2023-12

BEST PRACTICES TO CONSIDER WHEN BUILDING A NATIONAL CIVIL RESERVE CYBER FORCE (CRCF) FRAMEWORK

Kroeller, Brian J.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BEST PRACTICES TO CONSIDER WHEN BUILDING A NATIONAL CIVIL RESERVE CYBER FORCE (CRCF) FRAMEWORK

by

Brian J. Kroeller

December 2023

Co-Advisors: Shannon A. Brown
Cristiana Matei

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE BEST PRACTICES TO CONSIDER WHEN BUILDING A NATIONAL CIVIL RESERVE CYBER FORCE (CRCF) FRAMEWORK	**5. FUNDING NUMBERS**
6. AUTHOR(S) Brian J. Kroeller	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Within an era marked by escalating cyber threats to American critical infrastructure and an alarming shortage of cybersecurity professionals, this thesis explores the feasibility and structure of a Civilian Reserve Cyber Force (CRCF). Drawing inspiration from an array of established models, the research highlights existing best practices such as the National Guard's organizational prowess, the Civil Reserve Air Fleets' benchmark public/private synergies, the State Defense Force's exceptional history of volunteerism, and the United States Space Forces' forward-thinking digital strategies. Mirroring international best practices, Estonia's comprehensive digital citizen initiative and strong North Atlantic Treaty Organization partnerships shores up its robust national cyber defense, while the UK's Cyber Reserves model exemplifies the successful melding of civilian expertise into military cyber operations. By synthesizing these elements, the thesis concludes with best practices among all the presented organizations along with recommended future research in the form of a provisional CRCF Concept of Operations table of contents, offering both a visionary blueprint for future cyber defense and a strategic roadmap to navigate potential pitfalls. The findings advocate for a holistic integration of proven strategies from domestic and global models, championing a unified, robust, and proactive CRCF to safeguard future American cyber interests.

14. SUBJECT TERMS cyber, homeland security, policy, S. 1324, H.R. 2894, civil cyber reserve, Civilian Reserve Cyber Force, CRCF	**15. NUMBER OF PAGES** 123
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

BEST PRACTICES TO CONSIDER WHEN BUILDING A NATIONAL CIVIL RESERVE CYBER FORCE (CRCF) FRAMEWORK

Brian J. Kroeller
Lieutenant Colonel, United States Air Force
BA, Lindenwood University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Approved by: Shannon A. Brown
Co-Advisor

Cristiana Matei
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Within an era marked by escalating cyber threats to American critical infrastructure and an alarming shortage of cybersecurity professionals, this thesis explores the feasibility and structure of a Civilian Reserve Cyber Force (CRCF). Drawing inspiration from an array of established models, the research highlights existing best practices such as the National Guard's organizational prowess, the Civil Reserve Air Fleets' benchmark public/ private synergies, the State Defense Force's exceptional history of volunteerism, and the United States Space Forces' forward-thinking digital strategies. Mirroring international best practices, Estonia's comprehensive digital citizen initiative and strong North Atlantic Treaty Organization partnerships shores up its robust national cyber defense, while the UK's Cyber Reserves model exemplifies the successful melding of civilian expertise into military cyber operations. By synthesizing these elements, the thesis concludes with best practices among all the presented organizations along with recommended future research in the form of a provisional CRCF Concept of Operations table of contents, offering both a visionary blueprint for future cyber defense and a strategic roadmap to navigate potential pitfalls. The findings advocate for a holistic integration of proven strategies from domestic and global models, championing a unified, robust, and proactive CRCF to safeguard future American cyber interests.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMC	Air Mobility Command
APHSCT	Assistant to the President for Homeland Security and Counterterrorism
AWS	Amazon Web Services
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDU	Cyber Defence Unit
CERIAS	Center for Education and Research in Information Assurance and Security
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COG	Cyber Operations Squadron
CONOPS	Concept of Operations
COS	Cyber Operations Squadron
CRAF	Civil Reserve Air Fleet
CRCF	Civil Reserve Cyber Force
CRF	Cyber Reserve Force
CRG	Cyber Response Group
CRS	Congressional Research Service
CSC	Cyberspace Solarium Commission
CSIS	Center for Strategic and International Studies
CTIIC	Cyber Threat Intelligence Integration Center
CYBERCOM	Cyber Command
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIU	Defense Innovation Unit
DOD	Department of Defense
DOJ	Department of Justice

DOT	Department of Transportation
DPA	Defense Production Act
EDL	Estonian Defence League
EDL-CDU	Estonian Defence League-Cyber Defence Unit
EMAC	Emergency Management Assistance Compact
EO	Executive Order
FBI	Federal Bureau of Investigation
FCEB	Federal Civilian Executive Branch
FEMA	Federal Emergency Management Agency
GAO	Government Accountability Office
H4D	Hacking for Defense
ICOAST	Intelligence Community Analysis and Signature Tool
ISAC	Information Sharing and Analysis Centers
IT	Information Technology
JCDC	Joint Cyber Defense Collaborative
JEDI	Joint Enterprise Defense Infrastructure
JFHQ-DODIN	Joint Force Headquarters-DOD Information Network
KPI	Key Performance Indicators
KSA	Knowledge, Skills, and Abilities
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center
NCFTA	National Cyber Forensics and Training Alliance
NCIJTF	National Cyber Investigative Joint Task Force
NDS	National Defense Strategy
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OhCR	Ohio Cyber Reserve

OPM	Office of Personnel Management
PPD	Presidential Policy Directive
PRC	People's Republic of China
RIA	Information Systems Authority (Estonia)
RSD	Reserve Service Day
SCADA	Supervisory Control and Data Acquisition
SDF	State Defense Force
SISA	State Information Systems Authority
SPP	State Partnership Program
STEM	Science, Technology, Engineering, and Mathematics
TTP	Tactics, Techniques, and Procedures
UCG	Unified Cyber Coordination Group
UK	United Kingdom
USSF	United States Space Force
USTRANSCOM	United States Transportation Command

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis examines the concept of establishing a Civilian Reserve Cyber Force (CRCF) in the United States, a strategic response to the escalating cyber threats targeting critical infrastructure amid a growing shortage of cybersecurity professionals. Drawing on established models like the National Guard, Civil Reserve Air Fleet (CRAF), State Defense Force (SDF), United States Space Force (USSF), and international examples from the UK and Estonia, the paper's research aims to offer a comprehensive blueprint for integrating civilian expertise into a future national cyber defense strategy.

The underlying challenges are discussed, and the thesis underscores the urgency of addressing cybersecurity issues, particularly against critical infrastructure. A hypothetical scenario is presented, depicting a major power grid disruption in the northeastern United States. This scenario serves as a realistic illustration of the vulnerabilities and potential impacts of cyber threats on essential services and the general populace. It emphasizes the dire need for a CRCF capable of preemptive response to such technological advancements and threats. The scenario narrative acts as a connective tissue of sorts between real-world examples of previous cyberattacks and the potential, innovative approaches for the creation of a CRCF; the importance of staying ahead of rapid technological advancements is highlighted, as is the need to seamlessly integrate the CRCF into the nation's defense mechanisms. Building upon the identified challenges, the research employs a qualitative methodology to analyze various models. Data is gathered from policy documents, case studies, and current literature on cybersecurity and national defense strategies. The focus is on extracting key insights from these models to inform the proposed CRCF framework. This approach ensures a comprehensive understanding of existing models and their applicability to the CRCF.

The research also emphasizes the need for a balanced approach in the CRCF that respects constitutional principles while effectively serving national security objectives. The potential of the CRAF as a public-private partnership framework is particularly highlighted. This organizational model is suggested as a strategic cyber deterrent and a blueprint for participant compensation within the CRCF. The organizational elements of

the CRAF, such as legislative aspects, private-public sectors collaboration, and severity levels, are proposed as offering insurance-like protections in the cyber domain. Furthermore, while building on these findings, the SDF is identified as a key model for talent retention within the CRCF. The SDF's low-cost, volunteer-driven structure makes it a compelling option, presenting critical attributes that could significantly bolster the CRCF's structure and efficacy. This framework offers essential elements for a future CRCF mission and presents an alternative to a nationally controlled line of effort. The National Guard's community-centric model provides a bridge between civilian aspirations and national defense needs, allowing civilians to align their personal and professional goals with broader national security objectives. Its presence in virtually every zip code facilitates a distributed and financially efficient structure, suitable for CRCF members to operate as "cyber nomads." Additionally, the National Guard's dual-militia construct offers accumulated cyber experience and successful retention of civilian expertise, enhancing cybersecurity capabilities. In contrast to the traditional models discussed, the thesis highlights the USSF as an emerging framework for the information age. The USSF, with its forward-looking digital philosophy and adaptability, offers invaluable insights for crafting the CRCF as a digitally-centric, agile entity. This adaptability is crucial for a CRCF designed to meet the dynamic challenges of cybersecurity.

In addition to American organizational models, the thesis also explores international civilian-based cyber forces from Estonia and the UK. These examples were selected for their commendable fusion of public-private sectors and rounded governmental strategies within Western-style democracies. These nations exhibit strong approaches to treating cyberattacks as significant threats to their national security. Estonia, with its comprehensive digital citizen initiative and strong NATO partnerships, shores up its robust national cyber defense. The UK's Cyber Reserves model exemplifies the successful melding of civilian expertise into military cyber operations. These international case studies offer invaluable lessons and potential hybrid strategies that can further inform and refine the American CRCF blueprint.

The overall thesis conclusion advocates for the holistic integration of these diverse strategies, championing a unified, robust, and proactive CRCF to safeguard future

American cyber interests. The proposed CRCF framework offers a visionary blueprint for future cyber defenses and a strategic roadmap to navigate potential challenges. The thesis concludes with a call for further research focusing on operational structure, long-term sustainability, and the integration of best practices among all the presented organizations. The importance of adaptability, volunteerism, public-private partnerships, and technological agility in creating a resilient and effective cyber reserve force cannot be understated. Overall, this comprehensive roadmap is poised to prepare the United States to meet both current and future cyber defense challenges, ensuring robust and agile twenty-first century national cybersecurity.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I extend my deepest gratitude to my wife, Crystal. Your unwavering support and understanding during my military career is the foundation upon which this endeavor was built. To my kids, Aubrey and Maxwell: thank you for being the constant source of motivation and light during this difficult journey.

I am indebted to my senior leadership, especially Colonel David Christensen, for providing me with the flexibility to balance my responsibilities as an Air National Guard Commander while pursuing this degree. A special thank you goes out to our unit's senior enlisted leader CMSgt. Bollenbaugh for his patience and understanding during my frequent absences, and for valuing my academic pursuits as much as our shared professional goals.

Lastly, to my fellow classmates of Cohort 2203/04: Your camaraderie, mentorship, and encouragement was invaluable. Each one of you played a part in keeping me grounded and focused, and I am proud to have taken this journey alongside such dedicated and uplifting defenders of democracy.

THIS PAGE INTENTIONALLY LEFT BLANK

I. CHAPTER I – A CIVIL RESERVE CYBER FORCE FRAMEWORK PROPOSAL

A. PROBLEM STATEMENT

Cyberattacks in both the private and public sectors are growing. According to survey of Cybersecurity 202 Network members, eighty-one percent feel the United States is more vulnerable or just as vulnerable to cyberattacks as it was five years ago.[1] In 2021, North America saw an alarming 105 percent surge in ransomware cyberattacks, or attacks designed to render computer systems unusable until the company or owners pay a financial ransom to unlock their networks or files.[2] In addition to government networks, increasing cyberattacks threaten private sector operations across critical industries with close ties to government and the American economy.

As the cyber threat grows both in size and complexity, the United States has striven to organize its talent in the cyber sectors and chart a path for a nationwide unified cyber protection effort. Notwithstanding these endeavors, the overall shortfall of cyber expertise in the public and private sector poses a major threat to the United States. As of today, a lack of trained cyber experts makes it impossible to fill the vast array of needs across the government and private sectors.[3] Per the New America report titled *The Need for C3*, private companies and the government cannot fill just under 300,000 open cybersecurity positions in the United States.[4] Various reasons contribute to this deficiency, ranging from higher education's inability to shift from traditional technology qualifications to the

[1] Joseph Marks and Aaron Schaffer, "The U.S. Isn't Getting Ahead of the Cyber Threat, Experts Say," *Washington Post*, June 6, 2022, https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/.

[2] Ahiah Taylor, "There's a Huge Surge in Hackers Holding Data for Ransom, and Experts Want Everyone to Take These Steps," *Fortune*, February 17, 2022, https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/#:~:text=Governments.

[3] Natasha Cohen and Peter W. Singer, "The Need for C3," New America, October 25, 2018, http://newamerica.org/cybersecurity-initiative/reports/need-c3/.

[4] Cohen and Singer.

overwhelming surge in-demand within the cybersecurity sector.[5] Facing the same workforce and talent shortage in cybersecurity as the states, the Department of Defense (DOD), Department of Homeland Security (DHS), and other federal agencies often cannot provide direct assistance for cyber incidents affecting governmental networks.[6] The failure of government to quickly prepare, respond, and deter cyberattacks can have nationwide consequences on the financial, economic, and safety sectors that can affect hundreds of millions of citizens.

As a corrective measure, given that ongoing cyberattacks continued throughout 2021, a bipartisan group of lawmakers introduced legislation to create a "Civilian Cybersecurity Reserve" or Civilian Reserve Cyber Force (CRCF) to counter growing cybersecurity vulnerabilities across the public/private sector.[7] The Civilian Cybersecurity Reserve Act (S. 1324 and H.R. 2894, submitted in 2021 and currently in a committee review) envisions the CRCF as a large group of citizens with cyber experience organized through a government agency, working alongside government cyber experts in an augmented capacity and at the ready to defend American interests against large-scale cyberattacks. As of late 2023, neither chamber is advancing this legislation. If signed by the president and enacted in law, these bills authorize the DOD and DHS to each create a provisional CRCF within their agencies to address increased cyber threats facing the United States. Unfortunately, the bills do not provide detailed guidance on how this effort will be implemented, either in its organization or the recruiting and retention of its talent.

However, current frameworks exist in both government and in public-private partnerships, and model unique characteristics to ensure the CRCF's success. The Civil Reserve Air Fleet (CRAF) provides efficient use of a particular requirement during times of national emergency; the State Defense Forces (SDF) has the ability to retain talent

[5] Marc van Zadelhoff, "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It," *Harvard Business Review*, May 4, 2017, https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it.

[6] Heidi L. Huhn, "Defending Infrastructure against Cyber Attacks through Qualified Cybersecurity Professionals in the Federal Government: A Case Study," *ProQuest Dissertations and Theses* (dissertation, Capella University, 2020), 72, ProQuest.

[7] Jacky Rosen, "S.1324 – 117th Congress (2021-2022): Civilian Cybersecurity Reserve Act," Pub. L. No. S.1324, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/1324.

through volunteerism; the tried and true "citizen airman and soldier" militia construct of the National Guard; and the essential "digital age tenets" of the United States Space Force (USSF). Together, these frameworks can form the foundation of a CRCF model and offer a concept of operations based on historical successes in support of the latest congressional cyber legislation. Yet the biggest challenge in the formation of a CRCF is the talent shortage and how to best incentivize an industry with extremely high salary and in-demand skill sets, which three of the four frameworks discussed above (CRAF, National Guard, and USSF) can help a prospective CRCF overcome.

This thesis explores how a national CRCF could employ best practices, with current and emerging frameworks used to leverage cyber talent in the civilian sector in order to protect national networks and critical infrastructure before, during, and after a cyberattack. Whether enacted in law or created by a government agency, the historical cyber policy, potential frameworks, and unique lines of effort outlined provides potential options in standing up a future CRCF capability.

B. RESEARCH QUESTIONS

How can cyber threats today pose a risk to American critical infrastructure within its traditional instruments of national power (diplomatic, informational, military, and economical) and how has the legislative and executive branches addressed the problem?

What could a civilian cyber reserve capability and organizational roadmap look like if implemented by Congress and signed into law by the president?

If implemented, which best practices provide value-added organizational and operational benefit to a future CRCF in the United States?

C. LITERATURE REVIEW

The literature review explored different points of view and methods in deterring the vast increase of cyberattacks against American critical infrastructure, including the actions of Congress since President Clinton's 1998 Presidential Decision Directive 63 titled

Critical Infrastructure Protection.[8] The review continues to President Biden's *National Cybersecurity Strategy* in March 2023.[9] The sources combined federal cyber strategies along with peer-reviewed journal articles and master's theses on the past, current, and forecasted cyberattacks against government and private sector networks. The literature identified four primary root causes related to increased worldwide cyber risk: the frequency of reported cyberattacks by criminal entities and nation-states against government and the private sector, the failure of academia in keeping up and educating the cybersecurity establishment, and the challenges in retaining cyber talent and, the prospects of joint partnerships among the public and private sectors to find consensus on a way ahead.

Overall, this literature review found an overwhelming consensus among the cybersecurity enterprise on how to best identify the challenges and vulnerabilities, but they diverge on how to best mitigate the risk against future cyber threats.

1. Cyberattacks Are Exponentially Growing

Cyberattacks on private and public sectors are growing worldwide. In 2021, North America, and especially the United States, saw an alarming 105 percent surge in ransomware cyberattacks, or attacks designed to render computer systems unusable until the company or owners pay a financial ransom to unlock their networks or files.[10] More importantly, the increase in cyberattacks are attributed to both nation-state and criminal actors, greatly complicating the victim's ability to counter the threat. The abundance of literature in this review substantiates that both the Russian Federation and the People's Republic of China (PRC) pose the biggest cyber threat to American national security.[11]

---

[8] Scott T. Roper, "U.S. National Cyberstrategy and Critical Infrastructure: The Protection Mandate and Its Execution" (master's thesis, Naval Postgraduate School, 2013), 24, http://hdl.handle.net/10945/37703.

[9] Glenn S. Gerstell, "Biden's New Cyber Strategy Will Acknowledge an Essential Truth: Market Forces Aren't Enough," *Barrons*, February 26, 2023, https://www.barrons.com/articles/biden-new-cyber-strategy-market-forces-cybersecurity-51675459082.

[10] Ahiah Taylor, "There's a Huge Surge in Hackers Holding Data for Ransom, and Experts Want Everyone to Take These Steps," *Fortune*, February 17, 2022, https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/#:~:text=Governments.

[11] White House, "Fact Sheet: The Biden-Harris Administration's National Security Strategy," 2022, 3, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/.

Whether through traditional espionage techniques or disruption within the virtual public square, the evidence in open source literature on cyberattacks against the United States by Russia and the PRC are well documented.[12] In an article from the *Journal of Strategic Studies* titled "Fancy bears and digital trolls: Cyber strategy with a Russian twist," authors Benjamin Jensen, Brandon Valeriano, and Ryan Maness state, "Cyber operations have become a modern manifestation of political warfare."[13] They describe the techniques of nation-states and their use the digital domain to disrupt, degrade, and deny critical processes such as free speech and voting integrity. Each cyber adversary carries unique strategies and "digital fingerprints" to justify attacks in support of their cyber objectives. While Jensen, Valeriano, and Maness claim that Russia prefers agitation and distraction to sow discontent among the American populace, they assert that Russia has not yet unleashed their full capabilities against critical infrastructure.[14] In *Cyber War and Strategic Culture: The Russian Integration or Cyber Power into Grand Strategy*, Dr. James Wirtz explains that Russia's cyber power is part of its hybrid warfare model and is used to create "fog of war" scenarios during a major conflict against notable adversaries.[15] Fog of war scenarios can range from spoofing strategic command and control to sowing doubt in the integrity of secure computer networks.[16] Although some descriptions of Russia's cyber strategy differ on the definition of hybrid warfare, the consensus of the cited readings solidifies Russia's use of common tactics, techniques, and procedures (TTPs) from past conflicts and agree that the Russians have yet to demonstrate the full use of their cyber arsenal.

The scholarly reports covered in this review overwhelmingly agree that the PRC's approach to cyberattacks differ from the Russian Federation, especially in the fields of

[12] Lorena González-Manzano et al., "Identifying Key Relationships between Nation-State Cyberattacks and Geopolitical and Economic Factors: A Model," *Security and Communication Networks* 2022 (June 2022): 1, https://doi.org/10.1155/2022/5784674.

[13] Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist," *Journal of Strategic Studies* 42, no. 2 (February 2019): 212, https://doi.org/10.1080/01402390.2018.1559152.

[14] Jensen, Valeriano, and Maness, 229.

[15] John P. Sullivan and James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, 2015, 35, https://hdl.handle.net/10945/59143.

[16] Sullivan and Wirtz, 35.

espionage and attacks against federal agencies.[17] In the thesis "Three if by Internet: Exploring the Utility of a Hacker Militia," author Matthew O'Loughlin revealed that from 2015—with publicly admitted attacks on the Office of Personnel Management (OPM)—to the present day's persistent hacking attempts on the American defense sector, China's covert (and sometimes overt) appetite for cyber espionage against the United States is not slowing down.[18] The Center for Strategic and International Studies (CSIS) published significant cyber incidents—including hackers linked to the Chinese government—breaching at least six government networks and causing great concern among all levels of the U.S. government.[19] CSIS indicated that the majority of recently reviewed materials deemed the PRC as the number one threat to the United States over other countries such as Russia, Iran or the Democratic People's Republic of Korea (DPRK). Ian Simon's Naval Postgraduate School's thesis titled "Effectiveness of National Cyber Policy to Strengthen the Security and Resilience of Critical Infrastructure Against Cyber Attacks" aligns with the vast majority of scholarly articles and argues current cyber activity by Chinese actors pose a threat to multiple U.S. sectors, such as federal agencies and the defense industry.[20] Another book by Valeriano, Jensen, and Maness titled *Cyber Strategy: The Evolving Character of Power and Coercion* shows that China may be reducing its espionage lines of effort and focus more on domestic control and building strategic foundations to best protect Chinese sovereignty.[21] Regardless of each nation-state's long-term strategies, the cited examples describe the more traditional cyberattacks against multiple facets of critical U.S. networks, with many authors advising its readers on the negative impacts if not mitigated.

---

[17] Jensen, Valeriano, and Maness, "Fancy Bears and Digital Trolls," 213.

[18] Matthew S. O'Loughlin, "Three If By Internet: Exploring the Utility of a Hacker Militia" (master's thesis, Naval Postgraduate School, 2017), 21, http://hdl.handle.net/10945/53027.

[19] "Significant Cyber Incidents," Center for Strategic and International Studies, February 20, 2023, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[20] Ian G. Simon, "Effectiveness of National Cyber Policy to Strengthen the Security and Resilience of Critical Infrastructure Against Cyber Attacks" (master's thesis, Naval Postgraduate School, 2020), 63, http://hdl.handle.net/10945/66140.

[21] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018), 170, ProQuest.

