxford: Princeton University Press, 2006.

Bierly, Paul E., Scott Gallagher, and John-Christopher Spender. “Innovation and Learning in High-Reliability Organizations: A Case Study of United States and Russian Nuclear Attack Submarines, 1970-2000.” *IEEE Transactions on Engineering Management* 55, no. 3 (2008): 393–408.

Bing, Chris. “Command and Control: A Fight for the Future of Government Hacking.” *Cyberscoop,* April 11, 2018. https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/.

Bjerga, Kjell Inge, and Torunn Laugen Haaland. “Development of Military Doctrine: The Particular Case of Small States.” *The Journal of Strategic Studies* 33, no. 4 (2010): 505–33.

Blau, Judith R., and William McKinley. “Idea, Complexity, and Innovation.” *Administrative Science Quarterly* 24 (1979): 200–219.

Blau, P. M., and R. A. Schoenherr. *The Structure of Organizations*. New York: Basic Books, 1971.

Blau, Peter M. “A Formal Theory of Differentiation in Organizations.” *American Sociological Review* 35 (1970): 201–18.

Boeke, Sergei. “National Cyber Crisis Management: Different European Approaches.” *Governance* 31 (2018): 449–64.

Boeke, Sergei, Matthijs A. Veenendaal, and Caitriona H. Heinl. “Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges and State Practices across Asia and Europe.” In *7th International Conference on Cyber Conflict*, 1–13. Tallinn, Estonia: NATO CCD COE Publications, 2015.

Boland, Walter R. “Size, External Relations, and the Distribution of Power: A Study of Colleges and Universities.” In *Comparative Organizations*, edited by W. V. Heydebrand, 428–41. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1973.

Borghard, E. D., and S. W. Lonergan. “The Logic of Coercion in Cyberspace.” *Security Studies* 26, no. 3 (2017): 452–81.

Borras, Susana, and Charles Edquist. “The Choice of Innovation Policy Instruments.” *Technological Forecasting & Social Change* 80 (2013): 1513–22.

Box-Steffensmeier, Janet M., and Bradford S. Jones. *Event History Modeling: A Guide for Social Scientists*. Cambridge: Cambridge University Press, 2004.

Bozeman, Barry. “Technology Transfer and Public Policy: A Review of Research and Theory.” *Research Policy* 29 (2000): 627–55.

Brangetto, Pascal. “National Cyber Security Organisation: France.” National Cyber Security Organisation. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015. https://ccdcoe.org/library/publications/national-cyber-security-organisation-france/.

Brazilian Air Force. “Oficiais-Generais de Aeronautica e Da Marinha Assumem Cargo No Exercito [General Officers of the Air Force and Navy Assume Positions under the Army],” April 25, 2017. https://www.fab.mil.br/noticias/mostra/29951/INTEROPERABILIDADE%20-%20Oficiais-Generais%20da%20Aeron%C3%A1utica%20e%20da%20Marinha%20assumem%20cargo%20no%20Ex%C3%A9rcito.

Brecher, Aaron P. “Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations.” *Michigan Law Review* 111, no. 3 (December 2012): 423–52.

Bremer, S. A. “The Contagiousness of Coercion: The Spread of Serious International Disputes, 1900-1976.” *International Interactions* 9, no. 1 (1982): 29–55.

Brenner, Susan W., and Leo L. Clarke. “Conscription and Cyber Conflict: Legal Issues.” In *2011 3rd International Conference on Cyber Conflict*, edited by C. Czosseck, E. Tyugu, and T. Wingfield, 1–12. Tallinn, Estonia: CCD COE Publications, 2011.

Brooks, Risa. *Shaping Strategy: The Civil-Military Politics of Strategic Assessment*. Princeton, New Jersey: Princeton University Press, 2008.

Bruggemann, Karsten, and Andres Kasekamp. “The Politics of History and the ‘War of Monuments’ in Estonia.” *Nationalities Papers* 36, no. 3 (2008): 425–48.

Bruno, Greg. “The Capital Interview: General William Lord on Cyberspace and the Future of Warfare.” Council on Foreign Relations, April 1, 2008. https://www.cfr.org/interview/capital-interview-general-william-lord-cyberspace-and-future-warfare.

Buchanan, Benjamin. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford: Oxford University Press, 2017.

———. “The Life Cycles of Cyber Threats.” *Survival* 58, no. 1 (2016): 39–58.

Bundeswehr. “Organisation: Kommando Cyber- Und Informationsraum,” n.d. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum#Z7_694IG2S0MG6200ANOPUS4Q2021.

———. “Organisation: Kommando Streitkraftebasis,” n.d. https://www.bundeswehr.de/de/organisation/streitkraeftebasis.

Burton, J. “NATO’s Cyber Defense: Strategic Challenges and Institutional Adaptation.” *Defence Studies* 15, no. 4 (2015): 297–319.

Buzanowski, J. G. “Gen. Schwartz Addresses Air Force Future.” U.S. Air Force, September 16, 2008. https://www.af.mil/News/Article-Display/Article/122408/gen-schwartz-addresses-air-force-future/.

Caceres, R., J. Guzman, and M. Rekowski. “Firms as Source of Variety in Innovation: Influence of Size and Sector.” *International Entrepreneurship and Management Journal* 39, no. 4 (2011): 437–69.

Cameron, A. Colin, and Pravin K. Trivedi. *Microeconometrics: Methods and Applications*. 8th edition. New York and Cambridge: Cambridge University Press, 2009.

Camison-Zornoza, Cesar, Rafael Lapiedra-Alcami, Mercedes Segarra-Cipres, and Montserrat Boronat-Navarro. “A Meta-Analysis of Innovation and Organizational Size.” *Organization Studies* 25, no. 3 (2004): 331–61.

Canon, B. C., and L. Baum. “Patterns of Adoption of Tort Law Innovations: An Application of Diffusion Theory to Judicial Doctrines.” *American Political Science Review* 75, no. 4 (1981): 975–87.

Capoccia, Giovanni, and R. Daniel Kelemen. “The Study of Critical Junctures: Theory, Narrative, and Counterfactuals in Historical Institutionalism.” *World Politics* 59, no. 3 (April 2007): 341–69.

Carley, Sanya, Sean Nicholson-Crotty, and Chris J. Miller. “Adoption, Reinvention and Amendment of Renewable Portfolio Standards in the American States.” *Journal of Public Policy* 37, no. 4 (2017): 431–58.

Caverley, Jonathan D. *Democratic Militarism: Voting, Wealth, and War*. New York: Cambridge University Press, 2014.

Cederman, L. E., and K. S. Gleditsch. “Conquest and Regime Change: An Evolutionary Model of the Spread of Democracy and Peace.” *International Studies Quarterly* 48, no. 3 (2004): 603–29.

Cendoya, Alexander. “National Cyber Security Organisation: Spain.” National Cyber Security Organisation. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2016. https://ccdcoe.org/library/publications/national-cyber-security-organisation-spain/.

Cha, Victor D. “Powerplay: Origins of the U.S. Alliance System in Asia.” *International Security* 34, no. 3 (2010 2009): 158–96.

Chaffetz, Jason, Mark Meadows, and Will Hurd. “The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation.” Report from the Committee on Oversight and Government Reform. Washington, D.C.: U.S. House of Representatives (114th Congress), September 7, 2016. https://republicans-oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

Chairman of the United States Joint Chiefs of Staff. “The National Military Strategy for Cyberspace Operations.” Washington, D.C.: United States Government, December 2006. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=2700103-Document-23.

“Chapter Four: Europe.” *The Military Balance*, 2013.

“Chapter Six: Asia.” *The Military Balance*, 2019.

Checkel, Jeffrey T. “Norms, Institutions and National Identity in Contemporary Europe.” *International Studies Quarterly* 43, no. 1 (1999): 83–114.

Chesney, Robert. “Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate.” *Journal of National Security Law and Policy* 5 (2012): 539–629.

Cheung, Tai Ming, Thomas G. Mahnken, and Andrew L. Ross. “Frameworks for Analyzing Chinese Defense and Military Innovation.” In *Forging China’s Military Might: A New Framework for Assessing Innovation*, 15–46. Baltimore, Maryland: Johns Hopkins University Press, 2014.

Chilton, Kevin P. “Full Operational Capacity (FOC) of U.S. Cyber Command (USCYBERCOM).” Memorandum. United States Strategic Command, September 21, 2010. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=2692110-Document-8.

CHIPS Magazine. “Interview with Air Force Major General William T. Lord, Air Force Cyberspace Command (Provisional) Commander.” *CHIPS: The Department of the Navy’s Information Technology Magazine*, September 2008. https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=2760.

Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge and London: The Massachusettes Institute of Technology Press, 2012.

Chung, Goo Hyeok, and Jin Nam Choi. “Innovation Implementation as a Dynamic Equilibrium: Emergent Processes and Divergent Outcomes.” *Group & Organization Management* 43, no. 6 (2018): 999–1036.

Cilluffo, Frank J., and Joseph R. Clark. “Repurposing Cyber Command.” *Parameters* 43, no. 4 (2013): 111–18.

Clark, J. “Policy Diffusion and Program Scope: Research Directions.” *Publius: The Journal of Federalism* 15 (1985): 61–70.

Clarke, Richard, and Robert Knake. *Cyber War: The Next Threat to National Security*. New York: Harper Collins, 2010.

Cohen, Eliot A. “Change and Transformation in Military Affairs.” *Journal of Strategic Studies* 27, no. 3 (2004): 395–407.

Cohen, W. M., and D. A. Levinthal. “Absorpative Capacity: A New Perspective on Innovation and Learning.” *Administrative Science Quarterly* 35 (1990): 128–52.

Collier, Jamie. “Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom.” Book Chapter. Oxford, 2016. https://www.politics.ox.ac.uk/materials/publications/15664/strategies-of-cyber-crisis-management.pdf.

“Colombia Rises to the Cyber Challenge.” *Dialogo*, April 1, 2013. https://dialogo-americas.com/en/articles/colombia-rises-cyber-challenge.

Congressional Budget Office. “The U.S. Military’s Force Structure: A Primer.” Washington, D.C.: Congress of the United States, July 2016. https://apps.dtic.mil/dtic/tr/fulltext/u2/1014153.pdf.

Cook, Richard J., and Jerald F. Lawless. *Multistate Models for the Analysis of Life History Data*. Monographs on Statistics and Applied Probability. Boca Raton, Florida: CRC Press, 2018.

Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, David Altman, Michael Bernhard, et al. “V-Dem [Country-Year] Dataset V10.” University of Gothenburg: Varieties of Democracy Institute: Varieties of Democracy (V-Dem) Project, 2020.

Craig, Anthony, and Brandon Valeriano. “Conceptualising Cyber Arms Races,” 141–58. Tallinn, Estonia, 2016.

———. “Reacting to Cyber Threats: Protection and Security in the Digital Age.” *Global Security and Intelligence Strudies* 1, no. 2 (2016): 21–41.

Curley, Gregg. “The Provision of Cyber Manpower: Creating a Virtual Reserve.” *MCU Journal* 9, no. 1 (Spring 2018): 191–217.

Dalgaard-Nielsen, Anja. “Organizing Special Operations Forces: Navigating the Paradoxical Pressures of Institutional-Bureaucratic and Operational Environments.” *Special Operations Journal* 3, no. 1 (2017): 61–73.