A gap in the literature on cyberattacks at the local and state government levels existed until the topic of election integrity became commonplace among national media around 2018. Donald Norris's journal article titled "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity" states that although most peer-reviewed studies in local government cybersecurity occurred over the past twenty years, recent studies addressing cyberattacks on local and state government since 2019 have shed light on the seriousness of the problem.[22] Since 2019, multiple studies have addressed the hole in cybersecurity at the local government level. Ashlee Frandell and Mandy Freeney's journal article "Cybersecurity Threats in Local Government: A Sociotechnical Perspective" concluded that authorities need a combination of societal and technological responses to address cyberthreats at the managerial levels,[23] while Jay Kesan and Lingeng Zhang's study attempted to measure the monetary loss of personal data from cyberattacks.[24]

Regardless of the level of government, the consensus of the literature outlines the negative effects of nation-states or criminal intrusions into the American psyche, greatly disrupting vital government roles such as secure voting systems and overall trust between government and the American populace. The only contrarian view against this consensus is the opinion that cyber threats will continue to exist in a "grey zone" between cyber war and the cyber peace of plausible deniability, and never utilized as a true weapon of mass destruction.[25] Dominika Dziwisz of the University of Kraków further broke down the argument, defining the "grey zone" activities as below the threshold of armed aggression and stating that, because of this threat of uncontrollable escalation, that the world should

[22] Donald F. Norris et al., "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity," *Public Administration Review* 79, no. 6 (December 2019): 896, https://doi.org/10.1111/puar.13028.

[23] Ashlee Frandell and Mary Feeney, "Cybersecurity Threats in Local Government: A Sociotechnical Perspective," *The American Review of Public Administration* 52, no. 8 (November 2022): 535, https://doi.org/10.1177/02750740221125432.

[24] Jay P. Kesan and Linfeng Zhang, "An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures, and Cyber Losses," *IEEE Transactions on Emerging Topics in Computing* 9, no. 2 (April 2021): 594, https://doi.org/10.1109/TETC.2019.2915098.

[25] Dominika Dziwisz, "Cyber Pearl Harbor Is Not Coming Us Politics Between War and Peace," *Politeja* 4, no. 79 (2022): 112, ProQuest.

not be concerned of a "cyber Pearl Harbor" type of attack against the United States.[26] This point of view may ring true for the nation-state, but its logic may not work for the criminal entities, who are not concerned with the follow-on actions of the intended target.

2. Academia Struggling to Meet Demand/Lack of Cyber Talent in the Workforce

Empirical evidence over the past ten years affirms the lack of trained cyber experts currently available to fill the vast array of needs across the government and private sectors. Marc van Zadelhoff's *Harvard Business Review* article titled "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It" reported that by 2020, the field of cybersecurity is expected to have over 1.5 million vacancies[27] and the federal government's Chief Information Officer's (CIO) Council projects a shortage of 1.8 million cyber experts across the globe by 2022.[28] Van Zadelhoff claims that businesses are caught up in old-fashioned hiring practices, such as myopic views on the requirement of college degrees and traditional experience backgrounds instead of considering non-traditional backgrounds and fresh new ways of thinking.[29]

The scholarly articles from multiple countries outside the United States such as Australia and the United Kingdom (UK) also shared the same concerns as their American academic counterparts, substantiating the primary root cause of poorly protected worldwide networks.[30] Steven Furnell asserted the workforce shortages throughout the UK occur at both the entry and experienced levels, with Parliament stating shortages also exist throughout the critical infrastructure enterprise.[31] Furnell proposed the need for and focus on an educational pipeline for cyber talent in both academia and corporations, allowing for

[26] Dziwisz, 111.

[27] Zadelhoff, "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It."

[28] Huhn, "Defending Infrastructure against Cyber Attacks through Qualified Cybersecurity Professionals in the Federal Government," 30.

[29] Zadelhoff, "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It."

[30] Steven Furnell, "The Cybersecurity Workforce and Skills," *Computers & Security* 100 (January 2021): 2, https://doi.org/10.1016/j.cose.2020.102080.

[31] Furnell, 2.

standardized paths and the levels of proficiency, as outlined in the UK's Chartered Institute of Information Security.[32] In the book *Cyber Security Education: Principles and Policies*, editor Greg Austin shared similar views with Furnell in the UK on their university systems not providing specific cyber degrees broken down into sub-components such as countering crime, protecting critical infrastructure, and countering misinformation.[33] In 2017, Australia took their first steps to realign their cyber security education with their national cyber strategy.[34] Austin did concede on the difficulties on hiring cyber experts in Australia, and places the problem not necessarily on the educators, but on the cyber labor market.[35] Furthermore, Austin frequently mentioned the difficulties that go into researching cyber security skills shortages and recommended more research from multiple disciplines, such as the labor, educational, public policy, and cybersecurity markets. Thus, the academics and experts agreed on the current lack of global cyber talent, especially in establishing national standardization requirements, and differed on where to focus their efforts in academia or the labor markets.

While the literature concurs on the current lack of cyber talent, scholar and expert works offered many untested hypotheses on how to move ahead. From Zadelhoff's "new collar" candidates for on-the-job training to the military changing its policy on recruiting standards, many ideas on expanding cyber talent are currently being discussed in all sectors.[36] Zadelhoff mentions IBM's solution to the cyber talent shortage is to look outside the conventional resumes and instead seek individuals who have a passion for problem solving and an understanding of risk management.[37] This concluded in IBM hiring twenty percent "new collar" cybersecurity positions on the merits of curiosity about the security field and learning new skills.[38] Christopher Ramezan of West Virginia University

[32] Furnell, 6.

[33] Greg Austin, ed., *Cyber Security Education: Principles and Policies* (London: Routledge, 2021), 215, https://doi.org/10.4324/9780367822576.

[34] Austin, 3.

[35] Austin, 199.

[36] Zadelhoff, "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It."

[37] Zadelhoff.

[38] Zadelhoff.

recommended breaking down the cybersecurity position requirements into nine sub-fields and develop pathways for each subject: architecture, auditing, education, governance risk and compliance, management, operations, penetration testing, software security, and threat intelligence. These ideas could provide a cross-pollination of experience throughout the cyber enterprise, thereby opening more hiring opportunities for employers.[39]

Some sectors fare worse than others in the lack of cyber talent, with authors in academia and the defense industry alike seeing the dangers in large pay disparities between the public and private sectors. The government's cyber sector, to include the military, is hemorrhaging due to the pay disparities between the public and private sectors. Many authors—most notably Ramezan in his "Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field" article—mention the requirement for government employees to retain a security clearance, often cutting out well-qualified talent due to past experiences.[40] This is a troubling development, as many of the nation's critical infrastructure requires government oversight and use the of Framework for Improving Critical Infrastructure Cybersecurity, developed by the National Institute of Standards and Technology (NIST.)[41] Heidi L. Huhn's dissertation titled "Defending Infrastructure against Cyber Attacks through Qualified Cybersecurity Professionals in the Federal Government" posited that ninety-seven percent of federal employees in information technology believe their systems are vulnerable due to the current shortage of cyber talent.[42] This trend highlights the importance of tight governmental cybersecurity controls by private citizens; there is a plurality of reviewed literature on this topic.

Several academic and expert works also described the revenue loss within the private sector from cyberattacks and ways to mitigate future incidents. Isaac Barnes's

[39] Christopher A. Ramezan, "Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field," *Journal of Information Systems Education* 34, no. 1 (Winter 2023): 94, ProQuest.

[40] Ramezan, 94.

[41] Tony Hubbard, Geoffrey L. Weber, and Jeffrey C. Steinhoff, "Protecting Data Assets in a Perilous Cyber World," *Journal of Government Financial Management* 66, no. 3 (September 2017): 29, EBSCOhost.

[42] Huhn, "Defending Infrastructure against Cyber Attacks through Qualified Cybersecurity Professionals in the Federal Government," 7.

"Implementation of Active Cyber Defense Measures by Private Entities: The Need for an International Accord to Address Disputes" argued that active cyber defense measures are required to retain secure networks to identity the attacker and potentially change their cost-benefit analysis to conduct future attacks.[43] Similarly, O'Loughlin's thesis highlighted the importance of partnerships between government and the civilian sectors to effectively implement unconventional cyber entities in the name of better cybersecurity.[44] O'Loughlin stated the merits of these partnerships, which can take on many forms: from groups of industry with similar security interests, to civilian groups under a direct threat from an outside entity (as seen in Poland, pushing back against Russian aggression).[45] Lastly, Srinath Perera's commented in the Swiss journal *Infomatics*, in an article titled "Factors Affecting Reputational Damage to Organizations Due to Cyberattacks," that both the private sector and government are equal partners in leveraging optimal cybersecurity to protect each stakeholders' "cyber reputation."[46] Perera identified the primary three elements which may impact a company's cyber reputation as the trust and privacy of customers, how customers view the organization, and the extent to which the incident—should a cyberattack occur—become publicly known.[47] Perera's article also mentioned past studies in the UK published findings on cyber risk management since 2008 which focused on quantifying the cyber reputation of an organization, but most of those results are no longer valid due to the fast pace of technology and the company's ability to keep up with its cybersecurity programs. As such, this body of literature revealed that a company's cyber reputation and their bottom line could make or break their business plan, and it is therefore imperative that a well-trained cyber workforce be available to shore up their long-term strategies.

[43] Isaac A. Barnes, "Implementation of Active Cyber Defense Measures by Private Entities: The Need for an International Accord to Address Disputes" (master's thesis, Naval Postgraduate School, 2018), V, http://hdl.handle.net/10945/61274.

[44] O'Loughlin, "Three If by Internet," V.

[45] O'Loughlin, 33.

[46] Srinath Perera et al., "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks," *Informatics* 9, no. 1 (March 2022): 19, ProQuest.

[47] Perera et al., 19.

Like most vocations, pay disparity is not the only challenge to a healthy cyber enterprise. Much of the reviewed literature revealed the high-pressure responsibility that often comes with a "feast or famine" operations tempo, and touched upon challenges within the cybersecurity field, regardless of its topic or intent. According to Adam Janofsky's journal article "Fighting the Bad Guys Daily: Why Cybersecurity Teams Focus on Managing Stress," stress among the cyber communities and rapid obsolesce of talent are driving cyber professionals out of the industry.[48] These concerns are due to inadequate budgets, lack of expertise, failure to keep up with changing technology, and enduring security threats tending to cross over from source to source, eventually leading to burnout and departure of the industry.[49] Andrew Ishmael's dissertation with Capital Technology University conducted a qualitative case study on the retention of qualified cybersecurity professionals and found that four pillars of cybersecurity retention—organizational support and engagement, opportunity, flexibility, and recognition—can act as a long-term solution and retain talent within the industry.[50] Lilly Chapa's "Cyber Workforce Shortcomings" in *Security System News* provided even longer-term remedies, such as teaching children and adults alike about cybersecurity career pathways, and stated the advantages of both the public and private sectors financially-supporting science, technology, engineering, and mathematic (STEM) programs throughout the American educational system.[51] Few of the referenced material recommended viable short-term solutions beyond properly coding job announcements and broadening the position description, illustrating the depth of the problem within the cybersecurity enterprise.

3. The Power of Partnerships in Countering Tomorrow's Cyber Threat

Enterprise leaders in the private sector are leaning on the federal government to provide a more comprehensive approach on cyber threats. Large cybersecurity corporations

[48] Adam Janofsky, "Fighting the Bad Guys Daily: Why Cybersecurity Teams Focus on Managing Stress," *WSJ Pro. Cyber Security*, May 22, 2018, ProQuest.

[49] Janofsky.

[50] Andrew R. Ishmael, "A Qualitative Case Study on the Retention of Qualified Cybersecurity Professionals," (PhD diss., Maryland, Capitol Technology University, 2021), 91, ProQuest.

[51] Lilly Chapa, "Cyber Workforce Shortcomings...," *Security Systems News* 22, no. 4 (April 2019): 10, ProQuest.

are lobbying for meaningful partnerships with the federal government to mitigate future cyberattacks. Sean Joyce of PricewaterhouseCoopers's Global & U.S. Cybersecurity raised the urgency of government to partner with the private sector and academia for updated laws, regulations, and corporate responsibilities.[52] *Barron's* author Glenn Gerstell indicated in his article titled "Biden's New Cyber Strategy Will Acknowledge an Essential Truth: Market Forces Aren't Enough" that President Biden's 2023 National Cyber Strategy will contain language toward enhanced cooperations with the private sector through centralized cyber authorities, measures to increase the cyber workforce through cybersecurity apprenticeships, strict regulations for more secure computer hardware, and strengthening international efforts to combat ransomware.[53] Thus, the consensus in the literature centers around the 2023 Cyber Security Strategy as the nexus that teams up the public and private sectors for real change.[54]

Overall, the reviewed literature did not provide any silver bullet solution to quickly improve the nation's cybersecurity posture against cyberattacks. The tangled web of public and private networks complicates a one-stop shop national approach to best protect American cyber infrastructure. Members in academia, government officials, or private sector individuals with a vested interest in crafting laws contributed the majority of research in this literature review. Of note, and in addition to the cited works, twenty-seven accredited non-peer-reviewed articles from the "cyber field" over the past ten years address similar issues from the review material and primarily side with the professors and lawmakers. These additional readings were imperative to rounding out the literature review and allowed for a more confident assessment within rapidly evolving cyberspace. All in all, the nearly unanimous assessment is that training the cyber experts of tomorrow can mitigate potential risks in the cyber domain. As stated in the introduction, the

[52] "Biden's Executive Order on Cybersecurity: What's in It and Who Should Be Ready for It," PricewaterhouseCoopers, 2023, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/bidens-executive-order-cybersecurity.html.

[53] Gerstell, "Biden's New Cyber Strategy Will Acknowledge an Essential Truth."

[54] White House, "Fact Sheet: The Biden-Harris Administration's National Security Strategy."

vulnerabilities in the cyber domain are clear, but the scholarly peer-reviewed literature is still undecided on how to best come together and reduce tomorrow's cyber risk.

D. RESEARCH DESIGN

Overall, this thesis explored the feasibility of a Civilian Reserve Cyber Force with public-private sector employees to best protect American critical infrastructure from adversarial cyberattacks at a time of mass shortages of cybersecurity experts. Specifically, this thesis investigated the feasibility of the formation of a CRCF. As ongoing cyberattacks continued throughout 2021, a bipartisan group of lawmakers introduced legislation to create a "Civilian Cybersecurity Reserve" to counter growing cybersecurity vulnerabilities across the public-private sector. The bill envisioned a CRCF as a large group of citizens with cyber talent and experience organized through a government agency, working alongside government cyber experts in an augmented capacity and at the ready to defend American interests against large-scale cyberattacks. This concept can work in theory, but many roadblocks are currently in the way to make this cyber force a reality. The notion of an active CRCF cannot be realized until three concepts are better understood:

1. The past, current, and impending impacts of federal law protecting Americans against cyberattacks (policy analysis).
2. Understanding the global shortage of cybersecurity experts and academia's struggle to train and build cyber talent (gap analysis).
3. If passed, how could a CRCF be best built, organized, and activated (case studies).

To answer the research question, this thesis conducted a qualitative—comparative policy and case study analysis—research design. First effort focused on a federal, cyber-based policy analysis which accurately described past, current, and impending congressional laws and executive orders required to establish boundaries on cyberattacks within the cyber domain. Most of the required research involved historical and current material and covered the descriptive and exploratory paradigms of this thesis, including

legislative and executive actions over the past nine to ten years on major cybersecurity initiatives. Since 2013, the executive and legislative branches implemented five executive orders (EO) and countless legislative proposals related to cybersecurity and its workforce, spanning three different administrations. High-profile cyber incidents continued to occur over the next five years, growing more sophisticated and with higher levels of complexity. It also described cyberattacks in the public sector (i.e., cyberattacks on the OPM and the Democratic National Committee's email servers in 2016) which led to major policy shifts, such as PPD-41 that outlines principles governing the federal government's response to a cyber incident and further defining the scope of the cyber domain. While the EO and PPDs advocated the creation of a commission which seeks to update and improve the security of the nation's cyber infrastructure, it also supported the idea of funding for a CRCF to help protect government networks and defend American interests against internal or transnational cyberattacks. For this to happen, a federal agency must identify, vet, and organize a group of ready reserve cyber talent while experiencing historic workplace shortages within both the public and private sectors.

Secondly, this thesis conducted four case studies on organizations that may contribute to a cyber reserve force: the Civil Reserve Air Fleet (CRAF), the State Defense Force (SDF), The National Guard, and the United States Space Force (USSF). The research used existing public-private and government partnership frameworks in studying the practicability of creating and fielding for a CRCF, each providing a unique characteristic to ensure the CRCF's success. The CRAF provides an efficient use of a particular requirement during times of national emergency, the SDF's ability to retain talent through volunteerism, the tried and true "citizen airman/soldier" militia construct of the National Guard, and the essential "digital age tenets" of the USSF. Together, these frameworks can form the foundation of a CRCF model and offer a concept of operations based on historical successes in support of the latest congressional cyber legislation. The case studies utilized laws and government policies, scholarly studies, peer-reviewed journal articles and books, think tank reports, and media coverage. Finally, the predictive aspect of this argument explored how a CRCF would be organized and operated. The thesis concluded with a summary and provisional concept of operations (CONOPS) based on a combination of

real-world case study conclusions mentioned above, and future scenarios based on peer-reviewed forecasts. From there, the thesis described how the force activates in an imagined, but not impossible, near future.

II. BACKGROUND ON THE CHALLENGES OF CYBERSECURITY AGAINST CRITICAL INFRASTRUCTURE

This chapter explores potential imperatives for establishing a CRCF to shield vital infrastructure against digital, non-kinetic threats. The narrative begins with a hypothetical depiction of an extensive power grid disruption in the northeastern U.S. anticipated for 2027, illuminating the profound consequences on essential services and the general populace. A retrospective assessment of previous cyberattacks connects real-world examples and demonstrates potential innovative approaches in the creation of a CRCF. The chapter concludes by highlighting the significance of preempting rapid technological advancements to seamlessly integrate a CRCF into the nation's comprehensive cybersecurity gameplan.

A. THOUGHT EXPERIMENT: A FICTIONAL FUTURE SCENARIO

In a conceivable near future—2027—a regional power grid responsible for supplying electricity to the northeastern United States catastrophically fails on a Tuesday at 8:03 AM Eastern Standard Time. This unprecedented event disrupts power for fifty-six million residents after a six-day period amid a record-breaking heatwave with temperatures soaring to 114 degrees Fahrenheit. The origin of this multi-state electrical failure remained initially obscure, with the possibility of a ransomware attack yet to be validated. The impact on New York City was particularly severe, with a sizable portion of its critical infrastructure brought to a standstill. Key services—from the dam locks that control river flows, to the air traffic control systems governing its three major airports—went offline. The financial institutions, including the Federal Reserve Bank of New York, were disconnected from international monetary networks. The city's reservoir pumping system was incapacitated, compromising ninety percent of the fresh water supply to its eight million inhabitants.

Panic immediately gripped the populace. Widespread runs on gas stations, a surge of citizens fleeing the city, and subsequent traffic accidents choking the island's limited bridge and tunnel networks paralyzed the metropolitan area to a complete standstill. The

New York Power Authority promptly communicated its status to DHS and the National Security Council (NSC) within the first 12 hours of the blackout, initiating a broad cyber-response action.

In anticipation of potential cascading power grid failures, the DHS federalized 200 members of the recently-established CRCF. This operation, spread across sixteen states, was activated via a smartphone application and provided specific reporting instructions, timelines, and mission data to safeguard additional critical infrastructures. The civilian cyber force, a carefully vetted group familiar with electrical grid operations, cooperated closely with the DOD, DHS partners, and specified sectors within the National Council of Information Sharing and Analysis Centers (ISACs).

Operating remotely, they followed a pre-defined cyber playbook, successfully stopping a cascade effect of grid failures beyond New York and northeastern United States. Their collective efforts prevented a broader catastrophe, saving lives and preserving trillions of dollars in commerce across the affected states. With the mission accomplished, the CRCF mission team stood down with its members reverting to their civilian roles. Embodying a new sense of digital volunteerism, each member of the CRCF was recognized by DHS for their efforts in protecting the nation in an era defined by its intricate digital dependencies.

B. HISTORICAL BACKGROUND ON PAST CYBER-ATTACKS

The United States government requires novel twenty-first century strategies for the establishment of a provisional CRCF. Over the past decade, although the federal government has responded to numerous cyber incidents, it has yet to face a "Cyber Pearl Harbor" scenario, a phrase famously stated by computer security analyst Winn Schwartau while discussing the threats of cyber-terrorism to Congress in 1991.[55] Enhanced funding for emergency management has established reliable frameworks designed to respond to traditional events such as natural disasters or terrorist attacks. While the United States has not yet encountered a large-scale national cyber incident perpetrated by a major nation-

[55] Winn Schwartau, "Asymmetrical Adversaries," *Orbis* 44, no. 2 (2000): 203, https://doi.org/10.1016/S0030-4387(00)00018-1.

state like China or Russia, its existing response plans for future cyberattacks are still grounded in the classic examples mentioned above. This reliance could potentially impede the agility needed to react to a dynamic, nationwide cyber incident. A national CRCF could adopt best practices to harness civilian sector cyber talent in the protection of national networks and critical infrastructure before, during, and after a cyberattack. The lessons learned from historical cyber policies and potential frameworks can guide the development of these new strategies. By anticipating the accelerated pace of change and leveraging emerging technologies, a CRCF becomes an integral part of the national cybersecurity infrastructure in the near future.

Regrettably, the federal government is not the sole entity at risk. The security of private sector industries is increasingly threatened by cyberattacks. According to a survey of Cybersecurity 202 Network members, 81 percent believe the United States is either more vulnerable or just as susceptible to cyberattacks as it was five years ago.[56] In 2021, North America witnessed an alarming 105 percent surge in ransomware cyberattacks, which are attacks designed to render computer systems inoperable until the company or owners pay a financial ransom to unlock their networks or files.[57]A cyber threat report from internet security firm SonicWall disclosed an astonishing rise in ransomware attacks targeting governments around the globe by 1,885 percent while other vital industries like healthcare witnessed a 775 percent surge in cyberattacks.[58] In May 2021, JBS Foods-USA, the globe's largest meat provider, fell victim to a ransomware attack and ultimately paid a ransom of $11 million in Bitcoin to prevent further disruption.[59] The FBI identified Revil, a group of Russian cyber ransomware attackers, as the perpetrators behind the JBS hack.[60] This recent surge in attacks can be attributed to lax security practices, complacency in

[56] Marks and Schaffer, "The U.S. Isn't Getting Ahead of the Cyber Threat, Experts Say."

[57] Taylor, "Ransomware Cyberattacks Surged in 2021."

[58] Ahiah Taylor, "There's a Huge Surge in Hackers Holding Data for Ransom, and Experts Want Everyone to Take These Steps," *Fortune*, February 17, 2022, https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/#:~:text=Governments.

[59] Taylor.

[60] Taylor, "There's a Huge Surge in Hackers Holding Data for Ransom, and Experts Want Everyone to Take These Steps,"

software updates, or a misplaced belief that their data is immune to such attacks.[61] As the cyber threat escalates in both size and complexity, the United States has yet to leverage its cyber sector talent and initiate the blueprint for a nationwide, unified cyber protection effort.