Damanpour, Fariborz. “Organizational Innovation: A Meta-Analysis of Effects of Determinants and Moderators.” *Academy of Management Journal* 34 (1991): 675–88.

———. “Organizational Size and Innovation.” *Organization Studies* 12, no. 3 (1992): 375–402.

———. “The Adoption of Technological, Administrative, and Ancillary Innovations: Impact of Organizational Factors.” *Journal of Management* 13 (1987): 675–88.

Damanpour, Fariborz, and William M. Evan. “Organizational Innovation and Performance: The Problem of Organizational Lag.” *Administrative Science Quarterly* 29 (1984): 392–409.

Damanpour, Fariborz, and D. J. Wischnevsky. “Research on Innovation in Organizations: Distinguishing Innovation-Generating from Innovation-Adopting Organizations.” *Journal of Engineering and Technology Management* 23, no. 4 (2006): 269–91.

Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” *Wired*, August 21, 2007. https://www.wired.com/2007/08/ff-estonia/.

“Defense Minister Mart Laar Resigns after Stroke.” *ERR*. May 6, 2012. https://news.err.ee/104235/defense-minister-mart-laar-resigns-after-stroke.

Demchak, Chris C. “Creating the Enemy: Global Diffusion of the Information Technology-Based Military Model.” In *The Diffusion of Military Technology and Ideas*, edited by Emily O. Goldman and Leslie C. Eliason, 307–47. Stanford, California: Stanford University Press, 2003.

Demchak, Chris C., and Peter Dombroski. “Rise of a Cybered Westphalian Age 2.0.” In *Understanding Cyber Security: Emerging Governance & Strategy*, edited by Gary Schaub, Jr., 77–101. London and New York: Rowman and Littlefield Publishers, Inc., 2018.

Department of Defense Appropriations for Fiscal Year 2006, Pub. L. No. H.R. 2863, § Committee on Appropriations, Subcommittee on Defense (2005).

Department of Defense Historian interview with author. Interview by Jason Blessing. Hanover, Maryland, September 25, 2019.

Deutscher Bundestag. “Antwort Der Bundesregierung: Auf Die Kleine Anfrage Der Abgeordneten Sevim Dağdelen, Christine Buchholz, Annette Groth, Weiterer

Abgeordneter Und Der Fraktion DIE LINKE – Drucksache 18/11688 – Strukturen Des Organisationsbereichs Cyber- Und Informationsraum Der Bundeswehr in Nordrhein-Westfalen [Answer from the Federal Governmetn to the Request from Sevim Dagdelen, Christine Buchholz, Annette Groth, Another MP, and the DIE LINKE Parliamentary Group in Drucksache 18/11668 on the Organizational Structures of the Cyber and Information Domain Service of the Bundeswehr in North Rhine-Westpahilia." Printed Matter. Berlin, Germany, May 9, 2017. http://dipbt.bundestag.de/doc/btd/18/122/1812277.pdf.

Devai, D. "Proliferation of Offensive Cyber Weapons: Strategic Implications and Non-Proliferation Assumptions." *Academic and Applied Research in Military Science* 15, no. 1 (2016): 61–73.

Dewar, Robert S., and Jane E. Dutton. "The Adoption of Radical and Incremental Innovations: An Empirical Analysis." *Management Science* 32 (1986): 1422–33.

DiMaggio, Paul J., and Walter W. Powell. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48, no. 2 (1983): 147–60.

Directorate of Social Communication of the Joint Command of the Armed Forces of Ecuador. "Fuerzas Armadas realiza taller para defini Infraestructura critica [Armed Forces conducts workshop to define Critical Infrastructure]." *Nota Periodistica No. 2015-04-20-01-DIR-C.S.* April 20, 2015. https://www.ccffaa.mil.ec/2015/04/20/fuerzas-armadas-realiza-taller-para-definir-infraestructura-critica/.

Dorfman, Zach, Kim Zetter, Jenna McLaughlin, and Sean D. Naylor. "Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks." *Yahoo! News*, July 15, 2020. https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html.

Dougherty, D., and C. Hardy. "Sustained Product Innovation in Large, Mature Organizations: Overcoming Innovation-to-Organization Problems." *Academy of Management Journal* 39, no. 5 (1996): 1120–53.

Drea, Edward J., Ronald H. Cole, Walter S. Poole, James F. Schnabel, Robert J. Watson, and Willard J. Webb. "History of the Unified Command Plan: 1946-2012." Washington, D.C.: Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, 2013.

Drezner, Daniel W. "Ideas, Bureaucratic Politics, and the Crafting of Foreign Policy." *American Journal of Political Science* 44, no. 4 (2000): 733–49.

Dyson, T. "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.

Dyson, Tom. “The Challenge of Creating an Adaptive Bundeswehr.” *German Politics*, 2019, 1–18.

———. *The Politics of German Defence and Security: Policy Leadership and Military Reform in the Post-Cold War Era*. New York: Berghahn Books, 2007.

———. “Unpacking Military Emulation: Absorptive Capacity and German Counterinsurgency Doctrine during ISAF.” *European Security* 29, no. 1 (2020): 33–54.

Ehala, Martin. “The Bronze Soldier: Identity and Threat Maintenance in Estonia.” *Journal of Baltic Studies* 40, no. 1 (2009): 139–58.

Eisenstadt, Michael J., and Kenneth M. Pollack. “Armies of Snow and Armies of Sand: The Impact of Soviet Military Doctrine on Arab Militaries.” In *The Diffusion of Military Technology and Ideas*, edited by Emily O. Goldman and Leslie C. Eliason, 63–92. Stanford, California: Stanford University Press, 2003.

Eliason, Leslie C., and Emily O. Goldman. “Introduction: Theoretical and Comparative Perspectives on Innovation and Diffusion.” In *The Diffusion of Military Technology and Ideas*, edited by Emily O. Goldman and Leslie C. Eliason, 1–30. Stanford, California: Stanford University Press, 2003.

Elkins, Zachary, A. T. Guzman, and Beth Simmons. “Competing for Capital: The Diffusion of Bilateral Investment Treaties, 1960-2000.” *International Organization* 60, no. 4 (2006): 811–46.

Elman, Colin. “The Logic of Emulation: The Diffusion of Military Practices in the International System.” Dissertation, Columbia University, 1999.

Emmott, Robin. “NATO Cyber Command to Be Fully Operational in 2023.” *Reuters*, October 16, 2018. https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9.

Engelhardt, Manfred. “Jointness in the Bundeswehr.” In *German Defence Politics*, edited by Ira Wiesner, 1st ed., 30:163–80. Bundeswehr Academy for Information and Communication Series. Germany: Nomos, 2013.

Erwin, Marshall Curtis. “Intelligence, Surveillance, and Reconnaisance (ISR) Acquisition: Issues for Congress.” Washington, D.C.: Congressional Reseach Service, April 16, 2013. https://fas.org/sgp/crs/intel/R41284.pdf.

“Estonia Hit by ‘Moscow Cyber War.’” *BBC News*, May 17, 2007. http://news.bbc.co.uk/2/hi/europe/6665145.stm.

Estonian Cyber Command Official interview with author. Interview by Jason Blessing. Tallinn, Estonia, June 14, 2019.

Estonian Defence Forces. “Cyber Command,” n.d. http://www.mil.ee/en/landforces/Cyber-Command.

———. “Terras: NATO Kavandab Eestisse Küberharjutusvälja Loomist [Terras: NATO Plans to Create a Cyber Training Range in Estonia],” June 12, 2014. https://mil.ee/uudised/terras-nato-kavandab-eestisse-kuberharjutusvalja-loomist/.

Estonian Minister of Defense (fmr.) Jaak Aaviksoo interview with author. Interview by Jason Blessing. Tallinn, Estonia, June 3, 2019.

Ettlie, J. E., W. P. Bridges, and R. D. O’keefe. “Organizational Strategy and Structural Differences for Radical versus Incremental Innovation.” *Management Science* 30, no. 6 (1984): 682–95.

Ettlie, J. E., and A. H. Rubenstein. “Firm Size and Product Innovation.” *Journal of Produce Innovation Management* 4, no. 2 (1987): 89–108.

European Union Agency for Cybersecurity. “European Defence Ministers Meet for Cyber Exercise Support by ENISA,” September 8, 2017. https://www.enisa.europa.eu/news/enisa-news/european-defence-ministers-meet-for-cyber-exercise-supported-by-enisa.

Evangelista, Matthew. “Explaining the Cold War’s End: Process Tracing All the Way Down?” In *Process Tracing: From Metaphor to Analytic Tool*, edited by Andrew Bennett and Jeffrey T. Checkel, 153–85. Cambridge, United Kingdom: Cambridge University Press, 2015.

———. *Innovation and the Arms Race: How the United States and the Soviet Union Develop New Military Technologies*. Ithaca and London: Cornell University Press, 1988.

Eveland, J.D., E.M. Rogers, and C.M. Klepper. “The Innovation Process in Public Organizations: Some Elements of a Preliminary Model.” Report to the National Science Foundation. Ann Arbor, MI: University of Michigan, 1977.

Evron, Gadi. “Battling Botnets and Online Mobs: Estonia’s Defense Efforts during the Internet War.” *Georgetown Journal of International Affairs* 9, no. 1 (Winter 2008): 121–26.

Ewens, Hendrik, and Joris van der Voet. “Organizational Complexity and Participatory Innovation: Participatory Budgeting in Local Government.” *Public Management Review* 21, no. 12 (2019): 1848–66.

Farrell, Henry, and Charles L. Glaser. “The Role of Effects, Saliencies and Norms in U.S. Cyberwar Doctrine.” *Journal of Cybersecurity* 3, no. 1 (2017): 7–17.

Farrell, Theo. “Figuring Out Fighting Organisations: The New Organisational Analysis in Strategic Studies.” *Journal of Strategic Studies* 19, no. 1 (1996): 122–35.

———. “Improving in War: Military Adaptation and the British in Helman Province, Afghanistan, 2006-2009.” *Journal of Strategic Studies* 33, no. 4 (2010): 567–94.

Farrell, Theo, and Terry Terriff. “Military Transformation in NATO: A Framework for Analysis.” In *A Transformation Gap? American Innovations and European Military Change*, 1–13. Stanford, California: Stanford University Press, 2010.

Fedorowicz, Jane, and Janis L. Gogan. “Reinvention of Interorganizational Systems: A Case Analysis of the Diffusion of a Bio-Terror Surveillance System.” *Information Systems Frontiers* 12 (2010): 81–95.

Felongco, Gilbert P. “Philippine Armed Forces Build Up Capability to Fight in Cyberspace.” *Gulf News*, November 23, 2016. https://gulfnews.com/world/asia/philippines/philippine-armed-forces-build-up-capability-to-fight-in-cyberspace-1.1934044.

Finn, Peter. “Cyber Assaults on Estonia Typify a New Battle Tactic.” *The Washington Post*, May 19, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

Fores, Beatriz, and Cesar Camison. “Does Incremental and Radical Innovation Performance Depend on Different Types of Knowledge Accumulation Capabilities and Organizational Size?” *Journal of Business Research* 69 (2016): 831–48.

Former Estonian Ministry of Defense Official #1 interview with author. Interview by Jason Blessing. Tallinn, Estonia, June 13, 2019.