C. BACKGROUND ON CYBERSECURITY LAWS

The federal government's understanding of national security and resilience must adapt to the new reality of cyberattacks and their threats to American critical infrastructure. The role of governmental bodies in protecting the integrity of the nation's cybersecurity infrastructure has become increasingly apparent and crucial. From EOs signed by the president to congressional bills seeking to fortify cyber defenses in 2023, various branches of government are now more intertwined with cybersecurity than ever before. Meanwhile, collaborative studies undertaken by federal entities are further exploring potential strategies and solutions to address these evolving challenges. Recent cyber laws, executive orders, and joint cyber studies discussed below explore their implications on the establishment of CRCF, which could potentially serve as a formidable vanguard in safeguarding America's cyber enterprises. Together, their collective impact on the broader cybersecurity domain can secure the nation's critical infrastructure against advanced cyber threats.

1. Executive Orders

Building on the foundation established by President Clinton's 1998 executive order aimed at protecting critical infrastructure, the federal government has since enacted a range of sophisticated policies designed to bolster cybersecurity.[62] From 2013 onwards, the executive and legislative branches have implemented five E.O.s and a multitude of legislative proposals, addressing cybersecurity and its workforce under three different administrations. Despite these proactive measures, the ensuing five years were marked by a series of high-profile cyber incidents, each more sophisticated and complex than the last.

[61] Taylor.

[62] National Security Council, *Critical Infrastructure Protection*, Presidential Decision Directive/NSC-63 (Washington, DC: National Security Council, 1998), https://irp.fas.org/offdocs/pdd/pdd-63.htm.

One prominent example is the 2016 cyberattacks on OPM and the Democratic National Committee's email servers, incidents that spurred President Obama to sign PPD-41.[63] PPD-41 establishes not only the principles guiding the federal government's response to cyber incidents, but also standardizes definitions, outlines concurrent lines of effort, and orchestrates coordination at the national, operational, and field levels. For example, PPD-41 standardizes the differences between a "cyber incident" or an observable occurrence in a network and a "significant cyber incident," which is defined as a violation or imminent threat to the nation's national security interests.[64] Furthermore, PPD-41 fostered greater collaboration between the government and the private sector by adopting successful models from traditional disaster response strategies. Alongside PPD-41, President Obama also issued an EO creating the "Commission on Enhancing National Cybersecurity," a blueprint delineating the government's response to hostile actions in the cyber domain.[65] Its roles are multifaceted and aimed at providing detailed roles such as short and long-term recommendations, promotion of best practices, engagement with stakeholders, and tasked with providing ways to leverage research and technology.[66] This order not only advocates for the establishment of a commission aimed at updating and enhancing the nation's cyber infrastructure security, but also endorsed funding for a CRCF capability that can safeguard government networks and defend American interests against both domestic and transnational cyberattacks.

While all these E.O.s aim to strengthen national cybersecurity, they have had limited success in adapting to the speed and dynamic nature of the digital world. In April 2023, the Government Accountability Office (GAO) published a series of high-risk efforts

[63] Barak Obama, "Presidential Policy Directive – United States Cyber Incident Coordination," The White House, July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[64] Obama.

[65] Barak Obama, "Executive Order -- Commission on Enhancing National Cybersecurity," The White House, February 9, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

[66] Obama.

to Congress that outlined progress or lack thereof since 2021.[67] The GAO identified "Ensuring the Cybersecurity of the Nation" as high-risk, not meeting the demonstrated progress outlined in the latest 2021 EO signed by President Obama.[68] Prominent examples such as the SolarWinds, Microsoft Exchange, and Colonial Pipeline cyberattacks revealed vulnerabilities in American informational systems, highlighting a need for improved cybersecurity defenses across public and private sector networks.[69] The discovery of the SolarWinds breaches toward the end of 2020 prompted the White House to convene a Unified Cyber Coordination Group (UCG) with private sector participation.[70] However, these efforts failed to align with the criteria for a significant cyber incident as specified in PPD-41, thereby undermining the standardization attempts made four years prior. Although the leadership commitment to ensuring cybersecurity of the nation remains a priority such as making more than 670 or the more than 4,000 GAO recommendations since 2010, more needs to be done to action priorities in innovation and proactive measures within cybersecurity policy.[71]

On May 12th, 2021, in a significant step forward, President Biden signed E.O. 14028 to enhance the nation's cybersecurity posture and safeguard government networks. This EO heralds a new era in the nation's approach to cybersecurity by mandating seven key actions (shown in Table 1) which can be incorporated into the baseline standards for a CRCF.

---

[67] Michelle Sager, *High- Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, DC: Government Accountability Office, 2023), 1, https://files.gao.gov/reports/GAO-23-106203/index.html#top.

[68] Sager, 149.

[69] Harvey Rishikof, "All That Which Is Old, Is New Again – Unlearned Lessons about Metrics of Success in Cyber," *The Cyber Defense Review* 7, no. 1 (2022): 122, https://www.jstor.org/stable/48642044.

[70] Cybersecurity and Infrastructure Security Agency, "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)," Cybersecurity and Infrastructure Security Agency, January 5, 2021, https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

[71] Sager, *High Risk Series*, 152.

Table 1. Summary of Actions and Outcomes for E.O. 14028 [72]

EO 14028 Action	Strategic Outcome
Eliminate obstacles that prevent the exchange of threat information between government and private entities	Eliminate contractual obstacles to disclosing breach details that could affect government networks
Update and enforce more robust cybersecurity protocols within the federal government	Accelerates secure cloud-based services and a zero-trust architecture within the federal government, similar to the DOD
Improve software supply chain security	Establish baseline standards on all future purchased government software
Establish a cybersecurity safety review board	Led by representatives from both the public and private sector and modeled after the National Transportation Safety Board
Create a playbook for cyber incident response	Standardizes a cyber-response playbook across the federal enterprise, guaranteeing all agencies achieve a specific standard and jointly act in response to the incident
Improve detection on government networks	Facilitates endpoint detection and response system across the federal government to rapidly detect malicious activity
Improve investigative and remediation capabilities	Mandates event log requirements for federal agencies

The actions outlined above provide a robust holistic approach to fortifying national defense in the digital domain. It removes silos, and promotes collective intelligence methods to tackle real-time threat mitigation. It also modernizes standards such as the transition to a zero-trust architecture, showcasing an emphasis on proactive measures before, during, and after a cyberattack. Along with standardized playbooks, the introduction of event log requirements underscores a commitment to transparency and post-incident analysis. If implemented, these actions signal a comprehensive effort and may better ensure American resiliency in the face of evolving cyber threats.

Efforts to bolster cybersecurity capabilities are evident in a variety of bills currently under review in Congress. As the frequency of cyber events heightened in 2021, a group

[72] Exec. Order No. 14028, "Improving the Nation's Cybersecurity" (2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

of bipartisan lawmakers introduced legislation aimed at forming a "Civilian Cybersecurity Reserve."[73] This proposed reserve aims to confront the expanding cybersecurity vulnerabilities plaguing both the public and private sectors. The original bipartisan bills were proposed in both the Senate and the House of Representatives.[74] The bills have passed committee, and were proposed by Sen. Jacky Rosen (D-NV), the only computer programmer to serve in Congress.[75] The bills advocate for the DHS and the DOD to collaborate in appointing volunteers of the "cyber reserve to six-month positions as federal civil service employees."[76] The genesis of this legislation can be traced to recommendations found in the National Commission on Military, National and Public Service and the Cyberspace Solarium Commission (CSC), which examine potential strategies for establishing a cybersecurity reserve corps.[77] Furthermore, Section 6.1.7 of the CSC outlines a proposal for the evaluation of varied military reserve models to better examine surge capabilities in a time of crisis and leverage established links between the public and private sectors.[78] Interestingly, these proposed models do not necessarily conform to the traditional uniformed service's standards for drilling, grooming, or physical requirements.[79] These initiatives are not only encouraging, but also indicate a growing momentum within Washington, D.C., toward the exploration of options and coordination groups focused on cyber-response. This progress is critical for establishing the legal foundation necessary for the realization of a CRCF.

[73] Rosen, S.1324 – 117th Congress (2021-2022): Civilian Cybersecurity Reserve Act.

[74] Rosen.

[75] Civilian Cyber Security Reserve Act, H.R. 2894, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/house-bill/2894/text?s=1&r=57.

[76] Rosen, S.1324 – 117th Congress (2021-2022): Civilian Cybersecurity Reserve Act.

[77] Jacky Rosen, "Rosen's Bipartisan Bill to Establish Civilian Cybersecurity Reserve Passes Senate Committee Unanimously," Senator Jacky Rosen, July 14, 2021, https://www.rosen.senate.gov/rosens-bipartisan-bill-establish-civilian-cybersecurity-reserve-passes-senate-committee-unanimously.

[78] Congress, *Cyberspace Solarium Commission – Report* (Washington, DC: Congress, 2020), 117, https://www.solarium.gov/report.

[79] Congress, *Cyberspace Solarium Commission: Legislative Proposals* (Washington, DC: Congress, 2020), https://www.solarium.gov/report.

2. Joint Studies

The feasibility of a Civilian Reserve Cyber Force to better protect critical infrastructure from cyberattacks may be an opportunity to align a long-awaited partnership between the public and private sectors.[80] Consider the role of the Cybersecurity and Infrastructure Security Agency (CISA): a federal body, which actively partners with private sector organizations like banks, utility companies, and healthcare institutions, providing them with resources and guidance to enhance their cybersecurity protocols. CISA has actively partnered with JPMorgan Chase in the banking sector while also teaming up with Atlantic Health System and Union Pacific, empowering these private entities with resources and guidance to amplify their internal security measures.[81] Additionally, the Financial Services Information Sharing and Analysis Center (FS-ISAC) stands out as a nexus for cooperation and a space where giants like Bank of America and Goldman Sachs share threat intelligence with federal agencies, reinforcing the financial sector's cyber defense. The SolarWinds hack in 2020, a high-profile cyberattack affecting both government and private entities, exemplified the critical need for public-private collaboration.[82] In its aftermath, both sectors pulled together, sharing crucial information that helped limit the attack's damage and expedite recovery. This incident underlined not only the importance of joint cybersecurity responsibility, but also the tangible benefits of such collective action against cyber threats. The proposed Civilian Reserve Cyber Force could serve as a model for this kind of public-private partnership, bringing together expertise from both sectors and presenting a united front against cyber threats to critical infrastructure.

[80] Alan Brill and Jonathan Fairtlough, "Fighting the First Battle of Cyberspace Preparedness: Finding Your Reserve Cyber-Warriors," *Information & Security* 44 (February 2019): 10, EBSCOhost.

[81] Kimberly Underwood, "CISA's Cybersecurity Advisory Committee Pivots to Meet the Threat," AFCEA International, June 1, 2023, https://www.afcea.org/signal-media/cyber-edge/cisas-cybersecurity-advisory-committee-pivots-meet-threat.

[82] Gordon Bitko, "What Public and Private Sector Leaders Can Do to Stop the Next SolarWinds Hack," *Forbes*, December 22, 2020, https://www.forbes.com/sites/gordonbitko/2020/12/22/what-public-and-private-sector-leaders-can-do-to-stop-the-next-solarwinds-hack/.

D. MAJOR STAKEHOLDERS IN AMERICAN CYBERSECURITY AND CYBER POLICY

The protection of American networks and data can be overwhelming and overly complex, especially when public and private networks are interwoven together. Catherine Theohary's *Congressional Research Service* (CRS) report, "Defense Primer: Cyberspace Operations," describes DHS taking the lead role in protecting critical infrastructure and managing cybersecurity for non-military federal entities while the DOD assists DHS to safeguard the Defense Industrial Base (DIB) and defense information networks.[83] Collectively, these two entities are tasked with protecting the homeland and its national interests from complex cyberattacks, but what about private industry? Should the private sector be on their own when determining their vulnerabilities or access to proprietary information? How can the DHS and DOD collaborate with the private sector and, fulfilling the role of government, protect American interests from nation-states or criminal cyberattacks? The government authorizes the use of military cyber assets in the event of a major cyberattack on U.S. critical infrastructure, but to what level without crossing the sacred lines between public and private property? How about standards in reporting attacks or information-sharing among public and private enterprises? The major stakeholders mentioned below aim to coordinate these questions along with reporting procedures to bridge the gap between the U.S. government and the private sector.

1. Executive Branch Groups

In response to escalating cyber threats, the executive branch has activated several coordination groups to bolster national cybersecurity infrastructure and procedures. The Cyber Response Group (CRG) plays a significant role in this defense network. It oversees the development and execution of federal strategies and protocols for significant cyber

[83] Catherine Theohary, *Defense Primer: Cyberspace Operations*, CRS Report No. IF10537 (Washington, DC: Congressional Research Service, 2022), 1, https://crsreports.congress.gov/product/details?prodcode=IF10537.

incidents.[84] The CRG supports the NSC's Deputies and Principals Committees, and is held accountable by the Assistant to the President for Homeland Security and Counterterrorism (APHSCT), who reports to the NSC, chaired by the president.[85] Simultaneously, the UCG operates as the main channel for unifying federal and private sector responses to cyber incidents, as mandated by PPD-41.[86] Rather than assuming an oversight role, the UCG seeks to facilitate unity of effort among various agencies, (i.e., when the UCG coordinated efforts during the SolarWinds hack in 2020).[87] The UCG may be activated by the NSC's Principles Committee, Deputies Committee, or the CRG, especially when a significant cyber incident jeopardizes critical infrastructure and induces broad impacts on public health, safety, economic stability, or national security.[88] The UCG crucially incorporates non-governmental cyber partners in response to significant cyber events as appropriate, effectively bridging the gap between the public and private sectors.[89] Together, the CRG and UCG form the cornerstone of the executive branch's strategy for mitigating cyberattacks, fostering a united front between public and private sectors. By combining their resources and expertise, these groups signify the government's concerted effort to strengthen cybersecurity defenses, and respond promptly and effectively to any cyber threats that the nation faces.

2. Department of Defense

The DOD plays a critical role alongside the DHS, Department of Justice (DOJ), and the Office of Director of National Intelligence (ODNI) in safeguarding American

[84] Cybersecurity and Infrastructure Security Agency, *Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems* (Washington, DC: Cybersecurity and Infrastructure Security Agency, November 2021), 41, https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

[85] Cybersecurity and Infrastructure Security Agency, 45.

[86] Obama, "Presidential Policy Directive – United States Cyber Incident Coordination."

[87] Quentin E Hodgson et al., *Managing Response to Significant Cyber Incidents: Comparing Event Life Cycles and Incident Response Across Cyber and Non-Cyber Events*, RRA1265-4 (Santa Monica, CA: RAND, 2022), 2, www.rand.org/t/RRA1265-4.

[88] Obama, "Presidential Policy Directive – United States Cyber Incident Coordination."

[89] Obama.

critical infrastructure from cyber threats. The DOD's principal responsibility lies in defending the United States against all major cyber threats, both domestic and international, which is primarily accomplished by the United States Cyber Command (CYBERCOM).[90] Furthermore, the DOD shares valuable threat intelligence and cyber defense capabilities with other federal agencies, notably DHS, Federal Bureau of Investigation (FBI), and the Cyber Threat Intelligence Integration Center (CTIIC).[91] For instance, the DOD collaborates with the DHS in protecting critical national infrastructure through the Joint Force Headquarters-DOD Information Network (JFHQ-DODIN), which defends the DOD's own networks, and also provides support to the DHS when requested. The DOD also works closely with the Director of National Intelligence to gather, analyze, and disseminate cyber threat intelligence through the Intelligence Community Analysis and Signature Tool (ICOAST).[92] Meanwhile, the DOJ leverages the DOD's resources and along with international partners in the legal aspects of cyber warfare and the prosecution of cyber criminals.[93] This collaborative and synergistic approach ensures a holistic defense against cyber threats and maximizes the capabilities of each agency, making the DOD, with its unique resources and capabilities, a fundamental pillar in the collective effort of the executive branch to fortify America's cyber defenses and protect critical infrastructure.

3. Department of Homeland Security

Emphasizing the pivotal role of the DHS, and specifically CISA, the government is bolstering its commitment to asset response activities within the greater cyber enterprise. Acting through the National Cybersecurity and Communications Integration Center (NCCIC), CISA has taken the lead in cooperating with industry and government partners to enhance comprehension of cybersecurity risks and strategize effective countermeasures.

---

[90] White House, *National Cybersecurity Strategy* (Washington, DC: White House, 2023), 15, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[91] White House, 11.

[92] Office of the Inspector General of the Intelligence Community, *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (Washington, DC: Office of the Inspector General of the Intelligence Community, 2021), 9, https://www.dni.gov/files/ICIG/Documents/Publications/Reports/2022/CISA_Joint_Final.pdf.

[93] White House, *National Cybersecurity Strategy*, 31.

Notably, Section 6 of E.O. 14028 directed CISA to "develop a standard set of operational procedures (playbook) to be used in planning and conducting cybersecurity vulnerability and incident response activity respecting Federal Civilian Executive Branch (FCEB) Information Systems."[94] This playbook reveals the roles of critical cyber stakeholders and normalizes shared practices, thus promoting a coordinated response between government and private entities. The concerted efforts of entities like CISA in establishing procedural norms are essential to mitigating the implications of cyber threats on national security.

4. Department of Justice

In recognition of the increasingly borderless nature of cyber threats, the DOJ has sought to equip itself to confront transnational cyber incidents. Just as physical threats to national security have transcended geopolitical boundaries, cyber threats often emerge from nation-state actors or foreign criminal elements, making their origins both diverse and potentially remote. Such terrain necessitates a robust intelligence and investigative framework at the federal level. In this context, the DOJ, functioning through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), serves as the lead agency for threat response activities.[95] These efforts reflect a pivotal shift in strategy, re-orienting from a predominantly domestic focus to an approach that comprehends the global dimensions of cyber threats. As critical infrastructure becomes more vulnerable to cyberattacks around the world, the role of agencies like the DOJ will be instrumental in ensuring a strong, initiative-taking response to cyber threats, irrespective of their source or nature.

5. Office of the Director of National Intelligence

In the scope of intelligence support during a significant cyber incident, the ODNI takes the lead.[96] The CTIIC, an agency under ODNI, serves as the central authority for

[94] Exec. Order No. 14028, Improving the Nation's Cybersecurity.

[95] Obama, "Presidential Policy Directive – United States Cyber Incident Coordination."

[96] Obama.

providing situational awareness, sharing relevant intelligence information, and delivering integrated analysis of threat trends and events.[97] They offer key assistance toward collaborative agency initiatives focused on devising strategies to reduce or counteract adversary threats.[98] The CTIIC also coordinates intelligence gathering efforts pertaining to the cyberattack, which involves pinpointing intelligence shortfalls via the National Intelligence manager for Cyber, one of the four divisions within the CTIIC.[99] The importance of the ODNI and its sub-agencies in the intelligence response to a cyber incident is irrefutable, offering a comprehensive and unified approach to threat intelligence that can facilitate more robust, coordinated, and effective responses to cyber threats. This makes ODNI's role pivotal in the grand scheme of national cybersecurity strategy, and it stands as a beacon of effective intelligence management in an increasingly cyber-centric world.

6. Public-Private Sector Partnerships

The DOD, recognizing the critical importance of innovation and its ties to emerging missions and frameworks, has established multiple programs over the past five years. Former Defense Secretary Ash Carter emphasized the necessity for the DOD to adapt swiftly, given the ever-changing global environment, advocating for openness and connection with the innovative community as vital strategies for mission success.[100] Mirroring the private sector's embrace of risk and acceptance of failure as part of their "cyber scientific method" approach to innovation, the DOD has similarly cultivated

[97] "Who We Are – ODNI," The Cyber Threat Intelligence Integration Center, accessed July 31, 2023, https://www.dni.gov/index.php/ctiic-who-we-are.

[98] Department of Homeland Security, *National Cyber Incident Response Plan* (Washington, DC: Department of Homeland Security, 2016), 33, https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[99] "Organization: Cyber Threat Intelligence Integration Center," National Counterterrorism Center, accessed July 31, 2023, https://www.dni.gov/index.php/nctc-who-we-are/organization/241-about/organization/cyber-threat-intelligence-integration-center.

[100] Terri Moon Cronk, "Carter: DOD, Private-Sector Tech Innovation Keep U.S. Ahead," DOD News, March 3, 2016, https://www.defense.gov/News/News-Stories/Article/Article/685675/carter-dod-private-sector-tech-innovation-keep-us-ahead/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F685675%2Fcarter-dod-private-sector-tech-innovation-keep-us-ahead%2F.

partnerships with private sector groups in their native environments.[101] Notable initiatives such as Hacking for Defense (H4D) and the Defense Innovation Unit (DIU) underscore this commitment to innovation.

H4D, an educational initiative designed by Stanford University (and now adopted by several institutions worldwide), is one such groundbreaking program.[102] It employs design-thinking and the Lean Startup model to address complex problems in defense and intelligence communities, including cybersecurity.[103] As a congressionally funded DOD program, H4D has so far resolved over 750 national security problems, leading to the establishment of fourteen startups.[104] These startups have introduced innovative solutions ranging from mobile training platforms to devices enabling first responders to see through walls.[105] Participants like Max Weintraub, a former H4D student, testify to the program's success, citing the transformative educational experiences it provides, from partnering with the Army Asymmetric Warfare Group's effort to parse actionable intelligence from social media to working as a program manager at the DOD's National Security Innovation Network.[106]

On the other hand, the DIU focuses exclusively on rapidly adopting commercial technology across the military enterprise.[107] Its six priority areas—artificial intelligence, autonomy, cyber, energy, human systems, and space—require swift acquisition timelines.[108] The DIU employs a three-phase process to expedite prototype development, with successful products such as the cybersecurity vulnerability hunter, Mayhem, and

[101] Michael Bold, "Hacking for Defense Turns 5," *Army ALT Magazine* (Fort Belvoir, United States: Superintendent of Documents, May 21, 2021), ProQuest.

[102] Bold.

[103] "About the Hacking for Defense Course," Hacking for Defense, accessed July 20, 2022, https://www.h4d.us/about-h4d.

[104] Bold, "Hacking for Defense Turns 5."

[105] Ann Vaughan, "Hacking for Defense Turns 5 – USAASC," United States Army Acquisition Support Center, May 21, 2021, https://asc.army.mil/web/news-hacking-for-defense-turns-5/.

[106] Vaughan, 64.

[107] Defense Innovation Unit, "About DIU," Defense Innovation Unit, accessed July 20, 2022, https://www.diu.mil/about.

[108] Defense Innovation Unit.

GigEagle, a skill-matching application for Reserve Component forces.[109] This focus on innovation has resulted in significant strides in areas such as persistent cyber "hunt forward" missions, a top priority for CYBERCOM.[110]

These innovative programs, particularly H4D and DIU, present enticing opportunities for recruiting talent and managing a prospective CRCF. The intersection of civilian interest in national defense and these platforms might form the foundation for a future CRCF, contributing to national security without the need for military service. Emphasizing this integration of public and private sector innovation, these initiatives represent the federal government's strategic investment in maintaining a competitive edge in the face of evolving cyber threats.

E. CONCLUSION

The multitude of cybersecurity laws and initiatives, as well as the collaborative efforts among key stakeholders, reflect the urgency and complexity of addressing cyber threats to American critical infrastructure. Existing and proposed executive and legislative measures such as the PPD-41, CSC, and the bipartisan drive to establish a Civilian Cybersecurity Reserve underscore the necessity for a comprehensive and robust approach. Furthermore, the dynamic roles of the DOD, DHS, DOJ, and the ODNI highlight the imperative for strategic cooperation in countering cyber threats. In addition to legacy organizations such as ISACs, innovative programs like H4D and the DIU serve as bridges to integrate civilian expertise and private sector innovation into the defense sphere. As cyberattacks grow, these collaborations and legislative measures lay the groundwork for policy-making that could potentially establish a CRCF, a critical asset in protecting the

[109] "App Aims to Match Reserve, Guard Talent with DOD Needs," U.S. Department of Defense, accessed July 20, 2022, https://www.defense.gov/News/News-Stories/Article/Article/2675967/app-aims-to-match-reserve-guard-talent-with-dod-needs/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F2675967%2Fapp-aims-to-match-reserve-guard-talent-with-dod-needs%2F.

[110] Public Affairs, "U.S. Conducts First Hunt Forward Operation in Lithuania," U.S. Cyber Command, May 4, 2022, https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/ https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3020430%2Fus-conducts-first-hunt-forward-operation-in-lithuania%2F.

nation's cybersecurity infrastructure. The subsequent chapter will evaluate existing frameworks apt for the CRCF, drawing insights from past cyber policies and potential models. Together, these collective efforts signal a strategic and integrated approach in developing a resilient defense against evolving cyber threats.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES ON AMERICAN RESERVE MODELS

In examining the cybersecurity challenges posed to critical infrastructure, it became clear that a robust defense framework is essential. Cyber threats continue to grow in both complexity and subtlety, demanding an adaptive *and* collaborative response. The proposed CRCF stands at the crossroads of these enduring principles and the nuances of modern cybersecurity. Drawing inspiration and structural insights from four tested American models, these examples can anchor this new initiative and offer best practices for strategic planning purposes. CRAF, with its innovative public-private partnership, mirrors the spirit of collaboration essential in today's interconnected world. Meanwhile, the SDF epitomizes localized resilience, reflecting the importance of grassroots cybersecurity measures through volunteerism. The National Guard exemplifies adaptability, seamlessly merging civilian responsibilities with military readiness. Lastly, the newly activated USSF offers glimpses into the future, emphasizing its organization by the merits of the information era. By synthesizing the insights from these distinct entities, this chapter explores options of how the CRCF could be rooted in traditional and emerging organizational models to tackle the unique challenges of the digital age.

A. TRADITIONAL ORGANIZATIONAL MODELS

Within the context of America's defense architecture, the traditional models of the CRAF, SDF, and National Guard occupy distinctive roles, each shaped by historical precedents and unique objectives. While the digital domain may seem a world apart from the operational theaters of these entities, the underlying principles which drive their successes merit further examination for the development of a CRCF. The longevity and effectiveness of these traditional models underscore not just their adaptability, but also their ability to integrate diverse sectors and communities toward a unified national security aim. Among them, the CRAF stands as a testament to the power of public-private synergy in achieving strategic objectives.

1. Civil Reserve Air Fleet

The CRAF serves as a compelling example of the synergy achieved when the public and private sectors collaborate to meet national priorities. Emerging from the legacy of the Berlin Airlift of 1949, the CRAF illustrates the integration of civilian air carriers into military support roles.[111] The 1951 Defense Production Act (DPA), enacted by President Truman, formalized this crucial partnership, uniting the Department of Commerce, the Department of Defense, and civilian airlift industry leaders.[112] In 1967, stewardship transitioned to the Department of Transportation, underscoring the continued significance of this public-private alliance.[113] Throughout the CRAF's progression, the lasting merits of combined efforts in tackling grand-scale challenges becomes evident.

The CRAF's proven history of timely activations in crisis scenarios underscores its efficacy as a public-private alliance dedicated to national defense. As of August 2021, the CRAF comprises twenty-four carriers with a combined fleet of 450 aircrafts.[114] Before this date, the CRAF had been activated twice: first during Operations Desert Shield and Desert Storm from August 1990–May 1991, and then during Operation Iraqi Freedom from February 2002–June 2003.[115] The evacuation in Afghanistan marked the CRAF's third activation, classified as a Stage I requirement due to its humanitarian emphasis.[116] This

[111] Robert E. Gallagher, Gerald F. Burch, and John H. Batchelor, "United States Civil Reserve Air Fleet (CRAF): A Brief History—Formation, Functionality, and Future," *Transportation Research Record* 2676, no. 4 (April 2008): 473, https://doi.org/10.1177/03611981211061553.

[112] Heidi Peters, *Afghanistan Evacuation: The Civil Reserve Air Fleet (CRAF) and the Defense Production Act (DPA)*, CRS Report No. IN11731 (Washington, DC: Congressional Research Service, 2021), 1, https://crsreports.congress.gov/product/pdf/IN/IN11731.

[113] Robert E. Gallagher, Gerald F. Burch, and John H. Batchelor, "United States Civil Reserve Air Fleet (CRAF): A Brief History—Formation, Functionality, and Future," *Transportation Research Record: Journal of the Transportation Research Board* 2676, no. 4 (April 2022): 473–82, https://doi.org/10.1177/03611981211061553.

[114] Peters, *Afghanistan Evacuation: The Civil Reserve Air Fleet (CRAF) and the Defense Production Act (DPA)*.

[115] Gallagher, Burch, and Batchelor, "United States Civil Reserve Air Fleet (CRAF)," April 1, 2022, 475–476.

[116] Peters, *Afghanistan Evacuation: The Civil Reserve Air Fleet (CRAF) and the Defense Production Act (DPA)*.

consistent responsiveness across different crises highlights its enduring value in times of national need.

Building on its historical successes, the CRAF program in its contemporary structure involves air carriers volunteering their aircraft through agreements with the Department of Transportation (DOT) and Transportation Command (USTRANSCOM), located at Scott Air Force Base, Illinois.[117] As a reciprocal gesture, these carriers are prioritized in transporting commercial cargo and passengers during peacetime on behalf of the DOD.[118] The collaborative dynamics involve DOT overseeing the civil carriers' participation, while USTRANSCOM is responsible for the fleet's activation, executed through the Secretary of Defense.[119] This framework can be adapted to cyber-based needs by involving relevant government entities and their cyber industry counterparts. Just as the CRAF leverages private airlines for national defense purposes, a similar model could be envisioned where entities like CISA partner with major cyber industry stakeholders, such as Google and Amazon Web Services, to collaboratively address the nation's pressing cybersecurity needs. Much like partnerships with tech giants can optimize governmental cyber defense, the operational structure of the CRAF demonstrates a balanced approach between public necessity and private capacity.

Drawing parallels from established frameworks like the CRAF provides a blueprint for optimizing modern cyber defense mechanisms. The CRAF framework offers additional capabilities that can benefit the scale and scope of the CRCF mission during a national need. CRAF has three main segments: national, international, and aeromedical evacuation.[120] The DOD can augment the Air Mobility Command's (AMC) cargo fleet

---

[117] Luke A. Nicastro, *Defense Primer: United States Transportation Command*, CRS Report No. IF11479 (Washington, DC: Congressional Research Service, 2020), https://crsreports.congress.gov/product/pdf/IF/IF11479.

[118] Department of Transportation, "Civil Reserve Air Fleet," Civil Reserve Air Fleet, November 20, 2020, https://www.transportation.gov/mission/administrations/intelligence-security-emergency-response/civil-reserve-airfleet-allocations.

[119] Peters, *Afghanistan Evacuation: The Civil Reserve Air Fleet (CRAF) and the Defense Production Act (DPA)*.

[120] Earl Matthews, "Incoming: A Model for Building a Civilian Reserve Cyber Corps," *Signal Magazine*, December 1, 2017, https://www.afcea.org/content/incoming-model-building-civilian-reserve-cyber-corps.

based on national need or the level of demand defined in three stages: Stage I for minor crises or humanitarian relief, Stage II for major theater war, and Stage III for periods of national mobilization.[121] Civilian carriers participating in the program must meet stringent standards. For instance, U.S.-registered carriers are required to allocate 40-percent of their fleet capable of participating in the CRAF while ensuring availability of four complete crews for each aircraft in the program.[122] Aircraft must be available twenty-four, forty-eight, or seventy-two hours after the AMC assigns a CRAF mission, with air carriers retaining resource control, while mission direction remains under AMC purview.[123] Addressing similar minimum needs sets the bar for the kind of readiness expected in the face of a large-scale cyberattack, necessitating CRCF support.

Assessing the spectrum of demand—from local to national scales—is instrumental in understanding the depth of a cyberattack and predicting the necessary cyber expertise required.[124] The CRAF's essence is its role as a safety net, supplementing air transport resources for both military and humanitarian endeavors, while functioning as a powerful deterrent and augmenting force.[125] Integrating the distinct organizational facets of the CRAF, from its legislative underpinnings to its public and private alliances can equip the CRCF with a similar safeguard in the cyber arena. As the discussion progresses into other established frameworks, the National Guard emerges as another model of study for shaping the CRCF.

2. The National Guard

Tracing its lineage back to America's earliest militia in 1636, the National Guard of 2023 stands as a formidable pillar in confronting the nation's most acute cyber

[121] Matthews.

[122] Peters, *Afghanistan Evacuation: The Civil Reserve Air Fleet (CRAF) and the Defense Production Act (DPA)*, 2.

[123] Air Mobility Command, "Civil Reserve Air Fleet," Air Mobility Command, accessed July 19, 2022, https://www.amc.af.mil/About-Us/Fact-Sheets/Display/Article/144025/civil-reserve-air-fleet/.

[124] Gallagher, Burch, and Batchelor, "United States Civil Reserve Air Fleet (CRAF)," April 2022, 2.

[125] Air Mobility Command, "Civil Reserve Air Fleet."

challenges.[126] As a versatile and economical dual-purpose operational force, the National Guard and its dual-militia construct extends strategic depth not only to the Army and Air Force but also to the nascent Space Force, all the while being primed to respond to homeland emergencies.[127] Most of its soldiers and airmen balance their Guard commitments with civilian jobs or education, fostering a continuous exchange of skills in both tradecraft and leadership within their dual roles.[128] The National Guard's dual-militia construct, addressing both domestic and overseas challenges, presents capabilities unparalleled by other frameworks. This unique construct entails:

- Accumulated cyber experience spanning decades, battling threats from nation-states as well as non-state criminal actors.[129]
- Successful retention of civilian expertise: the National Guard's reserve corps has already harnessed civilian talent effectively, enhancing cybersecurity capabilities to defend its networks and offering support when mobilized by state or federal entities.[130]
- Adaptable and timely personnel activation: the National Guard demonstrates remarkable versatility in supporting varied mission requirements. For instance, in 2020, they distributed over 632 million meals, supplied more than 539 million pieces of personal protective equipment, screened over 16.1 million individuals for COVID-19, combated record-setting wildfires on the west coast, and aided in rapid recovery post the onslaught of numerous hurricanes on the Gulf Coast.[131]

---

[126] "How We Began," National Guard, November 2020, https://www.nationalguard.mil/About-the-Guard/How-We-Began/.

[127] National Guard, *2022 National Guard Bureau Posture Statement* (Washington, DC: National Guard, 2022), 4, https://www.nationalguard.mil/Features/Posture-Statement/.

[128] Bonnie M. Vest, "'I Am a Citizen Soldier': Negotiating Civilian and Military in the Post-9/11 National Guard" (Ph.D., New York, State University of New York at Buffalo, 2012), vii, ProQuest.

[129] National Guard, *2022 National Guard Bureau Posture Statement*, 17.

[130] National Guard, 5.

[131] National Guard, 4.

A National Guard member working as an IT security specialist for a major tech company during the week, for instance, can directly apply the latest civilian cybersecurity practices during Guard drills on weekends, bridging the knowledge gap between the private sector and military.[132] Other examples include the Guard's reach into disaster response through shared-resources such as Emergency Management Assistance Compacts (EMAC) or trading skills with foreign cyber allies as seen with the Maryland Air National Guard's 175th Cyber Operations Squadron effort with the Estonia Defence League's Cyber Defence Unit, through the U.S. National Guard's State Partnership Program (SPP).[133] These distinctive arrangements grant the DOD the advantage of maintaining highly-skilled personnel in one location over extended durations without a loss in operational capability, in stark contrast to the active-duty segments where frequent reassignments are the norm. The National Guard's operational versatility and deep-rooted connection with civilian sectors make it an exemplary model for integrating varied expertise. Harnessing these attributes within a CRCF not only enriches the framework's strategic depth but also bolsters its adaptability and responsiveness in the face of evolving cyber threats. Developing on the strengths of the National Guard's operational framework, a CRCF member can be given the flexibility to offer support based on their expertise and interest. This organizational model could opt for missions that align with their skillset, whether it is defending critical infrastructure or specializing in specific cyber threats like ransomware attacks or denial of service.

Linguistic abilities, among other specializations, can also be capitalized on, especially within the intelligence community. It also offers an appropriate blend of leveraging the experience of forces adept at navigating a multifaceted global security environment while simultaneously preparing for an array of emerging threats, both kinetic and non-kinetic. Such an approach not only capitalizes on unique skills but also ensures that the force is agile, adaptable, and prepared to counter a spectrum of cyber threats. While the National Guard provides a robust foundation, the best practices of a State Defense

[132] David Forscey and Monica M. Ruiz, "The Hybrid Benefits of the National Guard," Lawfare, July 23, 2019, https://www.lawfaremedia.org/article/hybrid-benefits-national-guard.

[133] Forscey and Ruiz.

Force, another potential model, focuses more on harnessing cyber talent through volunteerism and purpose of mission.

3. State Defense Force

The success of a national CRCF depends on its ability to retain multiple generations of cyber talent throughout the United States that connects national needs with citizens willing to volunteer their time in service of the homeland, but wanting no part of military service or its culture. This connective tissue of volunteerism and national pride exists in an SDF framework. SDFs are organized, volunteer-based militias with a long and distinguished history of service in the United States. Under subsection I of Title 32, section 109 of the U.S. Code: states, and any other territory of the United States, in addition to its National Guard, may organize and maintain defense forces under state jurisdiction, but it may not be called, ordered, or drafted into the armed forces.[134] Currently, twenty-three states and U.S. territories—including Puerto Rico—retain SDFs, each structured to serve their state's intended purpose, from local emergency response to retaining communication systems.[135] For example, many state guards was integral in domestic crises during the COVID-19 pandemic, when members managed tasks from vaccine distribution to facility decontamination.[136] Their versatility is also underscored by their engagement in a variety of situations, including natural disasters (e.g., storms and wildfires), state-specific endeavors (i.e., the Afghan evacuee resettlement and Operation Lone Star on the U.S. southern border), and collaborations where they often lead or train in tandem with the National Guard.[137] These groups do not operate independently, but through the Adjutant General of its affiliated state acting as the state's senior military commander.[138] This command structure aligns with many aspects of a National Guard unit, providing both

[134] Maintenance of Other Troops, 32 U.S.C. § 109 (1994). https://www.govinfo.gov/app/details/USCODE-1997-title32/USCODE-1997-title32-chap1-sec109.

[135] Jonathan R. Pohnel, "State Defense Forces and Their Role in American Homeland Security" (master's thesis, Naval Postgraduate School, 2015), i, https://hdl.handle.net/10945/45242.

[136] Bob Haskell, "State Guards," *National Guard Magazine*, June 2022, https://www.ngaus.org/magazine/state-guards.

[137] Haskell.

[138] Pohnel, "State Defense Forces," 9.

standardization for its members and a proven organic model for complex operations. Thus, the SDF framework not only offers a standardized approach, but could also serve as an adaptable and tested model suitable for multifaceted cyber operations.

The SDF presents a potent alternative to nationally directed efforts, offering distinct advantages that can significantly enhance a future CRCF mission. To begin with, the cost-effectiveness of the SDF framework is hard to ignore, given that the backbone of its force comprises dedicated volunteers.[139] Notably, a substantial segment of the SDF personnel boasts a background in military service or roles linked to first response and security, ensuring heightened unit cohesion and a unified sense of mission during activations.[140] Another distinct edge is the state-centric control of the SDF, allowing a governor to fine-tune their SDF to address state-specific challenges, be it responding to wildfire mitigation in Oregon or hurricanes in Louisiana.[141] In the case of Hurricane Katrina, 2,274 SDF personnel from eight states deployed, supporting joint operation centers, medical assistance, shelter management, and transportation of civilians.[142] In total, the SDF's adaptability and region-specific expertise position it as an indispensable tool, poised to bridge the gap between localized challenges and the overarching objectives of a robust CRCF.

Additionally, policymakers inclined toward a more state-driven or decentralized structure may find the SDF an appealing model. Such a framework can adeptly harness and streamline a state's existing cybersecurity resources, especially shoring up election security lines of effort. The state-centric alignment is evident in the recommended five-step best practice process laid out in both the National Cyber Incident Plan of 2016 and the CISA Cyber Playbook of 2021, which includes:

---

[139] Pohnel, 9.

[140] Pohnel, 53.

[141] Pohnel, i.

[142] Martin Hershkowitz, *Available State Defense Force After Action Reports from Hurricanes Katrina and Rita Deployments* (Germantown, MD: State Defense Force Publication Center, 2006), 14, https://webcache.googleusercontent.com/search?q=cache:eBcK-23xVDgJ:https://apps.dtic.mil/sti/tr/pdf/ADA496872.pdf&cd=10&hl=en&ct=clnk&gl=us.

- Taking stock of cyber resources within each state, with an emphasis on human capital.[143]
- Bolstering coordination between a state's fusion center and the designated agency overseeing emergency management.[144]
- Actively seeking cyber intelligence and fostering information-sharing with pivotal federal agencies.[145]
- Constituting a state-centric group dedicated to cyber incident response and management, similar to the National Guard.[146]
- Launching cybersecurity initiatives targeting local governments and municipalities.[147]

Such a flexible and state-centric framework can provide governors with enhanced authority, thereby enabling an already functional group to zero-in on critical state and sub-state level concerns. These range from ensuring election integrity to safeguarding local IT infrastructure against emerging threats. The Ohio Cyber Reserve (OhCR), a specialized unit under Ohio's SDF, recently showcased its capacity when a member was deployed to assist in mitigating a cybersecurity breach impacting an undisclosed government agency in 2021.[148] This integrated response, facilitated in tandem with the Ohio National Guard, not only exemplified the state's forward-leaning approach to cyber threats, but also highlighted the critical role of leveraging civilian expertise to defend essential infrastructures and

[143] Department of Homeland Security, *National Cyber Incident Response Plan*, 16.

[144] Department of Homeland Security, 13.

[145] Department of Homeland Security, 20.

[146] Department of Homeland Security, 17.

[147] Cybersecurity and Infrastructure Security Agency, *CISA Cybersecurity Strategic Plan* (Washington, DC: Cybersecurity and Infrastructure Security Agency, 2023), 8, https://webcache.googleusercontent.com/search?q=cache:p8qUgcqbFSsJ:https://www.cisa.gov/cybersecurity-strategic-plan&cd=13&hl=en&ct=clnk&gl=us.

[148] Stephanie Beougher, "Ohio Cyber Reserve Member Deployed in Cybersecurity Response," *Buckeye Guard Magazine*, February 18, 2021, https://ong.ohio.gov/stories/2021/feb/20210218-ocr-deployment.html.

communications.[149] This collaboration between the OhCR and the Ohio National Guard reinforces the tangible benefits of state level initiatives, demonstrating that when cyber expertise is partnered with governmental support, the results are swift, effective, and tailored to the specific needs of the community in crisis.

In assessing the three traditional organizational models above, it becomes clear that each offers unique strengths tailored to specific contexts and challenges. From the flexibility and deep-rooted connections of the SDF to the robust infrastructure and experience of the National Guard, these models have been instrumental in addressing various threats over the years. As the cyber scene continues to evolve with increasingly complex challenges, there is a pressing need to explore emerging organizational models. These new models, like the USSF, could be better equipped to address the multifaceted nature of modern cyber threats, marrying the tried and true practices of traditional models with innovative approaches suited for the modern age.

B. EMERGING ORGANIZATIONAL MODEL

Emerging organizational models adeptly combine the successful characteristics of their predecessors along with modern innovation and rapidly advancing technology. While the recently-established Cybersecurity Safety Review Board is modeled after the practices of the National Transportation Safety Board, crafting a flexible and robust CRCF may demand fresh approaches to guarantee its lasting significance and to serve the interests of both cyber professionals and the public.[150] Beyond specialized entities, broader collaborations between the government and private sector, exemplified by initiatives like H4D and the DIU, endeavor to swiftly integrate cutting-edge technology from hubs like Silicon Valley directly into the tactical forefront.[151] These emergent strategies are tailored for digital operations: they're interconnected, innovation-driven, adaptive, and prioritize digital supremacy. The USSF is the most recent addition to the military services and could offer a blueprint for constructing a CRCF that has been inherently digital from its inception.

[149] Beougher.

[150] Exec. Order No. 14028, Improving the Nation's Cybersecurity.

[151] Hacking for Defense, "About the Hacking for Defense Course."

It can offer novel approaches that are agile, resilient, and digitally supreme to counter the dynamic cyber threats of today and tomorrow.

1. United States Space Force

The USSF, established on December 20, 2019, as the first new military service in over 70 years, exemplifies an organization built from the ground up for the digital age—a prerequisite for any future cyber force.[152] Its interconnected, innovative, adaptive, and digitally dominant strategy could act as a springboard template for the CRCF, allowing it to respond swiftly to significant cyberattacks. The USSF's emphasis on digital technology, talent management, streamlined hierarchy, and specific skill sets equips it to adapt to quickly changing situations and ensures a high probability of success. In its foundational strategy, the USSF embraced lean, agile, and mission-focused attributes to minimize bureaucratic layers, offering valuable insights for a CRCF aiming to be 'born digital'.[153]

Building upon the foundation laid by the USSF, their approach to recruitment, retention, and training exemplifies precision. They aim for a 'digitally fluent' organization, ensuring each member is attuned to the technological demands of the modern age.[154] This dedication is underscored by the USSF's Space Force Vision, delineated by three distinctive tenets tailored for a modern defense force: [155]

- Interconnectedness: An architecture constructed around "data-centric" designs, promoting dispersed collaborative teams.[156]
- Innovation: A persistent commitment to evolving with and adopting emergent technologies, as well as attracting top-tier cyber talent.[157]

[152] SF/CTIO, *U.S. Space Force Vision for a Digital Service* (Washington, DC: United States Space Force, 2021), 2, https://www.spaceforce.mil/News/Article/2597623/space-force-unveils-its-vision-for-a-digital-service/.