Former Estonian Ministry of Defense Official #2 interview with author. Interview by Jason Blessing. Tallinn, Estonia, June 11, 2019.

Former Estonian Ministry of Defense Official #3 interview with author. Interview by Jason Blessing. Tallinn, Estonia, May 24, 2019.

Former NSA Director of Information Warfare interview with author. Interview by Jason Blessing. Washington, D.C., March 11, 2019.

Forsman, H., and U. Annala. “Small Enterprises as Innovators: The Shift from a Low Performer to a High Performer.” *International Journal of Technology Management* 51, no. 1/2 (2011).

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

Gartzke, Erik. “Democracy and the Preparation for War: Does Regime Tyupe Affect States’ Anticipation of Casualties?” *International Studies Quarterly* 45, no. 3 (2001): 467–84.

Gates, Robert M. *Duty: Memoirs of a Secretary at War*. New York: Alfred A. Knopf, 2014.

Gelzis, Gederts. “Latvia Launches Cyber Defence Unit to Beef Up Online Security.” *Deutsche Welle*. March 4, 2014. https://www.dw.com/en/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936.

George, Alexander L., and Andrew Bennett. *Cases Studies and Theory Development in the Social Sciences*. Cambridge and London: MIT Press, 2005.

Germain, R. “The Role of Context and Structure in Radical and Incremental Logistics Innovation Adoption.” *Journal of Business Research* 35 (1997): 117–27.

German Ministry of Defense. “Abschlussbericht Aufbaustab Cyber- Und Infromationsraum [Final Report from the Cyber and Information Domain Steering Committee].” Berlin, Germany, April 2016. http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf.

Gilardi, F. “Methods for the Analysis of Policy Interdependence.” In *Comparative Policy STudies*, edited by Isabelle Engeli and Christine Rothmayr Allison, 185–204. Springer, 2014.

———. “Transnational Diffusion: Norms, Ideas, and Policies.” In *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse, and Beth Simmons, 2:453–77. London: Sage Publications Ltd, 2013.

Gilli, Andrea, and Mauro Gilli. “The Diffusion of Drone Warfare?: Industrial, Organizational, and Infrastructural Constraints.” *Security Studies* 25, no. 1 (2016): 50–84.

Glick, H.R., and S.P. Hays. “Innovation and Reinvention in State Policymaking: Theory and the Evolution of Living Wills.” *Journal of Politics* 53 (1991): 835–50.

Gode, K.M. Memo to Louis Freeh. “Re: SOLAR SUNRISE, CITA Matter; OO: HQ.” Memo, February 25, 1998. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=3145116-Document-02.

Goetz, Von John, Marcel Rosenbach, and Alexander Szandar. “National Defense in Cyberspace.” *Der Spiegel*, February 11, 2009. https://www.spiegel.de/international/germany/war-of-the-future-national-defense-in-cyberspace-a-606987.html.

Goldman, Emily. “Cultural Foundations of Military Diffusion.” *Review of International Studies* 32, no. 1 (2006): 69–91.

Goldman, Emily O. “Introduction: Military Diffusion and Transformation.” In *The Information Revolution in Military Affairs in Asia*, edited by Emily O. Goldman and Thomas G. Mahnken, 1–22. New York: Palgrave MacMillan, 2004.

———. “Receptivity to Revolution: Carrier Air Power in Peace and War.” In *The Diffusion of Military Technology and Ideas*, edited by Emily O. Goldman and Leslie C. Eliason, 267–303. Stanford, California: Stanford University Press, 2003.

Goldman, Emily O., and Leslie C. Eliason, eds. *The Diffusion of Military Technology and Ideas*. Stanford, California: Stanford University Press, 2003.

Goldman, Emily O., and Thomas G. Mahnken, eds. *The Information Revolution in Military Affairs in Asia*. New York and London: Palgrave MacMillan, 2004.

Goldman, Emily O., and Andrew L. Ross. “Conclusion: The Diffusion of Military Technology and Ideas- Theory and Practice.” In *The Diffusion of Military Technology and Ideas*, edited by Emily O. Goldman and Leslie C. Eliason, 371–404. Stanford, California: Stanford University Press, 2003.

Goldstone, Jack A. “Cultural Orthodoxy, Risk, and Innovation: The Divergence of East and West in the Early Modern World.” *Sociological Theory* 5, no. 2 (1987): 119–35.

Gomez, Miguel Alberto N. “Arming Cyberspace: The Militarization of a Virtual Domain.” *Global Security and Intelligence Studies* 1, no. 2 (2016): 42–65.

Gompert, D., and Martin Libicki. “Cyber Warfare and Sino-American Crisis Instability.” *Survival* 56, no. 4 (2014): 7–22.

Gorwa, Robert, and Max Smeets. “Cyber Conflict in Political Science: A Review of Methods and Literature,” 1–24. Toronto, Canada, 2019.

Gotkowska, Justyna. “The Cyber and Information Space: A New Formation in the Bundeswehr.” Osrodek Studiow Wschodnich, April 12, 2017. https://www.osw.waw.pl/en/publikacje/analyses/2017-04-12/cyber-and-information-space-a-new-formation-bundeswehr.

Graham, Mary. “Welcome to Cyberwar Country, USA.” *WIRED*, February 11, 2008. https://www.wired.com/2008/02/cyber-command/?currentPage=all.

Gramaglia, Matteo, Emmet Tuohy, and Piret Pernik. “Military Cyber Defense Structures of NATO Members: An Overview.” Background Paper. Tallinn, Estonia: International Centre for Defence and Security (RKK/ICDS), December 2013. https://icds.ee/wp-content/uploads/2013/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf.

Grauer, Ryan. “Moderating Diffusion: Military Bureaucratic Politics and the Implementation of German Doctrine in South America, 1885-1914.” *World Politics* 67, no. 2 (April 2015): 268–312.

Gray, V. “Innovation in the States: A Diffusion Study.” *American Political Science Review* 67, no. 4 (1973): 1174–85.

Grier, Peter. “Misplaced Nukes.” *Air Force Magazine*, June 26, 2017. https://www.airforcemag.com/article/misplacednukes/.

Griffin, Stuart. “Military Innovation Studies: Multidisciplinary or Lacking Discipline?” *Journal of Strategic Studies* 40, no. 1–2 (2017): 196–224.

Grissom, Adam. “The Future of Military Innovation Studies.” *Journal of Strategic Studies* 29, no. 5 (2006): 905–34.

Groll, Elias. “Trump Elevates Cyber Command.” *Foreign Policy*, August 2017. https://foreignpolicy.com/2017/08/18/trump-elevates-cyber-command/.

Haas, P. M. “Introduction: Epistemic Communities and International Policy Coordination.” *International Organization* 46, no. 1 (1992): 1–35.

Haizler, Omry. “The United States’ Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking.” *Cyber, Intelligence, and Security* 1, no. 1 (January 2017): 31–45.

Halperin, Morton, Priscilla Clapp, and Arnold Kanter. *Bureaucratic Politics and Foreign Policy*. 2nd ed. Washington, D.C.: Brookings Institution Press, 2006.

Hansel, Mischa. “Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks.” *Journal of International Relations and Development*, 2016, 1–29.

Harbom, Lotta, Erik Melander, and Peter Wallensteen. “Dyadic Dimensions of Armed Conflict, 1946-2007.” *Journal of Peace Research* 45, no. 5 (2008): 697–710.

Hasik, James. “Mimetic and Normative Isomorphism in the Establishment and Maintenance of Independent Air Forces.” *Defense & Security Analysis* 32, no. 3 (2016): 256–63.

Hathaway, Melissa, Chris C. Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri. “United States of America: Cyber Readiness at a Glance.” Cyber Readiness Index 2.0. Arlington, VA: Potomac Institute for Policy Studies, September 2016. https://www.potomacinstitute.org/images/CRI/CRI_US_Profile_Web.pdf.

Haukkala, Hiski. “A Close Encounter of the Worst Kind? The Logic of Situated Actors and the Statue Crisis between Estonia and Russia.” *Journal of Baltic Studies* 40, no. 2 (2009): 201–13.

Haveman, H. A. “Between a Rock and a Hard Place: Organizational Change and Performance under Conditions of Fundamental Environmental Uncertainty.” *Administrative Science Quarterly* 37 (1992): 48–75.

Hays, Scott P. "Patterns of Reinvention: The Nature of Evolution during Policy Diffusion." *Policy Studies Journal* 24, no. 4 (1996): 551–66.

Hays, S.P. "Influences on Reinvention during the Diffusion of Innovations." *Political Research Quarterly* 49 (1996): 631–50.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington, VA: Cyber Conflict Studies Association, 2013.

"HEARING TO RECEIVE TESTIMONY ON COUNTER-ISIL (ISLAMIC STATE OF IRAQ AND THE LEVANT) OPERATIONS AND MIDDLE EAST STRATEGY." Hearing. Washington, D.C.: U.S. Senate Committee on Armed Services, April 28, 2016. https://www.armed-services.senate.gov/imo/media/doc/16-51_04-28-16.pdf.

Heiden, N. van der, and F. Strebel. "What About Non-Diffusion? The Effect of Competitiveness in Policy-Comparative Diffusion Research." *Policy Sciences* 45, no. 4 (2012): 345–58.

Herrera, Geoffrey L. *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. Albany, New York: State University of New York PRess, 2006.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49–60.

Hitt, Michael A., Robert E. Hoskisson, and R. Duane Ireland. "Mergers and Acquisitions and Managerial Commitment to Innovation in M-Form Firms." *Strategic Management Journal* 11 (1990): 29–47.

Horowitz, Michael C. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton, New Jersey: Princeton University Press, 2010.

Horowitz, Michael C., and Shira E. Pindyck. "What Is a Military Innovation? A Proposed Framework." Working Paper, December 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504246.

Howlett, Michael. "Policy Instruments, Policy Styles, and Policy Implementation: National Approaches to Theories of Instrument Choice." *Policy Studies Journal* 19, no. 2 (1991): 1–21.

Howlett, Michael, Ishani Mukherjee, and Jun Jie Woo. "From Tools to Toolkits in Policy Design Studies: The New Design Orientation towards Policy Formulation Research." *Policy and Politics* 43, no. 2 (2015): 291–311.

Hwang, Suk Joon, and Frances Berry. "Deterring Drunk Driving: Why Some States Go Further than Others in Policy Innovation." *International Journal of Environmental Research and Public Health* 16 (2019): 1749–67.

"IDF Scraps Plans for a Unified Cyber Command." *Israel Defense,* May 15, 2017. https://www.israeldefense.co.il/en/node/29613.

"In Fight Against ISIS, U.S. Adds Cyber Tools." National Public Radio, February 28, 2016. https://www.npr.org/2016/02/28/468446138/in-fight-against-isis-u-s-adds-cyber-tools.

Italian Ministry of Defence. "Il Sottosegratario Tofalo visita il Comando C4 Difesa e il CIOC [Undersecretary Tofalo visits the C4 Defense Command and the CIOC]." August 1, 2018. https://www.difesa.it/Primo_Piano/Pagine/Il-Sottosegretario-Tofalo-visita-il-Comando-C4-Difesa-e-il-CIOC.aspx.

Johansson, Grace. "NATO CCDCOE Coordinates NATO Cyber Education and Training." *SC Media,* February 8, 2018. https://www.scmagazineuk.com/nato-ccdcoe-coordinates-nato-cyber-education-training/article/1473351.

Johnson, Derek B. "Rogers: CyberCom Lacks Authority, Resources to Defend All of Cyberspace." *FCW: The Business of Federal Technology,* February 27, 2018. https://fcw.com/articles/2018/02/27/rogers-congress-sasc-nsa.aspx.

Jones, Benjamin T., and Shawna K. Metzger. "Different Words, Same Song: Advice for Substantively Interpreting Duration Models." *Political Science & Politics* 52, no. 4 (2019): 691–95.

———. "Evaluating Conflict Dynamics: A Novel Empirical Approach to Stage Conceptions." *Journal of Conflict Resolution* 62, no. 4 (2016): 819–47.

Junio, Timothy J. "How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate." *Journal of Strategic Studies* 36, no. 1 (2013): 125–33.

———. "Marching Across the Cyber Frontier: Explaining the Global Diffusion of Network-Centric Warfare." In *Cyberspaces in Global Affairs,* edited by Sean S. Costigan and Jake Perry, 51–74. Burlington, Vermont: Ashgate Publishing Company, 2012.

———. "The Politics and Strategy of Cyber Conflict." Dissertation, University of Pennsylvania, 2013.

Kaarbo, Juliet. "Power Politics in Foreign Policy: The Influence of Bureaucratic Minorities." *European Journal of International Relations* 4, no. 1 (1998): 67–97.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

Karabeshkin, Leonid A. "The Ongoing Transformation of the Estonian Defence Forces." In *Democratic Civil-Military Relations: Soldiering in 21st Century Europe,* edited by Sabine Mannitz, 128–45. London and New York: Routledge, 2012.

Karch, Andrew. “Emerging Issues and Future Directions in State Policy Diffusion Research.” *State Politics & Policy Quarterly* 7, no. 1 (2007): 54–80.

Kash, Wyatt. “Lessons from the Cyberattacks on Estonia.” *Government Computer News*, June 13, 2008. https://gcn.com/Articles/2008/06/13/Lauri-Almann--Lessons-from-the-cyberattacks-on-Estonia.aspx?Page=1.

Kaska, Kadri. “National Cyber Security Organisation: The Netherlands.” National Cyber Security Organisation. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015. https://ccdcoe.org/library/publications/national-cyber-security-organisation-the-netherlandskadri-kaskaactive-passive-cyber-defence-law-national-frameworks-policy-strategy-the-netherlands/.

Kaska, Kadri, Anna-Maria Osula, and Jan Stinissen. “The Cyber Defence Unit of the Estonian Defence League: Legal, Policy, and Organisational Analysis.” Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2013.

Keck, Zachary. “South Korea Seeks Offensive Cyber Capabilities.” *The Diplomat*, October 11, 2014. https://thediplomat.com/2014/10/south-korea-seeks-offensive-cyber-capabilites/.

Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security* 38, no. 2 (2013): 7–40.

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

Kier, Elizabeth. “Culture and Military Doctrine: France between the Wars.” *International Security* 19, no. 4 (1995): 65–93.

Kimberly, John R., and Michael R. Evanisko. “Organizational Innovation: The Influence of Individual, Organizational, and Contextual Factors on Hospital Adoption of Technological and Administrative Innovations.” *Academy of Management Journal* 24 (1981): 689–713.

Knake, Robert. “Obama’s Cyberdoctrine.” *Foreign Affairs*, May 6, 2016. https://www.foreignaffairs.com/articles/united-states/2016-05-06/obamas-cyberdoctrine.

Koontz, V. “Determinants of Individuals’ Knowledge, Attitudes and Decisions Regarding a Health Innovation in Maine.” Dissertation, University of Michigan, 1976.

Kopstein, J. S., and D. A. Reilly. “Geographic Diffusion and the Transformation of the Postcommunist World.” *World Politics* 53, no. 1 (2000): 1–37.

Kostyuk, Nadiya, and Yuri M. Zhukov. “Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?” *Journal of Conflict Resolution*, 2017, 1–31. http://journals.sagepub.com/doi/pdf/10.1177/0022002717737138.

Kozlowski, Andrzej. “Comparative Analysis of Cyberattacks on Estonia, Georgia, and Kyrgyzstan.” *European Scientific Journal* 3 (February 2014): 237–45.

Kraner, Jan. *Innovation in High Reliability Ambidextrous Organizations: Analytical Solutions Toward Increasing Innovative Activity*. Cham, Switzerland: Springer International Publishing, 2018.

Krause, Robert. “Air Force Cyberspace Symposium Now a Reality.” *Eighth Air Force Public Affairs*, November 29, 2007. https://www.8af.af.mil/News/Article-Display/Article/333938/air-force-cyberspace-symposium-now-a-reality/.

Krepinevich, Andrew F. “Cavalry to Computer: The Pattern of Military Revolutions.” *The National Interest*, no. 37 (1994): 30–42.

Kumar, Kamalesh, and Mary S. Thibodeaux. “Organizational Politics and Planned Organization Change: A Pragmatic Approach.” *Group & Organization Studies* 15, no. 4 (1990): 357–65.

Kuul, Marek. “Kaitseministeeriumi Küberpoliitika Osakonda Hakkab Juhtima Mihkel Tikk [Mihkel Tikk Will Head the Cyber Policy Department of the Ministry of Defense].” *ERR*, June 13, 2014. https://www.err.ee/514725/kaitseministeeriumi-kuberpoliitika-osakonda-hakkab-juhtima-mihkel-tikk.

Laforet, S. “Organizational Innovation Outcomes in SMEs: Effects of Age, Size, and Sector.” *Journal of World Business* 48, no. 4 (2013): 590–502.

Lall, Ranjit. “How Multiple Imputation Makes a Difference.” *Political Analysis* 24 (2016): 414–33.

Laporte, T. R., and P. M. Consolini. “Working in Practice but Not in Theory: Theoretical Challenges of ‘High Reliability Organizations.’” *Journal of Public Administration Research and Theory* 1, no. 1 (1991): 19–48.

Lasoen, Kenneth L. “Belgian Intelligence SIGINT Operations.” *International Journal of Intelligence and CounteriIntelligence* 32, no. 1 (2019): 1–29.

Lawson, Sean T., Haoran Yu, Sara K. Yeo, and Ethan Greene. “The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate,” 65–80. Tallinn, 2016.

Lee, Katherine J., and John B. Carlin. “Multiple Imputation in the Presence of Non-Normal Data.” *Statistics in Medicine* 36 (2017): 606–17.

Legro, Jeffrey W. “Military Culture and Inadvertent Escalation in World War II.” *International Security* 18, no. 4 (1994): 108–42.

Lehti, Marko, Matti Jutila, and Markku Jokisipila. “Never-Ending Second World War: Public Performances of National Dignity and the Drama of the Bronze Soldier.” *Journal of Baltic Studies* 39, no. 4 (2008): 393–418.

Leiblein, M. J., and T. L. Madsen. “Unbundling Competitive Heterogeneity: Incentive Structures and Capability Influences on Technological Innovation.” *Strategic Management Journal* 30 (2009): 711–35.

Leinhos, Ludwig. “Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr.” *Connections: The Quarterly Journal* 19, no. 1 (2020): 9–19.

Levinthal, D. A., and James G. March. “The Myopia of Learning.” *Strategic Management Journal* 14 (1993): 95–112.

Lewis, James A. “Managing New Style Warfare: An Interview with Keith Alexander.” Cyber From the Start. Accessed May 10, 2019. https://www.csis.org/podcasts/cyber-start.

———. “The Fifth Domain: An Interview with William Lynn.” Cyber From the Start. Accessed April 12, 2019. https://www.csis.org/podcasts/cyber-start.

———. “What Keeps You Up at Night? An Interview with Michael McConnell.” Cyber From the Start. Accessed April 26, 2019. https://www.csis.org/podcasts/cyber-start.

Lewis, James Andrew, and Gotz Neuneck. “The Cyber Index: International Security Trends and Realities.” New York and Geneva: United Nations Institute for Disarmament Research, 2013.

Leyen, Ursula von der. “Tagesbefehl [Daily Command],” September 7, 2015.

Libicki, Martin. “It Takes More Than Offensive Capability to Have an Effective Cyberdeterrence Posture:” Testimony. Washington, D.C.: U.S. House of Representatives Committee on Armed Services, March 1, 2017. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3515026-Document-12-Martin-C-Libicki-U-S-Naval-Academy.

Liles, Samuel, and Jacob Kambic. “Cyber Fratricide.” In *6th International Conference on Cyber Conflict*, 329–38. Tallinn, Estonia: NATO CCD COE Publications, 2014.

Lilly, Bilyana, and Joe Cheravitch. “The Past, Present, and Future of Russia’s Cyber Strategy and Forces.” In *20/20 Vision: The Next Decade*, edited by T. Jancarkova, L. Lindstrom, M. Signoretti, I. Tolga, and G. Visky, 129–55. Tallinn, Estonia: NATO CCD COE Publications, 2020.

Lin, Herbert S., and Amy B. Zegart. “Introduction.” In *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, 1–17. Brookings Institution Press, 2019.

Lindsay, John. “The Impact of China on Cyber Security: Fiction and Friction.” *International Security* 39, no. 3 (2015): 7–47.

Loonet, Teelemari. “Kaitseministeeriumis Alustas Tööd Küberpoliitika Osakond [Cyber Policy Department Begins Work in Ministry of Defense].” *Postimees*, February 4, 2014. https://www.postimees.ee/2684832/kaitseministeeriumis-alustas-tood-kuberpoliitika-osakond.

Lopez, C. Todd. “8th Air Force to Become New Cyber Command.” *Air Force Print News*, November 15, 2006. https://www.8af.af.mil/News/Article-Display/Article/333953/8th-air-force-to-become-new-cyber-command/.

Lynch, Lisa. “The Leak Heard Round the World? Cablegate in the Evolving Global Mediascape.” In *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, edited by Benedetta Brevini, Arne Hintz, and Patrick McCurdy, 56–77. Palgrave MacMillan, 2013.

Lynn, John A. “Heart of the Sepoy: The Adoption and Adaptation of European Military Practice in South Asia, 1740-1805.” In *The Diffusion of Military Technology and Ideas*, edited by Emily O. Goldman and Leslie C. Eliason, 33–62. Stanford, California: Stanford University Press, 2003.

Mahnken, Thomas G. “China’s Anti-Access Strategy in Historical and Theoretical Perspective.” *The Journal of Strategic Studies* 34, no. 3 (2011): 299–323.

Mahoney, James. “Path Dependence in Historical Sociology.” *Theory and Society* 29 (2000): 504–48.

———. “Process Tracing and Historical Explanation.” *Security Studies* 24, no. 2 (2015): 200–218.

Mahoney, James, and Gary Goertz. “The Possibility Principle: Choosing Negative Cases in Comparative Research.” *American Political Science Review* 98, no. 4 (November 2004): 653–69.

Mahoney, James, Khairunnisa Mohamedali, and Christoph Nguyen. “Causality and Time in Historical Institutionalism.” In *The Oxford Handbook of Historical Institutionalism*, 71–88. Oxford: Oxford University Press, 2016.

Maness, Ryan C., and Brandon Valeriano. “The Impact of Cyber Conflict on International Interactions.” *Armed Forces & Society* 42, no. 2 (2016): 301–23.