[153] SF/CTIO, 2.

[154] SF/CTIO, 4.

[155] SF/CTIO, 5.

[156] SF/CTIO, *U.S. Space Force Vision for a Digital Service*.

[157] SF/CTIO.

- Digital Dominance: Anchoring capabilities within a culture of affirmation, streamlined business processes, and a comprehensive digital engineering ecosystem.[158]

The tenets of the USSF align seamlessly with the foundational framework of a CRCF, mirroring the digital hallmarks of leading tech and IT companies like Google. This alignment not only promotes a common "digital" language but also ensures that processes are universally understood, fostering cohesion among CRCF participants.[159] The three tenets exemplified by the USSF—interconnectedness, innovation, and digital dominance—are vital cornerstones for establishing cohesion within a CRCF. Emphasizing a "data-centric" design, as seen in companies like Microsoft, ensures seamless information flow and incorporates a diverse array of insights, fostering mutual respect and trust needed for cyber operations with dispersed CRCF personnel.[160] Innovation, mirroring the forward-thinking drive of Silicon Valley companies like Tesla, keeps the CRCF at the forefront of cyber defense techniques, creating an environment of continuous innovation capital that retains interest within the mission and its nexus to national security.[161] Lastly, digital dominance, akin to Amazon's customer-centric belief system, provides access to the latest technology and industry standards in cybersecurity.[162] Together, these tenets not only provide CRCF with guiding principles but also foster a profound sense of identity, unity, and purpose, mirroring the digital excellence of leading tech companies.

Building upon the tenets mentioned above, Figure 1 goes into detail on the core digital pillars of the USSF:

---

[158] SF/CTIO.

[159] Barr Seitz, "Learning from Google's Digital Culture," McKinsey & Company, June 1, 2015, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/learning-from-googles-digital-culture.

[160] "Microsoft 365: Data-Centric Security in a Zero Trust World," Innovate Cybersecurity, October 21, 2021, https://innovatecybersecurity.com/news/microsoft-365-data-centric-security-in-a-zero-trust-world/.

[161] Nathan Furr and Jeff Dyer, "Lessons from Tesla's Approach to Innovation," *Harvard Business Review*, February 12, 2020, https://hbr.org/2020/02/lessons-from-teslas-approach-to-innovation.

[162] Daniel Slater, "The Imperatives of Customer-Centric Innovation," Amazon Web Services, Inc., accessed September 28, 2023, https://aws.amazon.com/executive-insights/content/the-imperatives-of-customer-centric-innovation/.

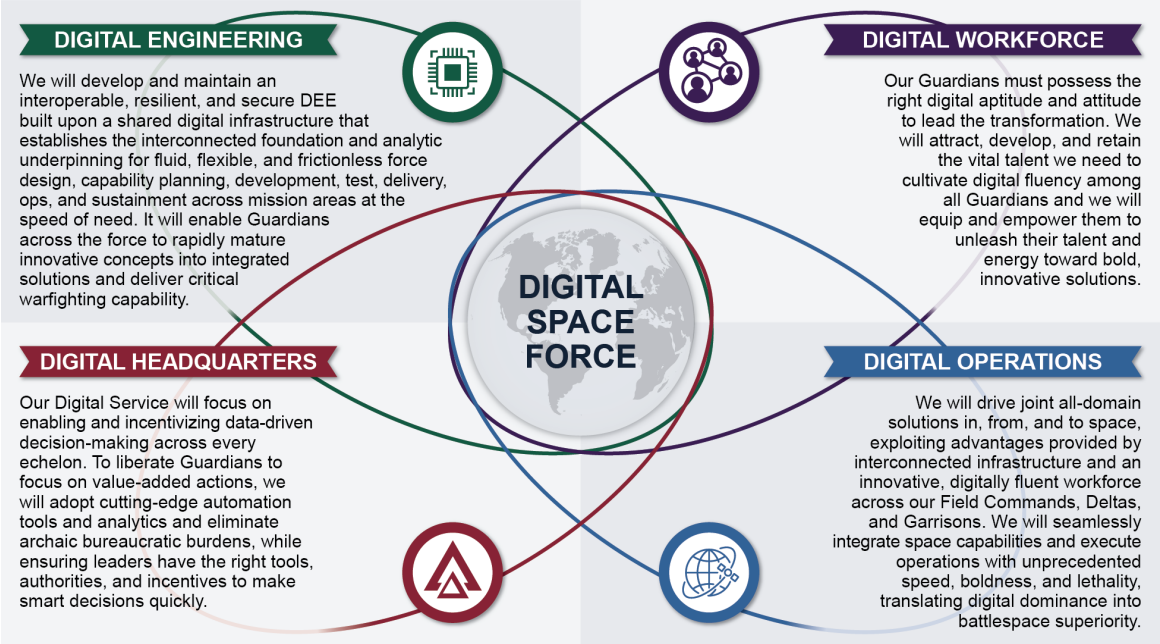

Figure 1. USSF Vision for a Digital Service May 2021[163]

Figure 1 delineates four digital pillars essential for a modernized approach: dedication to digital engineering to ensure advanced infrastructure, much like how companies like Boeing employing cutting-edge digital designs of its T-7A aircraft.[164] The development of a perpetually advancing digital workforce is reminiscent of Google's continuous employee training on emerging technologies.[165] The creation of a digitally integrated virtual digital headquarters for instantaneous collaboration and informed decision-making is similar to the integrated systems used by development and operational teams at Vodafone.[166] Lastly, the infusion of contemporary technology into all operational digital aspects is also seen with Amazon's use of artificial intelligence in logistics and

[163] Source: SF/CTIO, *U.S. Space Force Vision for a Digital Service*: 8.

[164] Courtney Albon, "Boeing: T-7A Program Sees Significant Efficiencies Due to Digital Engineering Tools," *Inside Defense*, June 2020, ProQuest.

[165] Katie Wartman and Trent He, "What Would Be Some Ways to Promote a Learning Culture and Drive Employee Engagement in Continuous Learning?," Cornell University Library, November 1, 2019, https://hdl.handle.net/1813/74577.

[166] Chris Mills, "How the Digital HQ Can Deliver Efficiency and Productivity—Even in Challenging Times," *CIO*, December 15, 2022, https://www.cio.com/article/415597/how-the-digital-hq-can-deliver-efficiency-and-productivity-even-in-challenging-times.html.

supply chain management.[167] Drawing inspiration from the USF's core digital tenets, these principles are pivotal in molding a CRCF adept at addressing today's cybersecurity complexities. By embedding digital engineering from the outset, much like how cybersecurity firm CrowdStrike designs AI-enabled adaptive threat detection systems, the CRCF can cultivate a dynamic ecosystem tailored for simulating and neutralizing diverse cyber threats, laying a sturdy groundwork for adaptability in the future.[168] By championing a digital-first approach, the CRCF not only asserts an immediate prowess against cyber adversaries but can also pave the way for agile, technology-driven operations.

Drawing from the USF's digital principles depicted in the previous graphic, the significance of a simplified organizational framework becomes evident for a CRCF's efficiency, particularly in the face of cyberattacks. The USSF exemplifies this with a flattened hierarchy, diverging from the common skill sets of other military branches.[169] Instead, the USSF focuses on specialized proficiencies, concentrating expertise in six primary areas: acquisition, engineering, cyberspace, intelligence, space operations, and digital software. This targeted focus allows the USSF to remain unwavering in its mission objectives, seamlessly aligning with its six core partner groups within its digitally based principles:

- International Partners
- Joint Partners
- Intelligence Partners
- Civil Partners

[167] Rupa Dash et al., "Application of Artificial Intelligence in Automation of Supply Chain Management," *Journal of Strategic Innovation and Sustainability* 14, no. 3 (2019): 47, ProQuest.

[168] Mmalerato Masombuka, Marthie Grobler, and Bruce Watson, "Towards an Artificial Intelligence Framework to Actively Defend Cyberspace," in *European Conference on Cyber Warfare and Security* (Reading, United Kingdom: Academic Conferences International Limited, 2018), 592, ProQuest.

[169] "Space Force Begins Transition into Field Organizational Structure," United States Space Force, July 24, 2020, https://www.spaceforce.mil/News/Article/2287005/space-force-begins-transition-into-field-organizational-structure/http%3A%2F%2Fwww.spaceforce.mil%2FNews%2FArticle-Display%2FArticle%2F2287005%2Fspace-force-begins-transition-into-field-organizational-structure%2F.

- Academic Partners
- Industry Partners

Each of the six partners above are crucial in cyber operations, allowing CRCF members to connect with groups already established within their full-time or past-career experiences. International Partners, such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, play a crucial role in expanding and strengthening cooperation among foreign companies and other nations.[170] Joint Partners like CYBERCOM are vital for optimizing coordination between public and private capabilities, ensuring defense mechanisms are updated and ready for emerging threats.[171] Integration with the Intelligence Partners like the CTIIC and ODNI ensures real-time threat coordination and proactive defensive measures against potential adversaries. ODNI is the principal agency for intelligence assistance in the event of a cyberattack.[172] In tandem, the CTIIC offers situational awareness, intelligence collaboration, trend analysis, and aids joint efforts for devising strategies to neutralize adversarial cyber threats.[173] Civil Partners such as the CISA pave the way for building enduring relationships in the cyber policy, regulations, and cyber architectures.[174] Collaborating with Academic Partners like Carnegie Melon's CyLab can bridge innovative research and academic initiatives in cybersecurity while cultivating dialogue among subject matter experts across different sectors to enhance global information security and assurance trusted standards in technology.[175] Lastly, Industry Partners like Google's Threat Analysis Group are imperative for the development and delivery of new cyber capabilities and for providing

[170] Barnes, "Implementation of Active Cyber Defense Measures by Private Entities," 37.

[171] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, no. 92 (First Quarter 2019): 12, ProQuest.

[172] Obama, "Presidential Policy Directive – United States Cyber Incident Coordination."

[173] Department of Homeland Security, *National Cyber Incident Response Plan*, 33.

[174] Cybersecurity Infrastructure and Security Agency, *CISA Strategic Intent* (Washington, DC: Cybersecurity Infrastructure and Security Agency, 2019), 5, https://www.cisa.gov/resources-tools/resources/cisa-strategic-intent.

[175] "CyLab Security & Privacy Institute," CyLab Security & Privacy Institute, October 10, 2023, https://www.cylab.cmu.edu/index.html.

real-time insights on emerging threats while collaborating throughout the tech industry to address state-sponsored hacking and influence campaigns as stated in Google's submission in response to the subcommittee questions for the record following the March 2021 hearing. These networked relationships can then be tailored to a specific cyber playbook and/or a prioritized set of cyber skills to be executed when required.

C. CONCLUSION

Throughout this chapter, a range of organizational frameworks were examined, both from traditional and emerging perspectives, to evaluate their strengths, potential adaptations, and applicability in the formation of a CRCF. Traditional models like the National Guard and SDF offer time-tested structures that emphasize state autonomy and community engagement. On the other hand, emerging blueprints, notably the USSF, highlight innovative approaches with a strong focus on digital dominance and agility. Each model offers unique insights and lessons that could shape the design, hierarchy, and philosophy of a future CRCF. The next chapter will focus on international perspectives, with case studies on the cyber reserve forces of the UK and Estonia. By juxtaposing both domestic frameworks and international models, the overarching goal of these two chapters is to distill best practices and effective strategies from across the globe. This cumulative wisdom will then be leveraged to create an American CRCF that stands resiliently against today's digital challenges while reflecting the nation's unique needs and culture.

IV. CASE STUDIES ON FOREIGN CIVILIAN CYBER RESERVE MODELS

While Chapter III provided an in-depth analysis of the potential American models for a CRCF, it becomes essential to explore best practices outside and beyond the U.S. perspective. Cyberattacks see no political or natural borders; many attacks against the United States are initiated from outside its physical boundaries. This reality underscores the importance of partnering with likeminded governments to collectively address and counter these threats, such as NATO. Recognizing that the cybersecurity enterprise is both vast and interconnected, it is sensible to draw insights from international success stories. Chapter IV takes this very approach by focusing on two cyber-centric nations, Estonia and the UK, which have effectively integrated civilian and volunteer expertise into their cyber defense strategies. Invaluable lessons and perhaps hybrid strategies that can further inform and refine the American CRCF blueprint are possible through understanding their frameworks and assessing their efficacies.

A. FOREIGN RESERVE CYBER FORCES

This chapter provides a detailed exploration of the civilian-based cyber forces from Estonia and the UK. Selected for their commendable fusion of the public-private sectors and their rounded governmental strategies, these countries exhibit strong approaches to treating cyberattacks as significant threats to their national security and in the case of Estonia, their overall societal fabric. The UK's Joint Cyber Reserve Force (CRF) was established in 2013 and operates within the British Armed Forces, leveraging cybersecurity talents across sectors to safeguard crucial assets.[176] The Estonian Defence League (EDL)'s Cyber Defence Unit (CDU) was founded in 2011, focusing primarily on national cyber defense.[177] A detailed assessment of these cyber force models could identify legit

[176] "Joint Cyber Reserve Force," Gov.UK, accessed October 6, 2023, https://www.gov.uk/government/groups/joint-cyber-reserve-force.

[177] 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 (CCDCOE), 2013), 8.

strategies and structures that could be instrumental in fortifying American critical infrastructure within the cyber domain.

B. UNITED KINGDOM

The UK's Joint CRF is a volunteer force of UK Commonwealth citizens that resides within the British Armed Forces.[178] The CRF formally stood up as part of the UK's National Cyber Security Strategy to leverage cybersecurity talent within the public and private sectors to protect critical infrastructure.[179] The CRF consists of full-time support personnel, reserves, civil service, and contractors that make up the UK's Whole Force concept.[180] The Whole Force aims to balance an integrated mix of military and civilian talent to deliver the required strategic outcomes of the government.[181] An example of this idea in action was the CRF's contribution to Project OASIS, which developed a national "test and trace" process during the COVID pandemic.[182] Key to the success of the Whole Force is the nexus of private technology sector with the public sector's long-term security goals. The study "Whole Force by Design: Optimizing Defence to Meet Future Challenges" by the Serco Institute said, "Decisive changes are required to advance the Whole Force and that any risks in embracing it are significantly outweighed by potential benefits."[183] This integration spurs innovation within the public-private environment, allowing the CRF to take on multifaceted cybersecurity challenges.

The British approach to fielding a cyber reserve force is similar to the U.S. National Guard or Reserves, requiring people to meet certain pre-requisites prior to joining the CRF. In addition to a traditional vetting process, a prospective member must be eighteen years of age or older, a citizen of the Commonwealth or having lived in the UK for the last ten

[178] Gov.UK, "Joint Cyber Reserve Force."

[179] Strategic Command, "Reserves Day: Our Joint Cyber Reserve Force," GOV.UK, accessed October 6, 2023, https://www.gov.uk/government/news/reserves-day-our-joint-cyber-reserve-force.

[180] Gov.UK, "Joint Cyber Reserve Force."

[181] Gov.UK.

[182] John Gearson et al., *The Whole Force by Design: Optimising Defence to Meet Future Challenges* (Serco Institute, 2020), 68, https://www.sercoinstitute.com/media/87/whole-force-by-design-serco-institute-kcl-report-final-131020.pdf&cd=3&hl=en&ct=clnk&gl=us.

[183] Gearson et al., 3.

years.[184] The CRF application process for the prospective member is in-depth, requiring both an application submission and in-person interview with a Cyber Technical Competency Board from all areas of the cybersecurity enterprise.[185] Once accepted, all members must gain a high-level security clearance, attend weekend duties throughout the year, work between nineteen to twenty-seven days per year within their Reserve Service Days (RSD), and be ready to mobilize during a crisis.[186] This process is time-consuming, but vital in integrating the civilian talent pool into government level cyber protection.

Once recruited, the reservist can leverage their knowledge, skills, and abilities (KSAs) to the needs of the Joint CRF, which has a KSA wish list.[187] Some examples of the CRF KSA wish list include vulnerability assessments, digital forensics, Supervisory Control and Data Acquisition (SCADA) systems, malware engineering, intelligence, software development, cloud architecture, risk analysts, big data, artificial intelligence, and technical surveillance.[188] From there, the cyber reservist is assigned to one of five units located throughout the UK and led by different components of the British Armed Forces. These locations include a Cyber Specialist Unit Corsham–Wiltshire, Joint Cyber Unit Cheltenham–Gloucestershire, Maritime Cyber Unit–Portsmouth Hampshire, Land Information Assurance Group–Corsham Wiltshire, and the 6th Cyber Reserve Squadron–Digby Lincolnshire.[189] These geographically-separated units provide many advantages to members of the CRF, from minimizing their travel from their home for efficient mobilization to staying up-to-date on the latest cyber threats close to their home unit. These characteristics when put together with common American organizational frameworks provide a great model for the United States to further explore.

[184] Gov.UK, "Joint Cyber Reserve Force."

[185] Gov.UK.

[186] Gov.UK.

[187] Gov.UK.

[188] Gov.UK.

[189] Gov.UK.

C. ESTONIA

Estonia is a small country in Northern Europe and considered one of the three countries along with Latvia and Lithuania that make up the Baltic States. Roughly twice the size of New Jersey, Estonia's population of 1.2 million people mostly live in or near the capital of Tallinn.[190] Gaining independence from centuries of external rule in 1918, Estonia was forcibly absorbed into the Soviet Union in 1940 until its collapse in 1991.[191] This newfound independence found common ground with Western values and an enduring sense of territorial defense, both in securing its physical border and cybersecurity.

The founding of the modern Estonian military began in 1918 after expelling both the German army and the Russian Red Army, resulting in the establishment of two national defense organizations.[192] The Estonian Defence Forces preserves the sovereignty of the state while the EDL focuses on territorial defense.[193] The Soviet Union officially disbanded the Estonian military after World War II but was re-established in 1991 after its liberation.[194] Estonia joined both the European Union and NATO in 2004, along with the other Baltic States, further distancing their society from past Russian aggression.[195] These new alliances opened new opportunities for Estonia to collaborate with Western partners, especially in the nascent world of transitional cyber threats.

Following a massive twenty-two day cyberattack on commercial and government networks in 2007, Estonia underwent a country-wide culture shift on protecting its digital

[190] Central Intelligence Agency, "Estonia," The World Factbook, October 3, 2023, https://www.cia.gov/the-world-factbook/countries/estonia/.

[191] Central Intelligence Agency.

[192] Monica M. Ruiz, "Is Estonia's Approach to Cyber Defense Feasible in the United States?," War on the Rocks, January 9, 2018, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.

[193] Monica M. Ruiz, "Establishing Volunteer U.S. Cyber Defense Units: A Holistic Approach," in *2017 International Conference on Cyber Conflict (CyCon U.S.)* (Washington, DC: CyCon U.S., 2017), 46, https://doi.org/10.1109/CYCONUS.2017.8167512.

[194] Ruiz, 46.

[195] Central Intelligence Agency, "Estonia."

infrastructure.[196] As a new alliance member, the EDF established the NATO CCDCOE in Tallinn in 2008, focusing on international cyber defense capabilities, training, and policy.[197] It soon became a world leader in cybersecurity research and cornerstone of NATO's cyber strategy, thrusting Estonia to a world leader in digital innovation. The 2008 formation of the CCDCOE resulted in a country-wide search for cyber talent in support of this NATO effort, fusing the need for cybersecurity talent with the requirement of participating in its nation's national security strategy.[198]

A year later, Estonia's initiative-taking cyber defense strategy manifested with the establishment of the EDL's CDU in 2009, which gained formal recognition by 2011. Open to all Estonian citizens, joining requires a nominal membership fee (twenty euros), age verification, loyalty to the republic, acknowledgment of Estonia's constitutional order, a background check, relevant cybersecurity knowledge or interest, and endorsements from two current EDL-CDU members.[199] Of note, the program does not mandate technical skills or prior military service, which promotes diversity within their talent pool among a small national population. Also, there is no formal enlistment period for service. Members of the EDL-CDU can maintain their membership if they meet the published requirements and remain in good standing unless expelled by leadership due to disciplinary issues.[200] This inclusive approach, combined with foundational cybersecurity training and periodic refreshers, ensures the EDL-CDU remains an adaptable and robust cybersecurity asset.

Today, the EDL-CDU acts as the country's protector of its cyber architecture while teaming up with international partners and educating the public on cyber awareness and detecting on-line misinformation.[201] Since 1993, the Maryland National Guard's 175th

---

[196] Kaska, Osula, and Stinissen, *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy, and Organisational Analysis*, 5.

[197] Michael N. Schmitt, "Introduction," in *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 1, ProQuest.

[198] Ruiz, "Establishing Volunteer U.S. Cyber Defense Units," 48.

[199] Marie Baezner, *Study on the Use of Reserve Forces in Military Cybersecurity* (Zurich, Switzerland: ETH Zurich, 2020), 9, http://hdl.handle.net/20.500.11850/413590.

[200] Baezner, 10.

[201] Kaska, Osula, and Stinissen, *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy, and Organisational Analysis*, 8.

Cyber Operations Group and the EDL forces have engaged in numerous exchanges as part of the National Guard's SPP, participating in multiple cyber training exercises, such as Exercise HEDGEHOG in 2018.[202] Another partnered exercise was the Baltic Blitz in 2023, which focused on cybersecurity best practices, training, and defense.[203] This collaborative endeavor has allowed both Maryland and Estonia to share insights, bolster their cyber defenses, and further cement their longstanding partnership.

Amidst their cyber resilience efforts, Estonia embeds cybersecurity education within its school curricula, facilitating workshops and competitions tailored to cultivate budding cyber professionals.[204] This is outlined in the Republic of Estonia's Cybersecurity Strategy 2019–2022.[205] Tallinn University of Technology (or TalTech for short) and the Center for Cyber Forensics and Cyber Security are at the forefront of this effort, organizing competitions such as KüberPähkel (Cyber Nut) and CyberSpike for 75,000 Estonian youth, ages six to eighteen years old, since 2008.[206] This comprehensive approach makes cybersecurity a way of life for adults and children alike while building long-term resilience within Estonian society as its citizens transition from the educational system to the workforce.[207]

---

[202] Thaddeus Harrington, "Maryland Guard, Estonian Partners Focus on Cyber Defense," Air National Guard, September 22, 2023, https://www.ang.af.mil/Media/Article-Display/Article/3534920/maryland-guard-estonian-partners-focus-on-cyber-defense/ https%3A%2F%2Fwww.ang.af.mil%2FMedia%2FArticle-Display%2FArticle%2F3534920%2Fmaryland-guard-estonian-partners-focus-on-cyber-defense%2F.

[203] Kurt Rauschenberg, "Md. Guard Exercises Cyber Awareness with Estonian Comrades," National Guard, May 18, 2018, https://www.nationalguard.mil/News/Article/1525147/md-guard-exercises-cyber-awareness-with-estonian-comrades/https%3A%2F%2Fwww.nationalguard.mil%2FNews%2FArticle-View%2FArticle%2F1525147%2Fmd-guard-exercises-cyber-awareness-with-estonian-comrades%2F.