Marsh, Robert M., and Hiroshi Mannari. “The Size Imperative? Longitudinal Tests.” *Organization Studies* 10, no. 1 (1989): 83–95.

Martelle, Michael. “Eligible Receiver 97.” Briefing Book. The Cyber Vault Project. George Washington University, August 1, 2018. The National Security Archive. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations.

Matania, Eviatar, Lior Yoffe, and Tal Goldstein. “Structuring the National Cyber Defence: In Evolution towards a Central Cyber Authority.” *Journal of Cyber Policy* 2, no. 1 (2017): 16–25.

Mauslein, Jacob. “Three Essays on International Cyber Threats: Target Nation Characteristics, International Rivalry, and Asymmetric Information Exchange.” Dissertation, Kansas State University, 2014.

May, Peter J. “Policy Design and Implementation.” In *The SAGE Handbook of Public Administration*, edited by B. Guy Peters and Jon Pierre, 279–91. London: Sage Publications Ltd, 2012.

McHugh, Kelly. “A Tale of Two Surges: Comparing the Politics of the 2007 Iraq Surge and the 2009 Afghanistan Surge.” *SAGE Open* 5, no. 4 (2015): 1–16.

McWhorter, Dan. “Mandiant Exposes APT1 - One of China’s Cyber Espionage Units and Releases 3,000 Inidcators.” Fireye, February 19, 2013. https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html.

Mechkova, Valeriya, Daniel Pemstein, Brigitte Seim, and Steven Wilson. “Measuring Internet Politics: Introducing the Digital Society Project (DSP).” Working Paper #1. Varieties of Democracy (V-Dem) Project, May 2019.

Mellingen, Kjetil. “Strategic Utilization of Norwegian Special Operations Forces.” Naval Postgraduate School, 2010.

Metzger, Shawna K., and Benjamin T. Jones. “Surviving Phases: Introducing Multistate Survival Models.” *Political Analysis* 24 (2016): 457–77.

Meyer, Alan D., and James B. Goes. “Organizational Assimilation of Innovations: A Multilevel Contextual Analysis.” *Academy of Management Journal* 31 (1988): 897–923.

Miller, Drew, Daniel B. Levine, and Stanley A. Horowitz. “A New Approach to Force-Mix Analysis: A Case Study Comparing Air Force Active and Reserve Forces Conducting Cyber Missions.” Alexandria, Virginia: Institute for Defense Analyses, September 2013.

Min, Eric. “Cheaper Talk: The Changing Nature of Wartime Negotiation in the Post-1945 Order.” Working Paper. University of California, Los Angeles, October 6, 2018.

Minarik, Tomas. “NATO Recognizes Cyberspace as a ‘Domain of Operations’ at Warsaw Summit.” NATO CCD COE Publications, July 2016. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

Ministry of Defense. “Cyber Security Strategy.” Republic of Estonia, May 2008.

———. “Estonian Long Term Defence Development Plan.” Republic of Estonia, January 22, 2009. https://www.ecfr.eu/page/-/Estonie_-_2009_-_Estonia_long_term_development_plan_2009_2018.pdf.

———. “Käskkirjaga nr 34: Küberpoliitika osakonna põhimäärus [Directive No. 34: Statutes of the Cyber Policy Department].” Republic of Estonia, January 31, 2014. https://www.kaitseministeerium.ee//sites/default/files/elfinder/article_files/kuberpoliitika_osakond.pdf.

———. “National Defence Development Plan 2013-2022.” Republic of Estonia, 2013. https://www.kaitseministeerium.ee//riigikaitse2022/riigikaitse-arengukava/index-en.html.

———. “National Defence Development Plan 2017-2026.” Republic of Estonia, 2017. https://www.kaitseministeerium.ee/riigikaitse2026/arengukava/eng/.

———. “National Defence Strategy: Estonia.” Republic of Estonia, 2011. https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

Ministry of Defense of Norway. “Cyberforsvaret offisielt etablert i dag [Cyber Defence Force officially established today],” September 18, 2012. https://www.regjeringen.no/no/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/Nyheter/2012/cyber/id699271/.

Ministry of Economic Affairs and Communication. “National Cyber Security Strategy for 2014-2014.” Republic of Estonia, September 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

Ministry of Education and Research. “Estonian Presidency of the Council of the European Union 2017.” Republic of Estonia, 2017. https://www.hm.ee/en/activities/european-union/estonian-presidency-council-european-union-2017#:~:text=Estonia%20was%20holding%20hold%20its,than%20500%20million%20EU%20citizens.

Ministry of Foreign Affairs. “Estonia in the European Union.” Republic of Estonia, n.d. https://vm.ee/en/estonia-european-union.

Mintrom, M., and S. Vergari. “Policy Networks and Innovation Diffusion: The Case of State Education Reforms.” *The Journal of Politics* 60, no. 1 (1998): 126–48.

Mintzberg, H. *The Structuring of Organizations*. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1979.

Mooney, C.Z., and M. H. Lee. "Legislative Morality in the American States: The Case of Pre-Roe Abortion Regulation Reform." *American Journal of Political Science* 39 (1995): 599–627.

Moore, Johannes. "From Conception to Birth: The Forces Responsible for AFCYBER's Evolution." Air University, 2014.

Morris, Tim P., Ian R. White, and Patrick Royston. "Tuning Multiple Imputation by Predictive Mean Matching and Local Residual Draws." *BMC Medical Research Methodology* 14, no. 75 (2014): 1–13.

Morrow, James D. "Alliances and Asymmetry: An Alternative to the Capability Aggregation Model of Alliances." *American Journal of Political Science* 35, no. 3 (1991): 904–33.

Most, B.A., and H. Starr. "Diffusion, Reinforcement, Geopolitics, and the Spread of War." *American Political Science Review* 74, no. 4 (1980): 932–46.

Moury, Taciana. "Brazilian Army Invests in Cyber Defense." *Dialogo*, May 12, 2017. https://dialogo-americas.com/en/articles/brazilian-army-invests-cyber-defense.

Moynihan, D. P. "A Theory of Culture-Switching: Leadership and Red-Tape during Hurricane Katrina." *Public Administration* 90, no. 4 (2012): 851–68.

Mukherjee, Anit. "Fighting Separately: Jointness and Civil-Military Relations in India." *Journal of Strategic Studies* 40, no. 1–2 (2017): 6–34.

Mulford, Laurie A. "Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. Cyber Command." National Defense University, Washington, D.C. https://apps.dtic.mil/dtic/tr/fulltext/u2/a587698.pdf.

Nakashima, Ellen. "Cyber-Intruder Sparks Massive Federal Response - and Debate over Dealing with Threats." *The Washington Post*. December 8, 2011. https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_print.html.

———. "Dismantling of Saudi-NSA Web Site Illustrates Need for Clearer Cyberwar Policies." *The Washington Post*. March 19, 2010. https://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html?sid=ST2010031901063.

———. "Gates Establishes Cyber-Defense Command." *The Washington Post*. June 24, 2009. https://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303492.html.

———. “Incoming NSA Chief Has a Reputation for Winning ‘All the Important Fights.’ Russia Will Be His Biggest Test Yet.” *The Washington Post*, April 1, 2018. https://www.washingtonpost.com/world/national-security/incoming-nsa-chief-has-a-reputation-for-winning-all-the-important-fights-russia-will-be-his-biggest-test-yet/2018/03/31/ee943ef0-23d6-11e8-badd-7c9f29a55815_story.html.

———. “Pentagon’s Cyber Command Seeks Authority to Expand Its Battlefield.” *The Washington Post*. November 6, 2010. https://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html?wprss=rss_world.

———. “U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms.” *The Washington Post*. February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

———. “U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies.” *The Washington Post*, May 9, 2017. https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.

NATO Cooperative Cyber Defence Centre of Excellence. “About Us.” *CCDCOE: NATO Cooperative Cyber Defence Centre of Excellence* (blog), n.d. https://ccdcoe.org/about-us.html.

———. “Centre Contributed to New Estonian Cyber Security Strategy,” December 29, 2014. https://ccdcoe.org/news/2014/centre-contributed-to-the-new-estonian-cyber-security-strategy/.

Nielsen, S. “The Role of the U.S. Military in Cyberspace.” *Journal of Information Warfare* 15, no. 2 (2016): 27–38.

Nooteboom, B., W. Van Haverbeke, G. Duysters, V. Gilsing, and A. Van den Oord. “Optimal Cognitive Dissonance and Absorbative Capacity.” *Research Policy* 36 (2007): 1016–34.

Nord, Walter R., and Sharon Tucker. *Implementing Routine and Radical Innovation*. Lexington, MA: Lexington Books, 1987.

North Atlantic Treaty Organization. “Centres of Excellence.” North Atlantic Treaty Organization, January 24, 2019. https://www.nato.int/cps/en/natohq/topics_68372.htm.

———. “Member Countries.” North Atlantic Treaty Organization, March 24, 2020. https://www.nato.int/cps/en/natohq/topics_52044.htm#:~:text=Cold%20War%20enlargement-

,Bulgaria%2C%20Estonia%2C%20Latvia%2C%20Lithuania%2C%20Romania%2C%20 Slovakia%20and,of%20enlargement%20in%20NATO%20history.

———. “NATO Supports Jordan’s National Cyber Defence Strategy,” July 19, 2017. https://www.nato.int/cps/en/natohq/news_146287.htm.

Nye, Jr., Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter /2017 2016): 44–71.

Office of the Director of National Intelligence. “Assessing Russian Activities and Intentions in Recent US Elections.” Intelligence Community Assessment. Washington, D.C.: United States Government, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Olsen, Tommy, and Marius Thormodsen. “Forging Norwegian Special Operation Forces.” Naval Postgraduate School, 2014.

Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups*. 2nd ed. Cambridge, MA: Harvard University Press, 1971.

Omonobi-Abuja, Kingsley. “Nigerian Army’s Cyber Warfare Command Begins Operation.” *Vanguard*, August 29, 2018. https://www.vanguardngr.com/2018/08/nigerian-armys-cyber-warfare-command-begins-operation/.

O’Neill, Patrick Howell. “The Cyberattack That Changed the World.” *The Daily Dot*, May 20, 2016. https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/.

Operation Inherent Resolve. “About CJTF-OIR,” n.d. https://www.inherentresolve.mil/About-CJTF-OIR/.

Osula, Anna-Maria. “National Cyber Security Organisation: Estonia.” Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Osula, Anna-Maria. “National Cyber Security Organisation: United Kingdom.” National Cyber Security Organisation. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015. https://ccdcoe.org/library/publications/national-cyber-security-organisation-united-kingdom/.

Papenfus, Joseph A. “Total Army Cyber Mission Force: Reserve Component Integration.” Master’s Thesis, Air War College, 2016.

Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. “The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.” Santa Monica, CA: RAND Corporation, 2014.

Pavitt, K. "What We Know about the Strategic Management of Technology." *California Management Review* 23, no. 3 (1990): 17–26.

Pavlou, Menelaos, Gareth Ambler, Shaun R. Seaman, Oliver Guttmann, Perry Elliott, Michael King, and Rumana Z. Omar. "How to Develop a More Accurate Risk Prediction Model When There Are Few Events." *The British Journal of Medicine* 351 (2015): 1–5.

Pemstein, Daniel, Kyle L. Marquardt, Eitan Tzelgov, Yi-ting Wang, Juraj Medzihorsky, Joshua Krusell, Farhad Miri, and Johannes von Romer. "The V-Dem Measurement Model: Latent Variable Analysis for Cross-National and Cross-Temporal Expert-Coded Data." V-Dem Working Paper. University of Gothenburg: Varieties of Democracy Institute, 2020.

Pepinsky, Thomas B. "A Note on Listwise Deletion versus Multiple Imputation." *Political Analysis* 26 (2018): 480–88.

Pernik, Piret. "Preparing for Cyber Conflict: Case Studies of Cyber Command." Tallinn, Estonia: International Centre for Defence and Security (RKK/ICDS), December 2018.

Pettersson, Therese, Stina Hogbladh, and Magnus Oberg. "Organized Violence, 1989-2018 and Peace Agreements." *Journal of Peace Research* 56, no. 4 (2019).

Posen, Barry R. *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*. Ithaca and London: Cornell University Press, 1984.

Prezelj, Iztok, Erik Kopac, Ales Ziberna, Anja Kolak, and Anton Grizold. "Quantitative Monitoring of Military Transformation in the Period 1992-2010: Do the Protagonists of Transformation Really Change More than Other Countries?" *Defence Studies* 16, no. 1 (2016): 20–46.

Raisch, Sebastian, and Julian Birkinshaw. "Organizational Ambidexterity: Antecedents, Outcomes, and Moderators." *Journal of Management* 34, no. 3 (2008): 375–409.

Reiter, Dan. "Learning, Realism, and Alliances: The Weight of the Shadow of the Past." *World Politics* 46, no. 4 (July 1994): 490–526.

Republic of Estonia. "National Security Concept of Estonia," May 12, 2010.

Resende-Santos, Joao. "Anarchy and the Emulation of Military Systems." *Security Studies* 5, no. 3 (1996): 193–260.

———. *Neorealism, States, and the Modern Mass Army*. Cambridge: Cambridge University Press, 2007.

Rice, Ronald E., and Everett M. Rogers. "Reinvention in the Innovation Process." *Knowledge: Creation, Diffusion, Utilization* 1, no. 4 (June 1980): 499–514.

Richards, Jason. “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security.” *International Affairs Review* 18, no. 2 (2008). http://www.iar-gwu.org/node/65.

Riigikogu. Estonian Defence Forces Organisation Act, Pub. L. No. RT I 2008, 35, 213, § 57 (2009). https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530102013067/consolide.

———. Kaitseväe põhimäärus [Statutes of the Defence Forces], Pub. L. No. RT I, 28.06.2018, 8, 45 (2018). https://www.riigiteataja.ee/akt/128062018008.

Roberts, Kristin. “Air Force Leadership Fired over Nuclear Issue.” *Reuters*, June 5, 2008. https://www.reuters.com/article/us-usa-airforce/air-force-leadership-fired-over-nuclear-issue-idUSWAT00960720080606.

Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, and Pablo Rodriguez. “Stocktaking Study of Military Cyber Defence Capabilities in the European Union (MilCyberCAP): Unclassified Summary.” RAND Corporation, 2013.

Rogers, E. M. “A Prospective and Restrospective Look at the Diffusion Model.” *Journal of Health Communication* 9, no. S1 (2004): 13–19.

Rogers, Everett M. *Diffusion of Innovations*. 5th ed. New York: Free Press, 2003.

Rogin, Josh. “Air Force to Create Cyber Command.” *FCW: The Business of Federal Technology*, November 13, 2006. https://fcw.com/articles/2006/11/13/air-force-to-create-cyber-command.aspx.

Rohde, David, and David E. Sanger. “How a ‘Good War’ in Afghanistan Went Bad.” *The New York Times*, August 12, 2007. https://www.nytimes.com/2007/08/12/world/asia/12afghan.html.

Rosen, Stephen Peter. *Winning the Next War: Innovation and the Modern Military*. Ithaca and London: Cornell University Press, 1991.

“Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardian*, May 16, 2007. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

“Russia ‘Was Behind German Parliament Hack.’” *BBC News*, May 13, 2016. https://www.bbc.com/news/technology-36284447.

Ruus, Kertu. “Cyber War I: Estonia Attacked from Russia.” *European Affairs* 9, no. 1–2 (Winter/Spring 2008). http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

Saltzman, I. “Cyber Posturing and the Offense-Defense Balance.” *Contemporary Security Policy* 34, no. 1 (2013): 40–63.

Samaan, J. L. “Cyber Command: The Rift in U.S. Military Cyber-Strategy.” *The RUSI Journal* 155, no. 6 (2010): 16–21.

Scherer, Frederic M., and David Ross. *Industrial Market Structure and Economic Performance*. Boston, MA: Houghton Mifflin, 1990.

Schlesinger, James R. “Report of the Secretary of Defense Task Force on DOD Nuclear Weapons Management: Phase II: Review of the DOD Nuclear Mission.” Arlington, VA, December 2008.

Schmidt, Andreas. “The Estonian Cyberattacks.” Book Chapter. Delft University of Technology, 2013. http://netdefences.com/wp-content/uploads/SchmidtA-2013-Estonian-Cyberattacks.pdf.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017.

Schneider, Jacquelyn. “The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict.” Dissertation, George Washington University, 2017.

Scott, W. Richard. *Organizations: Rational, Natural, and Open Systems*. Fourth Edition. New Jersey: Prentice-Hall, Inc., 1998.

Seaman, Shaun R., Jonathan W. Bartlett, and Ian R. White. “Multiple Imputation of Missing Covariates with Non-Linear Effects and Interactions: An Evaluation of Statistical Methods.” *BMC Medical Research Methodology* 12, no. 46 (2012): 1–13.

Seawright, Jason. *Multi-Method Social Science: Combining Qualitative and Quantitative Tools*. Cambridge, United Kingdom: Cambridge University Press, 2016.

Seker, Esnar, and Ihsan Burak Tolga. “National Cyber Security Organisation: Turkey.” National Cyber Security Organisation. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2018. https://ccdcoe.org/library/publications/national-cyber-security-organisation-turkey/.

Shachtman, Noah. “Air Force Suspends Controversial Cyber Command.” *WIRED*, August 13, 2008. https://www.wired.com/2008/08/air-force-suspe/.

Shaughnessy, Larry. “Gates Proposes Cutting Joint Forces Command from Defense Budget.” *CNN*, August 10, 2010. https://www.cnn.com/2010/POLITICS/08/09/gates.joint.forces/index.html.

Shead, Sam. “Estonia Is So Scared of a Russian Cyberattack That It’s Opening a Data Centre in the UK.” *Business Insider*, July 25, 2016. http://www.businessinsider.com/estonia-is-so-scared-of-a-russian-cyberattack-that-its-opening-a-data-centre-in-the-uk-2016-7.

Shipan, C. R., and C. Volden. “Bottom-up Federalism: The Diffusion of Antismoking Policies from U.S. Cities to States.” *American Journal of Political Science* 50, no. 4 (2006): 825–43.

Simmons, Beth, and Zachary Elkins. “The Globalization of Liberalization: Policy Diffusion in the International Political Economy.” *American Political Science Review* 98, no. 1 (February 2004): 171–89.

Siverson, R. M., and H. Starr. “Opportunity, Willingness, and the Diffusion of War.” *American Political Science Review* 84, no. 1 (1990): 47–67.

Skierka, Isabel. “Bundeswehr: Cyber Security, the German Way.” *Observer Research Fourndation*, October 20, 2016. https://www.orfonline.org/expert-speak/bundeswehr-cyber-security-the-german-way/.

Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment.” *International Security* 41, no. 3 (Winter /2017 2016): 72–109.

Smeets, Max. “A Matter of Time: On the Transitory Nature of Cyberweapons.” *Journal of Strategic Studies* 41, no. 1–2 (2018): 6–32.

———. “NATO Members’ Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis.” In *11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minarik, S. Alatulu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky, 163–78. Tallinn, Estonia: NATO CCD COE Publications, 2019.

———. “Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks.” In *9th International Conference on Cyber Conflict*, 1–18. Tallinn, Estonia: NATO CCD COE Publications, 2017.

Smeets, Max, and Herbert S. Lin. “Offensive Cyber Capabilities: To What Ends?” In *10th International Conference on Cyber Conflict*, 55–72. Tallinn, Estonia: NATO CCD COE Publications, 2018.

Smith, David J. “‘Woe from Stones’: Commemoration, Identity Politics and Estonia’s War of Monuments.” *Journal of Baltic Studies* 39, no. 4 (2008): 419–30.

Snyder, Jack. *Ideology of the Offensive: Military Decision Making and the Disasters of 1914*. Ithaca: Cornell University Press, 1984.

Sonmez, Felicia. “Leon Panetta, CIA Director, Unanimously Confirmed by Senate as Defense Secretary.” *Washington Post*, June 21, 2011.

https://www.washingtonpost.com/national/national-security/leon-panetta-cia-director-unanimously-confirmed-by-senate-as-defense-secretary/2011/06/21/AGajizeH_story.html.

Sorsa, Virpi, and Eero Vaara. “How Can Pluralistic Organizations Proceed with Strategic Change? A Processual Account of Rhetorical Contestation, Convergence, and Partial Agreement in a Nordic City Organization.” *Organization Science*, 2020, 1–26. https://doi.org/10.1287/orsc.2019.1332.

Spee, Paul, and Paula Jarzabkowski. “Agreeing on What? Creating Joint Accounts of Strategic Change.” *Organization Science* 28, no. 1 (2017): 152–76.

“Statement by Dr. Craig Fields and Dr. Jim Miller, Defense Science Board, Statement before the Armed Services Committee, United States Senate: Cyber Deterrence.” U.S. Senate Committee on Armed Services, March 2, 2017. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3694484-Document-09-Dr-Craig-Fields-and-Dr-Jim-Miller.

“Statement of Admiral Michael S. Rogers, Commander United States Cyber Command.” Testimony. Washington, D.C.: U.S. Senate, May 9, 2017. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3728886-Admiral-Michael-S-Rogers-Commander-United-States.

“Statement of Admiral Michael S. Rogers, Commander United States Cyber Command, before the Senate Committee on Armed Services.” U.S. Senate Committee on Armed Services, May 9, 2017. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3728886-Admiral-Michael-S-Rogers-Commander-United-States.

“Statement of Genernal Paul M. Nakasone, Command United States Cyber Command before the Senate Committee on Armed Services.” Testimony. Washington, D.C.: U.S. Senate Committee on Armed Services, February 14, 2016. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

Stulberg, Adam N., Austin Long, and Michael D. Salomone. *Managing Defense Transformation: Agency, Culture and Service Change*. London: Routledge, 2007.

Sutcliffe, Kathleen M. “High Reliability Organizations (HROs).” *Best Pract Res Clin Anaesthesiol* 25, no. 2 (June 2011): 133–44.

Temple-Raston, Dina. “How the U.S. Hacked ISIS.” *National Public Radio*, September 26, 2019. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

———. “Task Force Takes on Russian Election Interference.” *National Public Radio*, August 14, 2019. https://www.npr.org/2019/08/14/751048230/new-nsa-task-force-takes-on-russian-election-interference.

Teorell, Jan, Michael Coppedge, Staffan Lindberg, and Svend-Erik Skaaning. “Measuring Polyarchy Across the Globe, 1900-2017.” *Studies in Comparative International Development* 54 (2019): 71–95.