[204] Republic of Estonia Ministry of Economic Affairs and Communications, *Cybersecurity Strategy: Republic of Estonia 2019–22* (Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2019), 64.

[205] "Estonian Defence League," Kaitseliit, accessed October 6, 2023, https://www.kaitseliit.ee/en/cyber-unit.

[206] Kate-Riin Kont, "Cyber Literacy Skills of Estonians: Activities and Policies For Encouraging Knowledge-Based Cyber Security Attitudes," *Information & Media* 96 (May 2023): 86, https://doi.org/10.15388/Im.2023.96.67.

[207] Tallinn University of Technology, "CR14 and TalTech Signed an Agreement to Promote Estonian Youth Cyber Defense Competitions | TalTech," Tallinn University of Technology, accessed October 7, 2023, https://taltech.ee/en/news/CR14-and-TalTech-signed-an-agreement-to-promote-Estonian-youth.

D. COMMON THEMES AMONG THE FOREIGN PARTNERS

Amidst rising concerns over the nation's cybersecurity defenses, the U.S.'s Civilian Cybersecurity Reserve Act introduced in 2021 retained language to launch a CRCF pilot project.[208] An analysis of the cybersecurity strategies employed by the UK and Estonia reveals several consistent themes that could be adopted as best practices within the CRCF framework. Despite differences in the size of their forces and variations within the makeup of their volunteer military corps, these themes form the bedrock of a robust cybersecurity approach. The comparative analysis below focuses on these shared attributes, followed by potential American organizational models with similar mission sets. Key themes throughout the analysis encompass a strong emphasis on public-private partnerships, leveraging collective expertise for enhanced defense, profound national pride in safeguarding digital territories, and a dedicated culture of knowledge sharing from Estonia's nuanced hybrid defense to the UK's streamlined force distribution.

1. Robust Public-Private Sector Relationships

Estonia's forward-leaning approach to cybersecurity is evident in its enduring focus on retaining strong public/private partnerships. Despite being a small nation, its agility allows for rapid mobilization against cyber threats. The EDL-CDU collaborates effectively with the government, leveraging the strength of these partnerships to maximize cybersecurity capabilities. For instance, Estonia's Information System Authority (RIA) often works hand-in-glove with the EDL-CDU and other partners while simulating large-scale cyberattack on the country's critical infrastructure.[209] In mid-April 2023, the NATO CCDCOE hosted a pivotal cyber defense exercise in Tallinn. Attracting almost 3,000 participants, the RIA Cyber Security Centre notably coordinated the collaborative efforts of both the Estonian and U.S. teams.[210] This real-time exercise, called Locked Shields

[208] Civilian Cyber Security Reserve Act.

[209] Republic of Estonia, "RIA Coordinates Estonia's Participation in the Large-Scale Exercise Locked Shields 2023 | RIA," Republic of Estonia Information System Authority, April 18, 2023, https://www.ria.ee/en/news/ria-coordinates-estonias-participation-large-scale-exercise-locked-shields-2023.

[210] Republic of Estonia.

2023, tasked teams with prioritizing and safeguarding critical IT infrastructures.[211] Mart Noorma, the Director of NATO CCDCOE, emphasized the importance of collaboration, strategy, and legal acumen in the exercise.[212] He further stated, "Technical specialists cannot solve a cyber crisis alone. Usually, decision-makers and experts from different governmental bodies and walks of life are those who try to repel the attacks. This is why, in addition to cyber defence, we focus on strategy games, legal issues, and crisis communication at Locked Shields."[213] Estonia's success in cybersecurity underscores the indispensable role of collaborative public-private partnerships, as seen in their in-depth simulations and NATO-aligned drills, prioritizing the importance of vital alliances within the public/private sectors.

While Estonia's public sector cyber defense capabilities are robust, the synergy between the EDL-CDU and the private sector further strengthens their cyber resilience. Rather than competing with the private sector, many private companies endorse participation within the EDL-CDU to gain leadership skills, training, and overall cybersecurity experience. To further encourage joint participation, private entities have the option to approach the EDL-CDU for assistance through the State Information Systems Authority (SISA.)[214] This constructive collaboration between the public-private sectors not only fortifies Estonia's cyber defenses, but also ensures the swift mobilization of its available resources when a threat presents itself to Estonia's national security.

The British government understands the importance of relationship building between the military and business communities, which can be somewhat of a lagging trend in the United States. The enactment of the Armed Forces Covenant in 2011 aimed to prioritize the importance and value of this joint relationship.[215] According to the House of Commons Library, the Armed Forces Covenant is "a statement of the moral obligation

[211] Republic of Estonia.

[212] Republic of Estonia.

[213] Republic of Estonia.

[214] Baezner, *Study on the Use of Reserve Forces in Military Cybersecurity*, 9.

[215] Claire Mills and Louisa Brooke-Holland, "The Armed Forces Covenant and Status in Law," House of Commons Library, April 10, 2023, https://commonslibrary.parliament.uk/research-briefings/cbp-9072/.

which exists between the nation, the Government and the Armed Forces." or the promise from that nation to those who serve that they will ensure they are treated fairly.[216] The Armed Forces Covenant can be extended to businesses who support the armed forces community by encouraging its employees to volunteer for reserve service and supporting veterans in private sector opportunities.[217] For example, the BT Group, with headquarters in London, actively supports the armed forces through its Transition Force initiative, which aids service leavers in transitioning to civilian jobs.[218] Recognizing the unique cyber skills many veterans possess, BT Group offers tailored opportunities for them within its cybersecurity divisions. Similarly, Deloitte UK runs a Military Transition and Talent Programme, facilitating the integration of veterans into the corporate world, with veterans finding suitable roles within the firm's expanding cyber efforts.[219] Similar to Estonia, this good faith contract builds trust among the public and private sectors for the common good of the nation's national security goals.

2. National Pride

Estonia adopted an "all-nation" approach to its cybersecurity corps, allowing for all involved to cherish a personal sense of sacrifice in support of their national security policies.[220] The volunteer's opportunity to protect critical infrastructure instills a profound sense of pride in retaining their sovereignty as an independent nation, especially considering Russia's cyber influence operations within the Baltic States. The hybrid civilian-military approach to defend mission critical systems further aligns the important relationship and trust between both groups. As a result, personal relationships are built, allowing for the volunteers to quickly respond to a cyberattack without the delays in a bureaucratic system of national call-ups.

---

[216] Mills and Brooke-Holland, 3.

[217] Mills and Brooke-Holland, 3.

[218] BT, "Transition Force | BT Plc," Transition Force Workshops, accessed October 1, 2023, https://www.bt.com/about/transition-force.

[219] Deloitte, "Upskilling Ex-Military Personnel," accessed October 8, 2023, https://www2.deloitte.com/uk/en/pages/public-sector/articles/upskilling-ex-military-personnel.html.

[220] Ruiz, "Establishing Volunteer U.S. Cyber Defense Units," 48.

Recruiting civilians into the British defense world provides positive second and third order force multiplier effects. Reservists find a higher purpose in defending their nation that may not have had a career path in government due to physical or medical limitations.[221] This prospect opens amazing ways in which a civilian can be a part of a large defense organization while safeguarding national-level priorities. In addition to pay according to rank, CRF members are provided many of the same entitlements and benefits as military personnel.[222] There are also leadership courses available to civilian reserve members by senior military personnel that develop people skills to interact with senior decision-makers. All in all, and regardless of prior military affiliation, the reservists positively contribute to exercises and real-world operations while playing their part to serve King and country.

3. Knowledge Sharing

The EDL-CDU plays a pivotal role in facilitating a culture of continuous knowledge exchange among its volunteers and supporting stakeholders. For instance, their active participation in the Locked Shields exercise, organized by NATO's CCDCOE, serves as a conduit for international collaboration and shared learning.[223] Estonia's Cyber Hygiene program, aimed at enhancing threat awareness among public servants and available in twelve languages, often draws from the expertise within the EDL-CDU.[224] Additionally, Estonia's advanced cyber ranges act as hubs where professionals, including EDL-CDU members, collaborate on evolving cybersecurity tactics.[225] While Estonia's EDL-CDU exemplifies a model of cybersecurity excellence, the CRF offers another compelling approach, seamlessly merging the best practices of the public and private sectors.

---

[221] Strategic Command, "Reserves Day: Our Joint Cyber Reserve Force."

[222] Gov.UK, "Joint Cyber Reserve Force."

[223] Baezner, *Study on the Use of Reserve Forces in Military Cybersecurity*, 9.

[224] e-Estonia, "Free Cyber Hygiene Training in 12 Languages," e-Estonia, n.d., https://e-estonia.com/free-cyber-hygiene-training-in-12-languages/.

[225] Tallinn University of Technology, "CR14 and TalTech Signed an Agreement to Promote Estonian Youth Cyber Defense Competitions | TalTech."

From day one, the CRF emphasizes and encourages each reservist to proactively share their skills, knowledge, and abilities with other members. This culture of information-sharing creates an environment of mentorship among junior and senior leaders, benefiting both the civilian and military members. Knowledge sharing encourages public awareness about cyber threats, promoting a culture of cyber awareness and resilience among the population. Overall, this concept of collaboration is key to this program and a cornerstone of the Joint CRF spirit.

In summary, the incorporation of force multipliers from the UK and Estonian models are vital for enhancing the U.S. cyber force roadmap. One paramount strategy involves fostering genuine partnerships between public and private tech sectors and aiming to bridge any existing gaps. Moreover, it is essential to cultivate an inherent sense of national pride among the volunteers, achieved by immersing them in real-world operations and training opportunities. Unique entitlements further serve to augment this pride. Equally significant is the emphasis on knowledge sharing and training between civilians and governmental bodies, facilitating an environment where learning is reciprocal. As the digital domain continues to evolve, gleaning insights from global best practices can prove instrumental in bolstering the United States' cyber defense strategy.

E. CONCLUSION

As the nation contemplates the formation of a CRCF, it is imperative to craft a uniquely U.S. model, respectful of its constitutional commitments and cognizant of the need for mutual trust in collaboration. Chief among these concerns is understanding the differences in both culture and governmental regulations. Balancing the Fourth Amendment's protections against unwarranted intrusions with the need to establish genuine trust between the government and the private sector introduces intricate challenges in safeguarding both corporate and individual rights. While the best practices from Estonia and the UK can guide the development of a CRCF, it is crucial to tailor these strategies within today's political landscape of the United States. This ensures that the approach not only upholds constitutional principles but also effectively serves national security objectives.

V. CONCLUSION

This thesis sought to identify the core insights drawn from the various models and best practices examined and its applicability to laying the groundwork for an American CRCF. This collection of findings recognizes and highlights the most effective strategies to see this vision evolve from concept to reality. From the National Guard's centuries of organizational acumen and the CRAF's historically successful public-private partnerships to the USSF's twenty-first century operational approaches and SDF's unparalleled talent recruitment and retention methods, each model offers unique building blocks to support a commonsense blueprint. By emphasizing the most effective strategies and approaches from our international peers of Estonia and the UK, this chapter also offers a comprehensive perspective on potential obstacles to avoid during the foundational and initialization stages.

Lastly, recommended research for the future is presented as a provisional CRCF concept of operations (CONOPS); with a table of contents alongside executive summaries for each CONOPS chapter, the thesis provides added insight into a more coherent and strategic direction.

A. FINDINGS: BEST PRACTICES FROM DOMESTIC U.S. ORGANIZATIONS

The following primary findings identify the best in American organizational frameworks and foreign best practices essential for constructing an effective CRCF, to also include anticipated roadblocks along the way. The introduction of the Civilian Cybersecurity Reserve Act in 2021 to establish a CRCF pilot project came at a time of great uncertainty in the nation's ability to protect itself from cyberattacks. The four current operational models discussed below in Table 2 summarize each framework's role to their potential value in a CRCF.

Table 2. Summary of Frameworks and Their Value to a Future CRCF

Framework	Purpose / Description	CRCF Connection
National Guard (Best Organizational Model)	State-based militia with a dual construct, allowing for two chains of command at the state and federal level	Established organization that leverages civilian talent with national objectives
Civil Reserve Air Fleet (Proven Public/Private Partnership)	Voluntary program involving aircraft capability during a national defense related crisis	Established public/private framework that activates in a time of national crisis
State Defense Force (Good Model to Retain Talent Through Volunteerism)	State-based volunteer militia (not paid). All civilian forces, many with prior military or first responder experience. Anyone can join	Framework retains generations of cyber talent through a strong culture of volunteerism
United States Space Force (Required digital ethos)	Newest service that conducts global space operations, intentionally built to quickly adapt to technological changes	Built specifically for a "digital world" and rapid anticipated technological changes

1. Best Organizational Model: The National Guard

Building upon the evidence in this thesis along with hundreds of years of historical precedence, the National Guard's "citizen soldier/airman" spirit, along with its adaptability during a crisis can serve as an organizational blueprint for a CRCF. As discussed in Chapter III, five attributes listed in Table 3 outline the immediate value and common foundations that come with aligning a large civilian group to achieve one common large-scale goal. The attributes outlined in Table 3 are not just abstract concepts; they provide tangible advantages for any civilian considering participation in a CRCF.

Table 3. Potential National Guard Attributes to a CRCF

Strategic Attribute	Value to a CRCF
National Guard Access	The National Guard is community-based and easy to understand for civilians interested in serving in a "part-time" capacity
Distributed and Financially Efficient	Located in virtually every zip code and postured for any member of the CRCF to be a "cyber nomad" and work remotely in defense of their nation
Culturally Innovative	Citizen Soldiers / Airmen bring extensive experience from the private sector into the National Guard "mind hive," creating the perfect balance required in a civilian-based CRCF
Dual-Agility	Inherent connection to talent management within the cyber community
Existing Partnerships	Partners with all cyber-related stakeholders, from Governor's Councils and Congressional Delegates to joint cyber grounds and private enterprise

Starting with the National Guard Access, it is more than just an entry point. The access is a bridge between civilian aspirations and national defense needs. Grounded in a community-centric model, the National Guard stands as a viable option for civilians due to its familiarity and embedded presence within their own cities, towns, and neighborhoods. This familiarity of time and space offers civilians an opportunity to align their personal and professional goals with the broader objective of national security. By enlisting, they could selectively volunteer for missions that mirror their interests, be it defending critical infrastructure or leveraging specialized skills like countering ransomware attacks or denial of service threats. Additionally, linguistic expertise can play a pivotal role in cyber intelligence and operations.

On the other hand, the attribute of being distributed and financially efficient is not just about location; it is about adaptability and responsiveness in a distributed cyber environment. Having National Guard units peppered across the country means that a CRCF can readily tap into diverse local talent pools, enhancing the force's collective competence. The widespread distribution not only ensures representation but also fortifies the concept of a "cyber nomad," enabling CRCF members to effectively contribute from diverse

locations.[226] Cultural innovation is another essential attribute, given the rapidly evolving nature of cybersecurity. The National Guard is not just a military entity, but is enriched by citizen soldiers and airmen who carry vast and varied experience from the private sector.[227] This blend of military discipline and civilian innovation fosters an environment that combines the best of both worlds. It encourages out-of-the-box thinking, necessary for tackling complex cyber challenges, making it ideal for a CRCF which seeks a balance between structured strategies and innovative solutions. The dual-agility of the National Guard emphasizes its adaptability and its robust connection with the broader cyber community. This dual nature ensures that they remain at the forefront of talent management and can swiftly pivot in response to emerging threats or challenges, capitalizing on the dynamism of the civilian cyber sector. Lastly, the National Guard's existing partnerships serve as a testament to its collaborative spirit. With partnerships ranging from the National Guard's SPP and its joint cyber grounds to private enterprises, the CRCF would inherit a robust network of cyber talent.[228] This network could be pivotal in ensuring that the CRCF is always aligned with the broader national cybersecurity strategy, enjoy legislative support, and can effectively collaborate with private enterprises for shared objectives.

2. Proven Public-Private Partnership Framework: CRAF

Chapter III's exploration of the CRAF underlines its potential as a public-private partnership framework, suggesting it could be adapted to serve as a formidable model for the CRCF, both as a strategic cyber deterrent and a blueprint for participant compensation. Aligning the aforementioned organizational elements of the CRAF (legislative, private-public, and severity levels/triggering mechanisms) into the CRCF can provide the same insurance protections in the cyber domain. In addition, the research found that the CRAF acts as an insurance policy for the U.S. by providing additional air transportation assets for future military and humanitarian operations, which can be a powerful deterrent and force

[226] "The Cyber Nomad: Why More Cyber Security Professionals Are Going Digital | Cyber Security Career Advice," CareersinCyber.com, March 8, 2020, https://www.careersincyber.com/article/the-cyber-nomad-why-more-cyber-security-professionals-are-going-digital/.

[227] Forscey and Ruiz, "The Hybrid Benefits of the National Guard."

[228] Forscey and Ruiz.

multiplier in the greater cyber enterprise. This framework can also present a starting point for payment, as all airlines that participate in the CRAF are monetarily compensated by the government. All these attributes, when put together, can provide a starting point should Congress decide to pay CRCF members for their services, or build a hybrid model of volunteers and contractual participants when required.

3. Reliable Framework to Retain Talent: SDF

As discussed in Chapter III, when exploring current and domestic organizational frameworks, the SDF stands out as a compelling option, presenting critical attributes that could significantly bolster the structure and efficacy of a CRCF. The SDF framework offers five essential elements to a future CRCF mission and can serve as an alternative to a nationally controlled line of effort. First, maintaining an SDF is a low-cost endeavor, as most of its force are volunteers. Second, many SDF personnel are either retired from the military or served in a first responder/security related career, providing a common bond and sense of purpose when activated. Third, SDF is not controlled at the federal level, allowing a state or territory's governor to shape the SDF for their particular needs, from hurricane response in Louisiana to wildfire support in Oregon.[229] Fourth, the SDF could be a preferred framework among policy makers looking for more state control or a decentralized model. Lastly, the SDF can align their own existing cybersecurity resources to maximize utility of federal support through a five-step best practice process outlined in the National Cyber Incident Plan of 2016 and the CISA Cyber Playbook of 2021, as discussed in Chapter III. This optional framework can also give more deliberate or crisis action authority to the governors, allowing an already existing group to focus on concerns below state level, such as election integrity and threats to local IT systems.

4. Emerging Framework for the Information Age: USSF

Drawing from Chapter III's analysis, the USSF emerges as a pioneering framework for the information age, offering invaluable insights for crafting the CRCF as a digitally-centric, agile entity attuned to the dynamic world of cybersecurity. Its forward-looking

[229] Pohnel, "State Defense Forces," i.

digital philosophy and focus on partner-building are paramount to the success of a CRCF. Central to the USSF's design is its suite of digital tenets, which make it agile, adaptable, and fiercely contemporary. Digital engineering enables swift adaptation to technological shifts, a trait essential for a potentially geographically-separated CRCF team. Its digital headquarters model promotes centralized decision-making, translating strategic goals into actionable tasks, a format that would give the CRCF the edge in coordinating vast cyber operations. Investing in a digital workforce, as seen in the USSF, ensures that personnel remain on the cutting-edge, a must knowing the highly technical nature of cybersecurity. Moreover, the integration of digital operations melds technology with human insight, a combination vital for predicting and countering intricate cyber threats. Additionally, the flat hierarchy of the USSF fosters open communication and rapid decision-making, which is critical in empowering every CRCF member to actively remain up-to-date on current events and respond to challenges. Lastly, the USSF's focus on six partners in Table 4 are all crucial in cyber operations, allowing CRCF members to connect with groups already established within their full-time or past-career experiences.

Table 4. USSF Partners and Their Value to a CRCF [230]

Group	Value to a CRCF
International Partners	Expand / strengthen cooperation among foreign companies and other nations
Joint Partners	Optimize joint coordination among public/private capabilities
Intelligence Partners	Integrate with the intelligence community on coordinating real-time threats
Civil Partners	Build relationships in cyber, policy, regulations, and architectures
Academics Partners	Work with schools, civic organizations, think tanks, and innovation hubs
Industry Partners	Develop and deliver new cyber capabilities and evolved digital architectures

[230] United States Space Force, *Spacepower: Doctrine for Space Forces* (Washington, DC: United States Space Force, 2020), https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

As Table 4 illustrates, CRCF can match the USSF's multifaceted partnerships, thereby harnessing wide-ranging expertise to fortify its cyber defense infrastructure. Reaching out to international alliances, such as potential future collaboration with the UK's Joint CRF and Estonia's Cyber Reserves promise a global perspective on emerging threats and an opportunity for standardized cyber defenses. Joint operations with other national entities offer the combination of specialized resources and expertise, providing an enriched collaborative force during major cyber incidents. Integration with intelligence communities such as the DOD or NCCIC ensures an initiative-taking stance, equipping the organization with in-depth insights into covert cyber operations and evolving threat actors. Collaborations with tech giants like Google and Amazon Web Services—especially Amazon's "shared responsibility model"—can provide advanced defense tools and strategies, ensuring cloud security and resilient infrastructure.[231] Academic alliances, such as with Purdue's Center for Education and Research in Information Assurance and Security (CERIAS) and Carnegie Mellon's CyLab Security and Privacy Institute.[232] These organizations focus on cutting-edge research, next-generation algorithms, and fresh talent into the CRCF's sphere of influence.[233] By integrating these digital-centric relationships into its framework, a CRCF could begin to develop into an agile, resilient, and formidable force.

B. RECOMMENDATIONS: ADOPTING BEST PRACTICES FROM FOREIGN NATIONS INTO THE AMERICAN PLAYBOOK

Incorporating international best practices into the U.S. cyber defense strategy can provide invaluable insights, counteracting potential insular thinking and drawing from the proven successes of other nations. As with Estonia and the UK, all Western minded countries should stay adaptable and forward-thinking, both within their boundaries and by expanding their perspectives internationally. Obtaining insight and learning from the successes and challenges of foreign partners can offer the United States invaluable insights

[231] "Shared Responsibility Model – Amazon Web Services (AWS)," Amazon Web Services, Inc., accessed October 23, 2023, https://aws.amazon.com/compliance/shared-responsibility-model/.

[232] "About CERIAS," accessed October 23, 2023, https://www.cerias.purdue.edu/.

[233] CyLab Security & Privacy Institute, "CyLab Security & Privacy Institute."

and fresh perspective on building a capability from the ground up. These foreign exchanges and studies of best practices serve as a counter to American "group think" and offer other ideas to refine domestic strategies, enabling nations to build a resilient and robust cyber defense posture. As the United States embarks on fortifying its cyber frontiers, NATO countries like Estonia and the UK provide those applicable lessons.

The success stories of Estonia and the UK highlight three key pillars that can be directly correlated with domestic organizational models: public/private sector collaborations, deep-seated national pride, and the continuous flow of knowledge sharing. The United States, with its history of strong public/private collaborations exemplified by the CRAF, the profound sense of volunteerism embodied by the SDF, the sharing information in the National Guard, and the overall digital backbone of the USSF are well-poised to adapt and integrate these foreign principles and their potential applicability to American systems.

1. Robust Public/Private Sector Relationships in the United States

The United States currently operates multiple public/private partnerships that can amplify current force multipliers. As discussed in chapter 3, the CRAF provides a current example of the government working with the private sector airline industry in achieving national-level priorities. The CRAF is a classic framework that connects public/private partnerships to address vital airlift capabilities during a national-level emergency while providing airlift capability during a national defense related crisis.[234] Estonia's approach outlined in chapter 4 provided examples of businesses that have established protocols to directly engage with the EDL-CDU, illustrating a successful model of public/private interaction. This special relationship not only aids in immediate threat mitigation but also helps in fortifying future defense protocols, ensuring that the private sector remains a proactive stakeholder in the nation's cybersecurity matrix. Substituting cyber-based requirements along with their affiliated government and cyber industry partners as seen in Estonia can see mutual benefit like the airlift needs outlined in the CRAF mission

[234] Air Mobility Command, "Civil Reserve Air Fleet."

statements. The UK's CRF also taps into professionals from the private sector, academia, and retired personnel to harness specialist skills for cybersecurity roles within the military and government. One prime example is their collaboration with leading UK tech companies and universities to conduct advanced cybersecurity research, training programs, and simulated exercises.

By modifying these examples for the domestic market, the American CRCF can initiate similar partnerships with tech giants, such as Google, Amazon Web Services, and Microsoft, to access top-tier cyber talent as seen in National Guard units. By hosting joint cybersecurity exercises, research initiatives, and training programs, the American CRCF can ensure it stays at the forefront of cyber defense techniques. Such an integrated model not only leverages the rapid innovation of the tech industry but also ensures that the national defense apparatus benefits from the latest advancements in real-time. For example, CISA or another agency embedded with DHS can conduct the DOT and USTRANSCOM roles of managing the cyber needs (in lieu of airlift requirements) of the nation alongside private sector entities. This trait is pivotal to bridge the gap between large public entities and fast-moving private industry, allowing a CRCF to remain on the forefront of cyber threats.

2. National Pride

The essence of a successful national CRCF lies not only in harnessing technical prowess but also in evoking a profound sense of national pride and service across multiple generations of cyber talent. In the United States, the spirit of volunteerism, deeply rooted in national pride, is vividly exemplified by the SDF outlined in chapter 3. These SDFs stand as organized, volunteer-driven militias with an illustrious tradition of service in the American narrative. Operating distinctively from the National Guard, they are representative of the combination of citizen volunteerism and homeland defense. Just as Estonia and the UK's civil cyber reserve forces epitomize the synergy between national security and civic participation, the SDFs function as a force multiplier, preserving talent through dedicated volunteerism. Their operational structure resonates with the characteristics of a National Guard unit, ensuring both uniformity and a tried and true

framework for intricate operations. Through these parallel systems, it is evident that the fusion of national pride and cybersecurity are imperative to building a civilian-based cyber force, intertwining civic duty with the defense of American critical infrastructure.

3. Knowledge Sharing

Since the mid-1990s with President Clinton's executive order on protecting critical infrastructure, the U.S. government has emphasized fostering strong partnerships with the private sector to address cyber threats, particularly as most of the nation's critical infrastructure is owned and operated by private entities. Various government agencies, including CISA and the FBI, have long-established programs and initiatives aimed at sharing threat intelligence and best practices with businesses. The emergence of initiatives like CISA's Joint Cyber Defense Collaborative (JCDC) encourages private and public sectors to pool resources in a trusted environment, which highlights a shift toward more cooperative models.[235] This effort underscores the potential of melding government resources with private sector capabilities to confront shared cybersecurity threats. Additionally, the NIST publishes a widely adopted Cybersecurity Framework that aids organizations in managing and mitigating their cyber risks. President Biden, recognizing the evolving and intensifying threats in the digital domain, launched an updated National Cyber Strategy in March 2023 which underscored the necessity of public/private collaboration.[236] The strategy outlines measures to deepen these collaborations, enhance information-sharing, and foster joint initiatives to safeguard American digital assets and individual privacy.[237]

The importance of knowledge sharing in the cyber realm is paramount to enduring cybersecurity. The UK's CRF champions this very principle, cultivating an environment that thrives on mentorship and shared learning. This focus on collaboration not only sharpens skills within the force but also amplifies public awareness and resilience against

[235] Eugenia Lostri, James Andrew Lewis, and Georgia Wood, *A Shared Responsibility: Public-Private Cooperation for Cybersecurity* (Washington, DC: Center for Strategic and International Studies, 2022), https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

[236] White House, *National Cybersecurity Strategy*, 2.

[237] White House, 17.

cyber threats. Furthermore, strategic attributes derived from international models can offer valuable insights for the U.S. Specifically, the National Guard, with its community-driven nature, widespread presence, and innovative spirit, can serve as an ideal vessel to integrate these attributes. It is this harnessing of collective information that can drive a CRCF into overdrive, allowing for the necessary adaptability for a CRCF to remain in-place and become part of its overall strategic doctrine.

C. POTENTIAL AMERICAN ROADBLOCKS IN THE FORMATION OF A CRCF

Adapting the cyber reserve best practices of Estonia and the UK to the U.S as identified in chapter 4 poses significant challenges, from Fourth Amendment and privacy concerns to fostering trust between the government and the private sector. While these foreign models offer valuable insights, an American-centric CRCF necessitates a careful approach in its formation to address its unique legal, cultural, and institutional nuances.

1. Fourth Amendment and Privacy Concerns

The U.S. Constitution imposes significant constraints in the formation of a CRCF, especially as the Fourth Amendment safeguards citizens from unwarranted government intrusions. Such constraints may limit the scope of cyber operations, especially when it comes to domestic monitoring and immediate interventions during a cyberattack. This not only includes access to stored digital information belonging to a U.S. person, but also their hardware, such as a cell phone or laptop. The Supreme Court's unanimous decision in *Riley v. California* in 2014 underscores the importance of personal digital data in the context of the Fourth Amendment.[238] The ruling emphasized that warrantless searches of digital contents, even during arrests, stand against constitutional principles. In this case, the digital information on a personal cell phone was searched by law enforcement without a warrant, violating the victim's Fourth Amendment rights.[239] In another example, a major standoff between Apple and the FBI occurred in 2016 over a locked iPhone belonging to a mass

[238] Alan Butler, "Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights after Riley v. California," *Duke Journal of Constitutional Law & Public Policy* 10, no. 1 (2014): 84, Heinonline.

[239] Butler, 84.

shooter suspect in San Bernardino, CA.[240] The FBI sought Apple's assistance in unlocking the device, believing it contained crucial evidence to further the investigation. Apple resisted, citing concerns over creating a backdoor that would undermine the privacy and security of all iPhone users.[241] This incident underscored the tension between national security needs and individual privacy rights while also highlighting the challenges governmental agencies face when accessing encrypted information during investigations, even in the face of imminent threats. These rulings may hint at the numerous legal intricacies and boundaries that the CRCF would need to navigate, particularly when trying to access or analyze digital data during large-scale cyberattacks, all while upholding the rights of U.S. persons and staying within the confines of American law.

Unique American cultural concerns also come into play. While nations like Estonia (and the UK to a lesser extent) embrace a culture of collective cyber defense, ingraining such a mindset in the individualistic American populace might require another approach. Estonia's all-encompassing digital ID system and national digital backbone called X-Road provides country-wide secure data exchange with the public-private sectors.[242] The overwhelming population of Estonia trust—and believe in—its digital ecosystem and the savings it provides the government. So much so that the Estonian population prefers digital signatures over traditional signatures on paper, saving as much as two percent of the country's GDP.[243] This national confidence in the country's digital backbone is in contrast with the historical distrust and skepticism within U.S. society regarding governmental intelligence gathering and surveillance. There is precedent of illegal intelligence collection in the twentieth century, most famously on Dr. Martin Luther King, Jr. by the FBI before his assassination.[244] Then, there is the example of Edward Snowden's unlawful release of

[240] David Newkirk, "'Apple: Good Business, Poor Citizen': A Practitioner's Response," *Journal of Business Ethics* 151, no. 1 (October 2016): 13, https://doi.org/10.1007/s10551-016-3397-y.

[241] Newkirk, 15.

[242] Gary Anthes, "Estonia: A Model For e-Government," *Communications of the ACM* 58, no. 6 (May 2015): 18, https://doi.org/10.1145/2754951.

[243] Anthes, 18.

[244] Jules Boykoff, "Surveillance, Spatial Compression, and Scale: The FBI and Martin Luther King Jr.," *Antipode* 39, no. 4 (2007): 759, https://doi.org/10.1111/j.1467-8330.2007.00549.x.

highly classified National Security Agency (NSA) mass data collection procedures, and Americans continue to question how to balance between legitimate national security concerns and individual privacy rights.[245] Thus, while nations like Estonia have managed to weave cybersecurity seamlessly into their societal fabric, the U.S. faces the complex challenge of marrying its historic value of individual privacy with the pressing need for a more collective cyber defense.

2. Trust between Government and the Private Sector

On the commercial front, integrating private sector giants like Apple and Microsoft present another layer of complexity. In contrast to Estonia's transparent collaboration with businesses in cybersecurity, American tech firms still exhibit reluctance in sharing sensitive information.[246] Such hesitation can be reminiscent of Apple's standoff with the FBI in 2016 as mentioned above and Microsoft's refusal to comply with a 2013 warrant to release the emails of a suspected drug trafficker.[247] There are also concerns about proprietary, politics, and the procurement of technology. In 2019, the Pentagon awarded the $10 billion-dollar Joint Enterprise Defense Infrastructure (JEDI) cloud computing contract to Microsoft, which was contested by Amazon Web Services (AWS), alleging undue influence from President Trump in the decision-making process.[248] This dispute highlighted the broader challenges of trust and collaboration between U.S. tech giants and the government, particularly when business interests intersect with public procurement. Companies can also be reluctant to share crucial cybersecurity data with the state, fearful that proprietary or competitive intelligence might get inadvertently exposed, thus

[245] Michael Andregg, "Ethical Implications of the Snowden Revelations," *The International Journal of Intelligence, Security, and Public Affairs* 18, no. 2 (July 2016): 110, https://doi.org/10.1080/23800992.2016.1196942.

[246] Matt Apuzzo, David E. Sanger, and Michael S. Schmidt, "Apple and Other Tech Companies Tangle With U.S. Over Data Access," *New York Times*, September 7, 2015, https://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html.

[247] Apuzzo, Sanger, and Schmidt.

[248] Daniel J. Figuenick, "Billions, and Billions, and Billions: Recent Administrations, Cronyism, and the Need for Greater Independence in Contract Awards," *Public Contract Law Journal* 51, no. 4 (Summer 2022): 6, ProQuest.

jeopardizing their market standing.[249] Even well-intentioned legislation—such as the Cybersecurity Information Sharing Act of 2015, which was crafted to streamline information-sharing—can sometimes fall short, such as when personal information from a private server is shared with the government or how to handle emerging technologies like artificial intelligence.[250] In the end, combining the might of both the private sector and the government in a unified cybersecurity front presents the most potent defense against looming cyber threats.[251]

Estonia, with its agile structure, is proficient at rapidly mobilizing resources in the face of cyber threats. This rapid response is significantly attributed to the EDL-CDU, which maintains a symbiotic relationship with the nation's private sector. This collaboration, in turn, merges the nation's tools of diplomacy, information, military prowess, and economic strategies, ensuring a swift and cohesive response to cyber challenges.

Similarly, the United Kingdom has exhibited an acute understanding of the importance of harmony between its military and business sectors. The Armed Forces Covenant, a promise made by the nation to its servicemen and women, embodies this understanding. By extending this covenant to businesses, the UK has fostered an environment wherein employees are not only encouraged to serve in the reserves but also veterans find fruitful opportunities in the civilian world. This pact of trust and mutual respect between the sectors translates directly into bolstered national security. Additionally, the UK's integration of civilians into defense roles echoes a similar sentiment. The nation's approach enables even those who might have been sidelined due to physical or medical constraints to partake in national defense, thereby harnessing untapped potential. The U.S. resonates with this spirit of national pride through its SDF, a manifestation of patriotic volunteerism working synergistically with the National Guard.

---

[249] Jason Mallinder and Peter Drabwell, "Cyber Security: A Critical Examination of Information Sharing versus Data Sensitivity Issues for Organisations at Risk of Cyber Attack," *Journal of Business Continuity & Emergency Planning* 7, no. 2 (Winter2013/2014 2013): 103, http://libproxy.nps.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=94779800&site=ehost-live&scope=site.

[250] Bert Lathrop, "The Inadequacies of the Cybersecurity Information Sharing Act of 2015 in the Age of Artificial Intelligence," *Hastings Law Journal* 71, no. 2 (2020): 516, Heinonline.

[251] Lathrop, 505.

D. FUTURE RESEARCH

The core findings from this thesis function as an initial waypoint to a future CRCF, but as with most early organizational strategies, there are now identified gaps of knowledge which arose because of this research, pressing the need to address core questions to be further explored. It is imperative that these foundational queries are addressed, as they serve as the bedrock of any subsequent planning, and are central to this concept by evolving from the identified best practices into a central, organizational CRCF. For example, at what operational scales—local, state, regional, or national—should the CRCF manifest? Moreover, the intricate dilemma of talent acquisition and retention looms large. This encompasses multi-layered issues ranging from security clearance vetting processes and the importance of cyber certifications to the pivotal decision between a paid, volunteer, or hybrid force. Could the prospect of educational benefits or specialized job training serve as alluring incentives? In synthesizing answers to these questions, a draft CONOPS table of contents emerges as the compass that can shape the trajectory of subsequent research and ensure that the CRCF is not only envisioned but also pragmatically actualized.

The five-part, conceptual CONOPS table of contents listed below can provide additional avenues of approach for future research:

1. Tab 1: Stakeholders and Centers of Gravity

A collaborative approach is imperative to success. Creating a cyber working group from major stakeholders such as the FBI, CISA, CYBERCOM, NCCIC, and the National Cyber Forensics and Training Alliance (NCFTA) could optimize cybersecurity talent in both the public and private sectors to best protect American critical infrastructure from cyberattacks. Complementing this synergy with insights from the congressional CSC's 2019 study fosters a holistic strategy in merging public and private sector strengths to bolster America's defense against cyber threats. Finally, stakeholder mapping cannot forget the best practices and proven force multipliers from the UK and Estonian civilian cyber forces.

2. Tab 2: Organization and Operational Reach

Tab 2 explores prospective civilian cyber organizational models at the state, regional, and federal levels using current frameworks and partner cyber forces. The state-based cyber force can work in small cells which quickly mobilize and assist with local challenges, such as election security. A regional model can align with the Federal Emergency Management Agency (FEMA) or CISA to pool resources and talent. A national cyber force can tackle large-scale cyberattacks and optimize the "whole of government" approach to best protect critical infrastructure. The cost of this effort will rely on the implementation plan, agency overseeing the operation, and the initial size of the force. Staff can allocate the Congressional Research Service to compare National Guard organizations specializing in cybersecurity as initial data points.

3. Tab 3: Recruiting and Retention

In the endeavor to establish a robust CRCF, a pivotal component lies in the processes of recruiting and retaining top-tier cyber talent, which could be the most challenging aspect of building this unique capability. As seen in the governmental cybersecurity enterprise, this line of effort necessitates meticulous research and planning in several key areas. First and foremost is the vetting process for prospective members, ensuring that the CRCF is composed of individuals with not only the requisite skills, but also the character and integrity befitting a national defense initiative. Another area demanding attention is the establishment of minimum educational requirements and certifications. Determining the right balance between formal education and practical experience will be crucial in attracting the required talent pool of recruits. Professional development programs can also play a crucial role, providing CRCF personnel with pathways to climb the professional ladder, attend industry conferences, or gain access to exclusive training sessions. Furthermore, certifications in the cyber domain—such as CISSP, CompTIA Security+, GICSP, CISM, GCIH, and CHFI—can be promoted as benchmarks of excellence within the CRCF. The question of a paid position vs. volunteer work, or a hybrid award model, presents its own complexities. While a volunteer model may attract enthusiastic individuals dedicated to national service, a paid model could

ensure competitiveness in the talent market, especially when compared with lucrative private sector opportunities. Furthermore, once a member is onboarded, how can the government retain that cybersecurity talent conducive to continuous learning, professional growth, and ensuring a clear path of career progression within the CRCF? Each of these areas presents unique challenges and opportunities, and potentially opening lanes of dedicated research to inform decisions that will shape the future of the CRCF.

4. Tab 4: Implementation Plan and Timeline

Many in the public-private sectors are looking at the Presidential 2023 Cyber Security Strategy to be a potential nexus for joint cooperation through immediately implementing four changes at the federal level to immediately shape the national cyber terrain and provide foundational principles for both the public and private sectors. The origin of these recommendations are lessons learned from both the UK and Estonian Cyber forces and the results of the American Cyberspace Solarium Committee in 2021. The first recommended action is to remove barriers to threat-related information-sharing between the government and private sector. This will move the contractual barriers when a network is breached to counter the cyberattack. Second, the United States needs to improve its software supply chain security and establish baseline standards on all future purchased government software. Third, the federal government needs to establish a cybersecurity safety review board that is co-chaired by government and private sector leads, similar to that of the National Transportation Safety Board. Fourth, there needs to be a standardized playbook for cyber incident response that ensures all agencies meet a certain threshold and take unified steps before, during and after a cyberattack.

A phased CRCF implementation over four years with clearly defined milestones to ensure success and adaptability could be a good starting point. It allows the working groups to flex and adapt alongside a technology that changes by the day. In the first two years, policy introduction, stakeholder engagement, and initial recruitment and training would be the focus. The following two years would see the implementation of federal changes and the development of cyber forces at different levels. The final phase would be dedicated to continuous evaluation and optimization of CRCF, adapting to the evolving cyber domain.

Taking measured steps also allows opportunity for feedback, refinement, and course correction. This allows for a more resilient framework to anticipate and counter cyberattacks head on. After all, the primary objective of the CRCF is a forward-looking cyber defense force multiplier against nation-state and non-state threat actors.

In line with Table 5, CRCF legislation, if fully funded and implemented, can provide the first steps of proactive preparedness and strategic collaboration. Drawing insights from international models and capitalizing on the strengths of both public and private sectors, this phased approach could mark a significant leap toward a resilient cyber posture for the U.S.

Table 5. Potential Roadmap: From Congressional Passage to Implementation

Phase 1 – Stakeholder Engagement (1 to 2 Years)	
Year 1	Initiate formal request for the Congressional Homeland Security Committees to engage the Secretary of Homeland Security
	Establish a formal working group from the following agencies: FBI, CISA, CYBERCOM, NCCIC, and NCFTA
	Engage with the Congressional Cyberspace Solarium Commission and formally integrate their CRCF centric findings into long-term goals
Year 2	Research and analyze the successes and challenges of non-American CRCFs such as the British and Estonian civilian cyber forces
	Draft initial policy directives and recommendations
	Launch recruitment drives within the private sector and academia
	Begin training programs for the initial group of recruits (proof of concept)
Phase 2 – Federal Synergy and Force Development (1 to 2 Years)	
Year 3	Integrate CRCF concept of operations into federal cybersecurity policy frameworks
	Broaden recruiting efforts
	Prioritize cyber sectors requiring added protection
	Wargame scenarios using real-world equipment (enhance training modules)
	Integrate capabilities and familiarization training with partner countries
	Publish annual report with current status (initial operating capability, full operating capability, etc.) for final policy push
Year 4	Sponsor and market a nationwide cybersecurity awareness campaign, showcasing CRCF's role
	Finalize policy with federal agencies
	Prepare and submit a 5-year CRCF strategic plan
	Present plan to Congressional Homeland Security Committees and other stakeholders
Phase 3 – Continual Evaluation and Optimization (1 year)	

5. Tab 5: Summary of Information Gaps

Yet, as with any ambitious initiative, the CRCF policy will inevitably face challenges in its implementation and execution. The process of policy evaluation and revision is vital to identify these challenges and ensure the policy's continued relevance and effectiveness. As summarized in the CONOPS table of contents and follow-on executive summaries, some of the challenges in Table 6 need to be addressed prior to policy implementation.

Table 6. Anticipated Challenges Prior to CRCF Approval, Assemblage, and Activation

Challenges Prior to CRCF Implementation	Questions to Address the Challenge
Metrics for Success	Which key performance indicators (KPIs) are best within the cybersecurity enterprise?
Initial Size of the CRCF	How many cybersecurity experts are required to achieve initial strategic outcomes?
Assigned Governmental Agency	Does CISA have the bandwidth to adopt this mission?
	How would a training and recruitment plan be implemented?
	How would the CRCF and lead agency communicate?
	How would this mission be funded
Volunteerism vs. Paid or Hybrid Status	If monetarily compensated, how would it compare to similar roles in a lucrative cyber market?
	Is there enough interest solely based on national pride for a non-pay model similar to local pride in a volunteer fire department?
	Could educational benefits attract younger cyber talent?
Ensuring Long-Term CRCF Mission Funding	Which agency / department will fund this mission? Examples include DOD (NDAA), NSA budget through its collaborative research or the DHS budget through CISA?
Concrete Agreements between Private (Proprietary) and Public Networks	How can the federal government access any privately affiliated networks in an emergency without violating privacy laws

The policy implementation plan not only addresses current vulnerabilities, but lays the groundwork for future resilience, ensuring that the U.S. remains at the forefront of cybersecurity in the twenty-first century. The information outlined in the CONOPs can address the complexity of cyber threats and offer a collaborative approach to cybersecurity. These initiatives are not only encouraging, but also indicate a growing momentum within Washington, D.C., toward the exploration of options and coordination groups focused on cyber-response. This progress is critical for establishing the legal foundation necessary for the realization of a CRCF in the not-so-distant future.

E. FINAL THOUGHTS

The United States stands at a pivotal juncture where both domestic and international best practices can offer invaluable guidance. The National Defense Strategy (NDS) states that, for the first time in the nation's history, the homeland of the United States is no longer a sanctuary against adversarial threats.[252] The Joint Vision 2020 strategy correctly stated the U.S. military would not necessarily sustain a wide technological advantage due to our adversaries' ability to match our capabilities.[253] The four frameworks and their inherent value is in building a provisional CRCF immediately to anticipate tomorrow's acceleration of change and emerging technologies over the next four to six years. In addition to the domestic frameworks, the success accounts from Estonia and the UK underline the imperative of genuine public-private partnerships, national pride through volunteerism, and the relentless pursuit of knowledge. When it comes to protecting our critical infrastructure and digital economy, federal governmental stakeholders must acknowledge not only that the "home" and "away" cyber fight are one and the same, but that optimizing current and future civilian cyber talent is crucial to making it happen. By adapting these initial insights and follow-on research, the outlook of an American civilian cyber force will be robust and agile enough to tackle any forthcoming cyber-based threat.