Terriff, Terry, and Frans Osinga. “Conclusion: The Diffusion of Military Transformation to European Militaries.” In *A Transformation Gap? American Innovations and European Military Change*, edited by Terry Terriff, Frans Osinga, and Theo Farrell, 187–209. Stanford, California: Stanford University Press, 2010.

Terriff, Terry, Frans Osinga, and Theo Farrell, eds. *A Transformation Gap? American Innovations and European Military Change*. Stanford, California: Stanford University Press, 2010.

The Federal Government of Germany. “White Paper 2016 on German Security Policy and the Future of the Bundeswehr.” The Federal Government of Germany, July 13, 2016. https://www.dsn.gob.es/sites/dsn/files/2016_German_WhitePaper_SecurityPolicy_13jul2016.pdf.

The World Bank. “World Development Indicators.” Washington, D.C.: The World Bank, 2018.

Thelen, Kathleen. “How Institutions Evolve: Insights from Comparative Historical Analysis.” In *Comparative Historical Analysis in the Social Sciences*, edited by James Mahoney and Dietrich Rueschemeyer, 208–40. Cambridge University Press, 2003.

Tibshirani, Robert. “The Lasso Method for Variable Selection in the Cox Model.” *Statistics in Medicine* 16 (1997): 385–95.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. “International Cyber Incidents: Legal Considerations.” Cooperative Cyber Defence Centre of Exellence, 2010. https://ccdcoe.org/publications/books/legalconsiderations.pdf.

Toomse, Rene. “Small States’ Special Operations Forces in Preemptive Strategic Development Operations: Proposed Doctrine for Estonian Special Operations Forces.” *Special Operations Journal* 1, no. 1 (2015): 44–61.

Tsai, K. -H., and J. -C. Wang. “Does R&D Performance Decline with Firm Size? A Re-Examination in Terms of Elasticity.” *Research Policy* 34 (2005): 966–76.

Tushman, M. L., and C. A. O’Reilly. *Winning through Innovation: A Practical Guide to Leading Organizational Change and Renewal*. Cambridge, MA: Harvard Business School Press, 1997.

United States Congress. Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99–433 (1986). https://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf.

———. National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114–328 (2016). https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf.

United States Cyber Command Fusion Cell. “Situational Awareness Report 2010-SA-0025: WikiLeaks Release of Classified Documents from a Department of State Database.” United States Strategic Command, December 2, 2010. The National Security Archive. https://nsarchive2.gwu.edu//dc.html?doc=6792855-National-Security-Archive-United-States.

United States Department of Defense. “Agreed Operation Glowing Symphony Notification Plan,” November 4, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638021-Department-of-Defense-Agreed-Operation-Glowing.

———. “All Cyber Mission Force Teams Achieve Initial Operating Capability,” October 24, 2016. https://www.defense.gov/Explore/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/.

———. “Department of Defense Strategy for Operating in Cyberspace.” Washington, D.C.: United States Government, July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

———. “Report of the 2006 Quadrennial Defense Review.” Quadrennial Defense Review. Washington, D.C.: United States Government, February 6, 2006. https://archive.defense.gov/pubs/pdfs/QDR20060203.pdf.

———. “Report of the 2010 Quadrennial Defense Review.” Quadrennial Defense Review. Washington, D.C.: United States Government, February 2010. https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf.

———. “Report of the 2014 Quadrennial Defense Review.” Quadrennial Defense Review. Washington, D.C.: United States Government, March 4, 2014. https://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

———. “Summary: Department of Defense Cyber Strategy,” 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

———. “Summary of the 2018 National Defense Strategy of the United States of America,” January 19, 2018. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=4421221-Defense-Department-Summary-of-the-2018-National.

———. “The DOD Cyber Strategy.” Washington, D.C.: United States Government, April 2015. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

United States Department of Defense Science Board. “Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence,” February 2017. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3515021-Document-07-Defense-Science-Task-Board-Final.

United States Government. “National Security Presidential Directive (NSPD-54)/Homeland Security Presidential Directive (HSPD)-23,” January 8, 2008. https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

———. “National Security Strategy of the United States,” December 2017. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=4421220-The-White-House-National-Security-Strategy-of.

———. “Statement by President Donald J. Trump on the Elevation of Cyber Command,” August 18, 2017. https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

———. “The National Strategy to Secure Cyberspace.” Washington, D.C.: United States Government, February 2003. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=2700096-Document-16.

United States Government Accountability Office. “DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force.” Washington, D.C.: United States Government Accountability Office, March 2019. https://www.gao.gov/assets/700/697268.pdf.

———. “Military Transformation: Additional Actions Needed by U.S. Strategic Command to Strengthen Implementation of Its Many Missions and New Organization.” Report to the Subcommittee on Strategic Forces, Committee on Armed Services, House of Representatives. Washington, D.C.: United States Government Accountability Office, September 2006.

United States Space Command (USSPACECOM). “United States Space Command (USSPACECOM) Concept of Operations (CONOPS) For Computer Network Defense (CND).” Colorado: United States Government, October 1, 1999. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3131435-Document-03.

United States Strategic Command. “CDRUSSTRATCOM CONPLAN 8039-08 (U).” Offutt Air Base, NE: United States Government, February 28, 2008. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4356235-United-States-Strategic-Command-CDRUSSTRATCOM.

———. "FRAGORD 06 to USSTRATCOM OPORD 8000-17: Authorization to Conduct Operation GLOWING SYMPHONY," November 8, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638023-USSTRATCOM-Subj-FRAGORD-06-to-USSTRATCOM-OPORD.

———. "USCYBERCOM Announcement Message," May 21, 2010. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=2692108-Document-6.

U.S. Admiral (ret.) Michael Rogers interview with author. Interview by Jason Blessing. Tallinn, Estonia, May 27, 2019.

U.S. Air Force. "Air Force Art: Strategic Air Command (SAC) Shield (Color)," n.d. https://www.af.mil/News/Art/igphoto/2000639834/.

———. "Air Force Secretary Announces Provisional Cyber Command," September 19, 2007. https://www.af.mil/News/Article-Display/Article/125683/air-force-secretary-announces-provisional-cyber-command/.

———. "Michael W. Wynne," June 2008. https://www.af.mil/About-Us/Biographies/Display/Article/107896/michael-w-wynne/.

———. "New SECAF Sends 'Letter to Airmen,'" November 3, 2005. https://www.af.mil/News/Article-Display/Article/132876/new-secaf-sends-letter-to-airmen/.

U.S. Air Force/U.S. Cyber Command Consultant interview with author. Interview by Jason Blessing. Washington, D.C., March 12, 2019.

U.S. Army Major embedded in German Cyber and Information Domain Service interview with author. Interview by Jason Blessing. Telephone, August 20, 2019.

U.S. Cyber Command. "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," March 23, 2018. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=4421219-United-States-Cyber-Command-Achieve-and-Maintain.

———. "Beyond the Build: Delivering Outcomes through Cyberspace - The Commander's Vision and Guidance for US Cyber Command." Fort Meade, MD: United States Government, June 3, 2015. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=2692135-Document-27.

———. "Cyber Mission Force Training and Cyber Flag Update." Briefing. United States Government, October 22, 2013. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=5977841-National-Security-Archive-USCYBERCOM-Cyber#p21.

———. "CYBERCOM FRAGORD 01 to TASKORD 16-0063 To Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space," May 5, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3678213-Document-07-USCYBERCOM-to-CDRUSACYBER-Subj#document/p23.

———. "How Understanding Cyberspace as a Strategic Environment Should Drive Cyber Capabilities and Operations," November 30, 2016. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=6560991-National-Security-Archive-2-USCYBERCOM-How.

———. "Mission Analysis Brief: Cyber Support to Counter ISIL." Briefing. United States Government, April 12, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4311638-United-States-Cyber-Command-Mission-Analysis.

———. "U.S. Cyber Command History." Accessed July 13, 2019. https://www.cybercom.mil/About/History/.

———. "USCYBERCOM GENADMIN 16-0210 OPERATION GLOWING SYMPHONY," December 10, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638026-USCYBERCOM-to-USSTRATCOM-USCENTCOM-and-The.

———. "USCYBERCOM GENADMIN 17-0093 EXTENSION OF OPERATION GLOWING SYMPHONY," July 1, 2017. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638027-USCYBERCOM-Subj-USCYBERCOM-GENADMIN-17-0093.

———. "USCYBERCOM Operations Order (OPORD) 15-0055: Operations Order in Support of Operation Inherent Resolve," March 29, 2015. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=5751043-National-Security-Archive-COS-MEMO-11-FEB-19.

———. "USCYBERCOM OPORD 16-0188 OPERATION GLOWING SYMPHONY (OGS)," November 9, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638024-USCYBERCOM-Subject-USCYBERCOM-OPORD-16-0188.

U.S. Department of Defense. "DOD News Briefing on Mistaken Shipment to Taiwan with Secretary of Air Force Wynne, Lt. Gen. Ham and Principal Deputy Undersecretary Henry," March 28, 2008. https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=4179.

———. "DOD News Briefing with Secretary Gates from the Pentagon," June 5, 2008. https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=4236.

———. “Remarks to Air War College (Montgomery Alabama),” April 21, 2008. https://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1231.

U.S. House of Representatives Committee on Armed Services. “Implementing the Department of Defense Cyber Strategy,” September 30, 2015. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=3114903-Document-09.

U.S. Military Joint Chiefs of Staff. “Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.” U.S. Department of Defense, April 12, 2001.

———. “Joint Publication 3-12 (R), Cyberspace Operations,” February 5, 2013. The National Security Archive. https://nsarchive.gwu.edu/dc.html?doc=2692126-Document-18.

———. “The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow.” Washington, D.C.: United States Government, 2004. https://history.defense.gov/Portals/70/Documents/nms/nms2004.pdf?ver=2014-06-25-123447-627.

U.S. Subject Matter Expert #2 interview with author. Interview by Blessing Jason. Telephone, March 19, 2019.

USCYBERCOM JTF-ARES. “C-2 Mission Checklist - Operation GLOWING SYMPHONY (V11),” November 7, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638022-USCYBERCOM-JTF-ARES-C-2-Mission-Checklist.

———. “In Progress Review OP Glowing Symphony [Redacted],” October 7, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638020-USCYBERCOM-JTF-ARES-In-Progress-Review-OP.

———. “JTF-ARES: Operation Glowing Symphony,” November 10, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638025-USCYBERCOM-JTF-ARES-JTF-ARES-Operation-Glowing.

———. “Operation GLOWING SYMPHONY Overview,” September 16, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638019-USCYBERCOM-JTF-ARES-Operation-GLOWING-SYMPHONY.

———. “United States Cyber Command Concept of Operations - OPERATION GLOWING SYMPHONY,” September 13, 2016. The National Security Archive. https://nsarchive2.gwu.edu/dc.html?doc=4638018-USCYBERCOM-JTF-ARES-United-States-Cyber-Command.

Vaccaro, I. G., J. J. Jansen, T. Keil, and S. A. Zahra. “Management Innovation and Leadership: The Moderating Role of Organizational Size.” *Journal of Management Studies* 49, no. 1 (2012): 28–51.

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

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

———. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011." *Journal of Peace Research* 51, no. 3 (2014): 347–60.

Vavra, Shannon. "NSA's Russian Cyberthreat Task Force Is Now Permanent." *Cyberscoop*, April 19, 2019. https://www.cyberscoop.com/nsa-russia-small-group-cyber-command/.

Vennesson, Pascal. "Institution and Airpower: The Making of the French Air Force." *Journal of Strategic Studies* 18, no. 1 (1995): 36–67.

Vittinghoff, Eric, and Charles E. McCulloch. "Relaxing the Rule of Ten Events per Variable in Logistic and Cox Regression." *American Journal of Epidemiology* 165, no. 6 (2007): 710–18.

Volden, C. "States as Policy Laboratories: Emulating Success in the Children's Health Insurance Program." *American Journal of Political Science* 50, no. 2 (2006): 294–312.

Waldner, David. "What Makes Process Tracing Good?: Causal Mechanisms, Causal Inference, and the Completeness Standard in Comparative Politics." In *Process Tracing: From Metaphor to Analytic Tool*, edited by Andrew Bennett and Jeffrey T. Checkel, 126–52. Cambridge, United Kingdom: Cambridge University Press, 2015.

Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal* 3 (2011): 85–142.

Warner, Michael. "US Cyber Command's Road to Full Operational Capability." In *Stand Up and Fight: The Creation of US Security Organizations, 1942-2005*, edited by Ty Seidule and Jacqueline E. Whitt, 119–38. Carlisle, PA: Army War College Strategic Studies Institute, 2015.

Webster, Kaitlyn. "Rethinking Civil War." Dissertation, Duke University, 2019.

Weick, Karl E. "Organizational Culture as a Source of High Reliability." *California Management Review* 29, no. 2 (1987): 112–27.

Weick, Karl E., and Robert E. Quinn. "Organizational Change and Development." *Annual Review of Psychology* 50 (1999): 361–86.

Weinert, B. "Integrating Models of Diffusion of Innovations: A Conceptual Framework." *Annual Review of Sociology* 28 (2002): 297–326.

Weiss, Moritz, and Vytautas Jankauskas. "Securing Cyberspace: How States Design Governance Arrangements." *Governance*, 2018, 1–17.

Weyland, Kurt. *Bounded Rationality and Policy Diffusion: Social Sector Reform in Latin America*. Princeton, New Jersey: Princeton University Press, 2009.

White, Ian R., Patrick Royston, and Angela M. Wood. "Multiple Imputation Using Chained Equations: Issues and Guidance for Practice." *Statistics in Medicine* 30 (2011): 377–99.

White, Sarah P. "Subcultural Influence on Military Innovation: The Developmentof U.S. Military Cyber Doctrine." Dissertation, Harvard University, 2019.

Whyte, Christopher, Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness. "Rethinking the Data Wheel: Automating Open-Access, Public Data on Cyber Conflict." In *CyCon X: Maximising Effects*, 9–30. Tallinn, Estonia: NATO CCD COE Publications, 2018.

Wiener, Craig J. "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation." Doctoral Dissertation, George Mason University, 2016.

Wivel, Anders, and Matthew Crandall. "Punching Above Their Weight, but Why? Explaining Denmark and Estonia in the Transatlantic Relationship." *Journal of Transatlantic Studies* 17 (2019): 392–419.

Wolfe, Richard A. "Organizational Innovation: Review, Critique and Suggested Research Directions." *Journal of Management Studies* 31 (1994): 405–31.

Wreede, Liesbeth C. de, Marta Fiocco, and Hein Putter. "The Mstate Package for Estimation and Prediction in Non- and Semi-Parametric Multi-State and Competing Risks Models." *Computer Methods and Programs in Biomedicine* 99, no. 3 (2010): 261–74.

Wuthnow, Joel. "A Brave New World for Chinese Joint Operations." *Journal of Strategic Studies* 40, no. 1–2 (2017): 169–95.

Wynne, Michael. "Cyberspace as a Domain in Which the Air Force Flies and Fights." Presented at the C4ISR Integration Conference, Crystal City, VA, November 2, 2006. http://www.iwar.org.uk/iwar/resources/cybercommand/speech.htm.

———. "Letter to the Airmen of the United States." United States Air Force, December 7, 2005.

Yin, R. K. "Changing Urban Bureaucracies: How New Practices Become Routinized." Santa Monica, CA: RAND Corporation, 1978.

Young, Thomas-Durell. "Cooperative Diffusion through Cultural Similarity: The Postwar Anglo-Saxon Experience." In *The Diffusion of Military Technology and Ideas*, edited by

Emily O. Goldman and Leslie C. Eliason, 93–113. Stanford, California: Stanford University Press, 2003.

Zaltman, G., R. Duncan, and J. Holbek. *Innovations and Organizations*. New York: Wiley, 1973.

Zhou, K. Z., and C. B. Li. "How Strategic Orientations Influence the Building of Dynamic Capability in Emerging Economies." *Journal of Business Research* 53, no. 3 (2010): 224–31.

Zisk, Kimberly Marten. *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955-1991*. Princeton, New Jersey: Princeton University Press, 1993.

Zmud, Robert W. "An Examination of 'Push-Pull' Theory Applied to Process Innovation in Knowledge Work." *Management Science* 30 (1984): 727–38.

JASON BLESSING

United States Institute of Peace, Washington, D.C. 20037
Maxwell School of Citizenship and Public Affairs, Syracuse University, Syracuse NY 13204
jablessi@syr.edu | Phone available upon request | www.jason-blessing.com

EDUCATION

2015 – 2020 **Syracuse University**, Syracuse, NY
Ph.D., Political Science
Subfields: International Relations and Public Policy

2011 – 2013 **Virginia Polytechnic Institute and State University**, Blacksburg, VA
M.A. in Political Science

2007 – 2011 **The College of William and Mary**, Williamsburg, VA
B.A. in Government

FELLOWSHIPS

2020 – 2021 **DAAD Post-Doctoral Fellow**
Foreign Policy Institute, Johns Hopkins University School of Advanced International Studies, Washington, D.C. (Offer Accepted March 2020).

2019 – 2020 **USIP-Minerva Peace and Security Scholar**
Jennings Randolph Peace Scholar Dissertation Fellowship Program
United States Institute of Peace, Washington, D.C.

RESEARCH

Book Project

"The Diffusion of Cyber Forces: Military Innovation and the Dynamic Implementation of Cyber Force Structure."

Works in Progress

"The Diffusion of Cyber Forces, 2000-2018."

"Estonia's Road to Cyber Command."

"An Introduction to the Dataset on Cyber Force Structures (DCFS), 2000-2018."

"Implementing Military Innovations: A Stage-Based Process."

Conference Papers/Reports

"The Determinants of Military Organization for Cyber-Defense." Paper presented at the 2019 Annual American Political Science Association Conference.

“The Rhetoric of White Supremacist Terror: Assessing the Attribution of Threat.” Co-authored with Elise Roberts. Research report for The Andrew Berlin Family National Security Research Fund at The Institute for Security Policy and Law, Syracuse University.

Master’s Thesis

“From ‘Total Liberation’ to ‘Phased Liberation’: Temporality and Identity in the Provisional IRA and Hamas.”

GRANTS AND ACADEMIC AWARDS

2020 – 2021	DAAD Post-Doctoral Fellowship, Foreign Policy Institute, Johns Hopkins University School of Advanced International Studies. (Offer Accepted March 2020)
2019 – 2020	Jennings Randolph Peace Scholar Dissertation Fellowship, United States Institute of Peace.
2019	Summer Research Grant, Department of Political Science, Syracuse University, $1400 for dissertation research.
2019	Perryman Summer Research Grant, The Maxwell School for Citizenship and Public Affairs, $1200 for dissertation fieldwork.
2018	The Roscoe Martin Fund, The Maxwell School for Citizenship and Public Affairs, $1,200 for dissertation fieldwork.
2018	The Andrew Berlin Family National Security Fund, The Institute for Security Policy and Law, $5000 for dissertation fieldwork.
2018	Summer Fellowship, Political Science, Syracuse University, $4,000 for dissertation research.
2016	Global Black Spots Research Program, Moynihan Institute of Global Affairs, Syracuse University, $1000 for co-authored project with Elise Roberts.
2016	The Andrew Berlin Family National Security Fund, The Institute for Security Policy and Law, $1400 for co-authored project with Elise Roberts.
2016	The Andrew Berlin Family National Security Fund, The Institute for Security Policy and Law, $3500 for co-authored project with Elise Roberts.

2013	Best M.A. Thesis Award, Political Science, Virginia Tech.
2012 – 2013	Graduate Fellowship Award, $500, Virginia Tech.
2012	Outstanding First Year Student Award, Virginia Tech
2007 – 2011	State Masonic Lodge of Virginia Scholarship

PROFESSIONAL ACTIVITIES

2019	American Political Science Association (APSA) Annual Meeting, Washington D.C. "The Determinants of Military Organization for Cyber-Defense," paper presented at panel.
2019	International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.
2018 – 2019	Junior Scholar, Carnegie International Policy Scholars Consortium and Network, Henry A. Kissinger Center for Global Affairs, Johns Hopkins University School of Advanced International Studies
2018 – 2019	Future Professoriate Program, Syracuse University
2015 – Present	Student Association on Terrorism & Security Analysis (SATSA), Syracuse University
2015 – 2016	Bridging the Gap Working Group, Syracuse University
2013	Midwest Political Science Association (MPSA) Conference, Chicago, IL “Combatting the Financing of Terrorism: Assessing the International Monetary Fund’s Approach in Lebanon,” panel paper co-authored with William Christiansen.
2012	Midwest Political Science Association (MPSA) Conference, Chicago, IL “American Democracy and Voter Perception: Do Political Action Committees Influence Perceived Political Power?” poster session with William Christiansen, Lauren Crandall, and Alison Higgins

TEACHING EXPERIENCE

2015 – 2019	**Graduate Teaching Assistant** *Syracuse University, Syracuse, NY* Introduction to International Relations Constitutional Law The Politics of U.S. Public Policy The Judicial Process U.S. Foreign Policy

2011 – 2013	**Graduate Teaching Assistant** *Virginia Polytechnic Institute and State University, Blacksburg, VA* The Global Economy and World Politics Introduction to World Politics
2012	**Instructor of Record** *Virginia Polytechnic Institute and State University, Blacksburg, VA* Introduction to U.S. Government and Politics

EMPLOYMENT HISTORY

2019 – Present	**United States Institute of Peace**, Washington, D.C. *USIP-Minerva Peace and Security Scholar*
2015 – 2019	**Syracuse University**, Syracuse, NY *Graduate Teaching Assistant*
2018	**Qualitative Data Repository**, Syracuse, NY *Graduate Research Assistant*
2013 – 2015	**E*TRADE Financial Corporation**, Alpharetta, GA *Fraud Operations Analyst* *Financial Services Representative*
2011 – 2013	**Virginia Polytechnic Institute and State University**, Blacksburg, VA *Graduate Teaching Assistant* *Instructor*

LICENSES

Series 99 Securities License, FINRA, September 2014
Series 63 Securities License, NASAA, October 2013
Series 7 Securities License, FINRA, October 2013

LANGUAGE COURSEWORK

English – native language
Arabic – 5 semesters of Modern Standard Arabic, 1 semester of Iraqi Dialect
Spanish – 6 semesters