[252] Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 3, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[253] Mile Petrovski, "Analysis of the Strategic and Operational Concepts Contained in the Joint Vision 2020 of the U.S. Army and the Information Support of the Joint Warfare," *Bezbednosni Dijalozi* 5, no. 1 (June 1, 2014): 99–113, http://periodica.fzf.ukim.edu.mk/sd/SD%2005.1%20(2014)/SD%2005.1.09%20Petrovski,%20M.%20-%20Analysis%20of%20the%20Strategic%20and%20Operational%20Concepts.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Air Mobility Command. "Civil Reserve Air Fleet." Air Mobility Command. Accessed July 19, 2022. https://www.amc.af.mil/About-Us/Fact-Sheets/Display/Article/144025/civil-reserve-air-fleet/.

Albon, Courtney. "Boeing: T-7A Program Sees Significant Efficiencies Due to Digital Engineering Tools." *Inside Defense*, June 2020. ProQuest.

Amazon Web Services, Inc. "Shared Responsibility Model – Amazon Web Services (AWS)." Accessed October 23, 2023. https://aws.amazon.com/compliance/shared-responsibility-model/.

Andregg, Michael. "Ethical Implications of the Snowden Revelations." *The International Journal of Intelligence, Security, and Public Affairs* 18, no. 2 (July 2016): 110–31. https://doi.org/10.1080/23800992.2016.1196942.

Anthes, Gary. "Estonia: A Model For e-Government." *Communications of the ACM* 58, no. 6 (May 2015): 18–20. https://doi.org/10.1145/2754951.

Apuzzo, Matt, David E. Sanger, and Michael S. Schmidt. "Apple and Other Tech Companies Tangle With U.S. Over Data Access." *New York Times*, September 7, 2015. https://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html.

Austin, Greg, ed. *Cyber Security Education: Principles and Policies*. London: Routledge, 2021. https://doi.org/10.4324/9780367822576.

Baezner, Marie. *Study on the Use of Reserve Forces in Military Cybersecurity*. Zurich, Switzerland: ETH Zurich, 2020. http://hdl.handle.net/20.500.11850/413590.

Barnes, Isaac A. "Implementation of Active Cyber Defense Measures by Private Entities: The Need for an International Accord to Address Disputes." Master's thesis, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/61274.

Beougher, Stephanie. "Ohio Cyber Reserve Member Deployed in Cybersecurity Response." *Buckeye Guard Magazine*, February 18, 2021. https://ong.ohio.gov/stories/2021/feb/20210218-ocr-deployment.html.

Bitko, Gordon. "What Public and Private Sector Leaders Can Do to Stop the Next SolarWinds Hack." *Forbes*, December 22, 2020. https://www.forbes.com/sites/gordonbitko/2020/12/22/what-public-and-private-sector-leaders-can-do-to-stop-the-next-solarwinds-hack/.

Bold, Michael. "Hacking for Defense Turns 5." *Army ALT Magazine*, Fort Belvoir, United States: Superintendent of Documents, May 21, 2021. ProQuest.

Boykoff, Jules. "Surveillance, Spatial Compression, and Scale: The FBI and Martin Luther King Jr." *Antipode* 39, no. 4 (2007): 729–56. https://doi.org/10.1111/j.1467-8330.2007.00549.x.

Brill, Alan, and Jonathan Fairtlough. "Fighting the First Battle of Cyberspace Preparedness: Finding Your Reserve Cyber-Warriors." *Information & Security* 44 (February 2019): 9–15. EBSCOhost.

BT. "Transition Force | BT Plc." Transition Force Workshops. Accessed October 1, 2023. https://www.bt.com/about/transition-force.

Butler, Alan. "Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights after Riley v. California." *Duke Journal of Constitutional Law & Public Policy* 10, no. 1 (2014): 83–117. Heinonline.

CareersinCyber.com. "The Cyber Nomad: Why More Cyber Security Professionals Are Going Digital | Cyber Security Career Advice," March 8, 2020. https://www.careersincyber.com/article/the-cyber-nomad-why-more-cyber-security-professionals-are-going-digital/.

Center for Strategic and International Studies. "Significant Cyber Incidents." February 20, 2023. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Central Intelligence Agency. "Estonia." The World Factbook, October 3, 2023. https://www.cia.gov/the-world-factbook/countries/estonia/.

CERIAS. "About CERIAS." Accessed October 23, 2023. https://www.cerias.purdue.edu/.

Chapa, Lilly. "Cyber Workforce Shortcomings..." *Security Systems News* 22, no. 4 (April 2019): 10. ProQuest.

Cohen, Natasha, and Peter W. Singer. "The Need for C3." New America, October 25, 2018. http://newamerica.org/cybersecurity-initiative/reports/need-c3/.

Maintenance of Other Troops, 32 U.S.C. § 109 (1994). https://www.govinfo.gov/app/details/USCODE-1997-title32/USCODE-1997-title32-chap1-sec109.

———. *Cyberspace Solarium Commission – Report*. Washington, DC: Congress, 2020. https://www.solarium.gov/report.

———. *Cyberspace Solarium Commission: Legislative Proposals*. Washington, DC: Congress, 2020. https://www.solarium.gov/report.

Cronk, Terri Moon. "Carter: DOD, Private-Sector Tech Innovation Keep U.S. Ahead." DOD News, March 3, 2016. https://www.defense.gov/News/News-Stories/Article/Article/685675/carter-dod-private-sector-tech-innovation-keep-us-ahead/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F685675%2Fcarter-dod-private-sector-tech-innovation-keep-us-ahead%2F.

Cyber Threat Intelligence Integration Center. "Organization: Cyber Threat Intelligence Integration Center." National Counterterrorism Center. Accessed July 31, 2023. https://www.dni.gov/index.php/nctc-who-we-are/organization/241-about/organization/cyber-threat-intelligence-integration-center.

Cybersecurity and Infrastructure Security Agency. *CISA Cybersecurity Strategic Plan FY2024–2026*. Washington, DC: Cybersecurity and Infrastructure Security Agency, 2023. https://www.cisa.gov/cybersecurity-strategic-plan&cd=13&hl=en&ct=clnk&gl=us.

———. *Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*. Washington, DC: Cybersecurity and Infrastructure Security Agency, November 2021. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

———. "Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)." Cybersecurity and Infrastructure Security Agency, January 5, 2021. https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

———. *CISA Strategic Intent*. Washington, DC: Cybersecurity Infrastructure and Security Agency, 2019. https://www.cisa.gov/resources-tools/resources/cisa-strategic-intent.

CyLab Security and Privacy Institute. "CyLab Security & Privacy Institute." October 10, 2023. https://www.cylab.cmu.edu/index.html.

Dash, Rupa, Mark McMurtrey, Carl Rebman, and Upendra K. Kar. "Application of Artificial Intelligence in Automation of Supply Chain Management." *Journal of Strategic Innovation and Sustainability* 14, no. 3 (2019): 43–53. ProQuest.

Defense Innovation Unit. "About DIU." Defense Innovation Unit. Accessed July 20, 2022. https://www.diu.mil/about.

Deloitte. "Upskilling Ex-Military Personnel." Accessed October 8, 2023. https://www2.deloitte.com/uk/en/pages/public-sector/articles/upskilling-ex-military-personnel.html.

Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*. Washington, DC: Department of Defense, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Department of Homeland Security. *National Cyber Incident Response Plan*. Washington, DC: Department of Homeland Security, 2016. https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

Department of Transportation. "Civil Reserve Air Fleet." November 20, 2020. https://www.transportation.gov/mission/administrations/intelligence-security-emergency-response/civil-reserve-airfleet-allocations.

Dziwisz, Dominika. "Cyber Pearl Harbor Is Not Coming Us Politics Between War and Peace." *Politeja* 4, no. 79 (2022): 111–29. ProQuest.

e-Estonia. "Free Cyber Hygiene Training in 12 Languages." e-Estonia, n.d. https://e-estonia.com/free-cyber-hygiene-training-in-12-languages/.

Exec. Order No. 14028. Improving the Nation's Cybersecurity (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Figuenick, Daniel J. "Billions, and Billions, and Billions: Recent Administrations, Cronyism, and the Need for Greater Independence in Contract Awards." *Public Contract Law Journal* 51, no. 4 (Summer 2022): 599–622. ProQuest.

Forscey, David, and Monica M. Ruiz. "The Hybrid Benefits of the National Guard." Lawfare, July 23, 2019. https://www.lawfaremedia.org/article/hybrid-benefits-national-guard.

Frandell, Ashlee, and Mary Feeney. "Cybersecurity Threats in Local Government: A Sociotechnical Perspective." *The American Review of Public Administration* 52, no. 8 (November 2022): 558–72. https://doi.org/10.1177/02750740221125432.

Furnell, Steven. "The Cybersecurity Workforce and Skills." *Computers & Security* 100 (January 2021): 1–7. https://doi.org/10.1016/j.cose.2020.102080.

Furr, Nathan, and Jeff Dyer. "Lessons from Tesla's Approach to Innovation." *Harvard Business Review*, February 12, 2020. https://hbr.org/2020/02/lessons-from-teslas-approach-to-innovation.

Gallagher, Robert E., Gerald F. Burch, and John H. Batchelor. "United States Civil Reserve Air Fleet (CRAF): A Brief History—Formation, Functionality, and Future." *Transportation Research Record* 2676, no. 4 (April 2008): 473–82. https://doi.org/10.1177/03611981211061553.

———. "United States Civil Reserve Air Fleet (CRAF): A Brief History—Formation, Functionality, and Future." *Transportation Research Record: Journal of the Transportation Research Board* 2676, no. 4 (April 2022): 473–82. https://doi.org/10.1177/03611981211061553.

Gearson, John, Philip Berry, Joe Devanny, and Nina Musgrave. *The Whole Force by Design: Optimising Defence to Meet Future Challenges*. Serco Institute, 2020. https://www.sercoinstitute.com/media/87/whole-force-by-design-serco-institute-kcl-report-final-131020.pdf&cd=3&hl=en&ct=clnk&gl=us.

Gerstell, Glenn S. "Biden's New Cyber Strategy Will Acknowledge an Essential Truth: Market Forces Aren't Enough." *Barrons*, February 26, 2023. https://www.barrons.com/articles/biden-new-cyber-strategy-market-forces-cybersecurity-51675459082.

González-Manzano, Lorena, José M. de Fuentes, Cristina Ramos, Ángel Sánchez, and Florabel Quispe. "Identifying Key Relationships between Nation-State Cyberattacks and Geopolitical and Economic Factors: A Model." *Security and Communication Networks* 2022 (June 2022): 1–11. https://doi.org/10.1155/2022/5784674.

Gov.UK. "Joint Cyber Reserve Force." Accessed October 6, 2023. https://www.gov.uk/government/groups/joint-cyber-reserve-force.

Hacking for Defense. "About the Hacking for Defense Course." Accessed July 20, 2022. https://www.h4d.us/about-h4d.

Harrington, Thaddeus. "Maryland Guard, Estonian Partners Focus on Cyber Defense." Air National Guard, September 22, 2023. https://www.ang.af.mil/Media/Article-Display/Article/3534920/maryland-guard-estonian-partners-focus-on-cyber-defense/https%3A%2F%2Fwww.ang.af.mil%2FMedia%2FArticle-Display%2FArticle%2F3534920%2Fmaryland-guard-estonian-partners-focus-on-cyber-defense%2F.

Haskell, Bob. "State Guards." *National Guard Magazine*, June 2022. https://www.ngaus.org/magazine/state-guards.

Hershkowitz, Martin. *Available State Defense Force After Action Reports from Hurricanes Katrina and Rita Deployments*. Germantown, MD: State Defense Force Publication Center, 2006. https://webcache.googleusercontent.com/search?q=cache:eBcK-23xVDgJ:https://apps.dtic.mil/sti/tr/pdf/ADA496872.pdf&cd=10&hl=en&ct=clnk&gl=us.

Hodgson, Quentin E, Aaron Clark-Ginsberg, Zachary Haldeman, Andrew Lauland, Ian Mitch, United States, Rand Corporation Cybersecurity & Infrastructure Security Agency, and Homeland Security Operational Analysis Center. *Managing Response to Significant Cyber Incidents: Comparing Event Life Cycles and Incident Response Across Cyber and Non-Cyber Events*. RRA1265-4. Santa Monica, CA: RAND, 2022. www.rand.org/t/RRA1265-4.

Hubbard, Tony, Geoffrey L. Weber, and Jeffrey C. Steinhoff. "Protecting Data Assets in a Perilous Cyber World." *Journal of Government Financial Management* 66, no. 3 (September 2017): 26–31. EBSCOhost.

Huhn, Heidi L. "Defending Infrastructure against Cyber Attacks through Qualified Cybersecurity Professionals in the Federal Government: A Case Study." *ProQuest Dissertations and Theses*. Dissertation, Capella University, 2020. ProQuest.

Innovate Cybersecurity. "Microsoft 365: Data-Centric Security in a Zero Trust World." October 21, 2021. https://innovatecybersecurity.com/news/microsoft-365-data-centric-security-in-a-zero-trust-world/.

Ishmael, Andrew R. "A Qualitative Case Study on the Retention of Qualified Cybersecurity Professionals." PhD diss., Capitol Technology University, 2021. ProQuest.

Janofsky, Adam. "Fighting the Bad Guys Daily: Why Cybersecurity Teams Focus on Managing Stress." *WSJ Pro. Cyber Security*, May 22, 2018. ProQuest.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist." *Journal of Strategic Studies* 42, no. 2 (February 2019): 212–34. https://doi.org/10.1080/01402390.2018.1559152.

Kaitseliit. "Estonian Defence League." Accessed October 6, 2023. https://www.kaitseliit.ee/en/cyber-unit.

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 (CCDCOE), 2013.

Kesan, Jay P., and Linfeng Zhang. "An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures, and Cyber Losses." *IEEE Transactions on Emerging Topics in Computing* 9, no. 2 (April 2021): 582–96. https://doi.org/10.1109/TETC.2019.2915098.

Kont, Kate-Riin. "Cyber Literacy Skills of Estonians: Activities and Policies For Encouraging Knowledge-Based Cyber Security Attitudes." *Information & Media* 96 (May 2023): 80–94. https://doi.org/10.15388/Im.2023.96.67.

Lathrop, Bert. "The Inadequacies of the Cybersecurity Information Sharing Act of 2015 in the Age of Artificial Intelligence." *Hastings Law Journal* 71, no. 2 (2020): 501–33. Heinonline.

Lostri, Eugenia, James Andrew Lewis, and Georgia Wood. *A Shared Responsibility: Public-Private Cooperation for Cybersecurity*. Washington, DC: Center for Strategic and International Studies, 2022. https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.

Mallinder, Jason, and Peter Drabwell. "Cyber Security: A Critical Examination of Information Sharing versus Data Sensitivity Issues for Organisations at Risk of Cyber Attack." *Journal of Business Continuity & Emergency Planning* 7, no. 2 (July 2013): 103–11. EBSCOhost.

Marks, Joseph, and Aaron Schaffer. "The U.S. Isn't Getting Ahead of the Cyber Threat, Experts Say." *Washington Post*, June 6, 2022. https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/.

Masombuka, Mmalerato, Marthie Grobler, and Bruce Watson. "Towards an Artificial Intelligence Framework to Actively Defend Cyberspace." In *European Conference on Cyber Warfare and Security*, 589–596, XIII. Reading, United Kingdom: Academic Conferences International Limited, 2018. ProQuest.

Matthews, Earl. "Incoming: A Model for Building a Civilian Reserve Cyber Corps." *Signal Magazine*, December 1, 2017. http://url.afcea.org/December17.

Mills, Chris. "How the Digital HQ Can Deliver Efficiency and Productivity—Even in Challenging Times." *CIO*, December 15, 2022. https://www.cio.com/article/415597/how-the-digital-hq-can-deliver-efficiency-and-productivity-even-in-challenging-times.html.

Mills, Claire, and Louisa Brooke-Holland. "The Armed Forces Covenant and Status in Law," House of Commons Library, April 10, 2023. https://commonslibrary.parliament.uk/research-briefings/cbp-9072/.

Nakasone, Paul M. "A Cyber Force for Persistent Operations." *Joint Force Quarterly*, no. 92 (First Quarter 2019): 10–22. ProQuest.

National Guard. *2022 National Guard Bureau Posture Statement*. Washington, DC: National Guard, 2022. https://www.nationalguard.mil/Features/Posture-Statement/.

———. "How We Began." November 2020. https://www.nationalguard.mil/About-the-Guard/How-We-Began/.

National Security Council. *Critical Infrastructure Protection.* Presidential Decision Directive/NSC-63. Washington, DC: National Security Council, 1998. https://irp.fas.org/offdocs/pdd/pdd-63.htm.

Newkirk, David. "'Apple: Good Business, Poor Citizen': A Practitioner's Response." *Journal of Business Ethics* 151, no. 1 (October 2016): 13–16. https://doi.org/10.1007/s10551-016-3397-y.

Nicastro, Luke A. *Defense Primer: United States Transportation Command*. CRS Report No. IF11479. Washington, DC: Congressional Research Service, 2020. https://crsreports.congress.gov/product/pdf/IF/IF11479.

Norris, Donald F., Laura Mateczun, Anupam Joshi, and Tim Finin. "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity." *Public Administration Review* 79, no. 6 (December 2019): 895–904. https://doi.org/10.1111/puar.13028.

Obama, Barak. "Executive Order – Commission on Enhancing National Cybersecurity." The White House, February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

———. "Presidential Policy Directive – United States Cyber Incident Coordination," The White House, July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Office of the Director of National Intelligence. "Who We Are – ODNI." The Cyber Threat Intelligence Integration Center. Accessed July 31, 2023. https://www.dni.gov/index.php/ctiic-who-we-are.

Office of the Inspector General of the Intelligence Community. *Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015*. Washington, DC: Office of the Inspector General of the Intelligence Community, 2021. https://www.dni.gov/files/ICIG/Documents/Publications/Reports/2022/CISA_Joint_Final.pdf.

O'Loughlin, Matthew S. "Three If By Internet: Exploring the Utility of a Hacker Militia." Master's thesis, Naval Postgraduate School, 2017. http://hdl.handle.net/10945/53027.

Perera, Srinath, Xiaohua Jin, Alana Maurushat, and Joe Opoku De-Graft. "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks." *Informatics* 9, no. 1 (March 2022): 28. ProQuest.

Peters, Heidi. *Afghanistan Evacuation: The Civil Reserve Air Fleet (CRAF) and the Defense Production Act (DPA)*. CRS Report No. IN11731. Washington, DC: Congressional Research Service, 2021. https://crsreports.congress.gov/product/pdf/IN/IN11731.

Petrovski, Mile. "Analysis of the Strategic and Operational Concepts Contained in the Joint Vision 2020 of the U.S. Army and the Information Support of the Joint Warfare." *Bezbednosni Dijalozi* 5, no. 1 (June 1, 2014): 99–113. http://periodica.fzf.ukim.edu.mk/sd/SD%2005.1%20(2014)/SD%2005.1.09%20Petrovski,%20M.%20-%20Analysis%20of%20the%20Strategic%20and%20Operational%20Concepts.pdf.

Pohnel, Jonathan R. "State Defense Forces and Their Role in American Homeland Security." Master's thesis, Naval Postgraduate School, 2015. https://hdl.handle.net/10945/45242.

PricewaterhouseCoopers. "Biden's Executive Order on Cybersecurity: What's in It and Who Should Be Ready for It." 2023. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/bidens-executive-order-cybersecurity.html.

———. "U.S. Conducts First Hunt Forward Operation in Lithuania." U.S. Cyber Command, May 4, 2022. https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3020430%2Fus-conducts-first-hunt-forward-operation-in-lithuania%2F.

Ramezan, Christopher A. "Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field." *Journal of Information Systems Education* 34, no. 1 (Winter 2023): 94–105. ProQuest.

Rauschenberg, Kurt. "Md. Guard Exercises Cyber Awareness with Estonian Comrades." National Guard, May 18, 2018. https://www.nationalguard.mil/News/Article/1525147/md-guard-exercises-cyber-awareness-with-estonian-comrades/https%3A%2F%2Fwww.nationalguard.mil%2FNews%2FArticle-View%2FArticle%2F1525147%2Fmd-guard-exercises-cyber-awareness-with-estonian-comrades%2F.

Republic of Estonia. "RIA Coordinates Estonia's Participation in the Large-Scale Exercise Locked Shields 2023 | RIA." Republic of Estonia Information System Authority, April 18, 2023. https://www.ria.ee/en/news/ria-coordinates-estonias-participation-large-scale-exercise-locked-shields-2023.

Republic of Estonia Ministry of Economic Affairs and Communications. *Cybersecurity Strategy: Republic of Estonia 2019–22*. Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2019.

Rishikof, Harvey. "All That Which Is Old, Is New Again – Unlearned Lessons about Metrics of Success in Cyber." *The Cyber Defense Review* 7, no. 1 (2022): 121–28. https://www.jstor.org/stable/48642044.

Roper, Scott T. "U.S. National Cyberstrategy and Critical Infrastructure: The Protection Mandate and Its Execution." Master's thesis, Naval Postgraduate School, 2013. http://hdl.handle.net/10945/37703.

Rosen, Jacky. "Rosen's Bipartisan Bill to Establish Civilian Cybersecurity Reserve Passes Senate Committee Unanimously." Senator Jacky Rosen, July 14, 2021. https://www.rosen.senate.gov/rosens-bipartisan-bill-establish-civilian-cybersecurity-reserve-passes-senate-committee-unanimously.

———. S.1324 – 117th Congress (2021-2022): Civilian Cybersecurity Reserve Act, Pub. L. No. S.1324, 117th Cong. (2022). https://www.congress.gov/bill/117th-congress/senate-bill/1324.

Ruiz, Monica M. "Establishing Volunteer U.S. Cyber Defense Units: A Holistic Approach." In *2017 International Conference on Cyber Conflict (CyCon U.S.)*, 45–58. Washington, DC: CyCon U.S., 2017. https://doi.org/10.1109/CYCONUS.2017.8167512.

———. "Is Estonia's Approach to Cyber Defense Feasible in the United States?" War on the Rocks, January 9, 2018. https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.

Sager, Michelle. *High- Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*. GAO-23-106203. Washington, DC: Government Accountability Office, 2023. https://files.gao.gov/reports/GAO-23-106203/index.html#top.

Schmitt, Michael N. "Introduction." In *Tallinn Manual on the International Law Applicable to Cyber Warfare*, chap. 1. New York: Cambridge University Press, 2013. ProQuest.

Schwartau, Winn. "Asymmetrical Adversaries." *Orbis* 44, no. 2 (2000): 197–205. https://doi.org/10.1016/S0030-4387(00)00018-1.

Seitz, Barr. "Learning from Google's Digital Culture." McKinsey & Company, June 1, 2015. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/learning-from-googles-digital-culture.

SF/CTIO. *U.S. Space Force Vision for a Digital Service*. Washington, DC: United States Space Force, 2021. https://www.spaceforce.mil/News/Article/2597623/space-force-unveils-its-vision-for-a-digital-service/.

Simon, Ian G. "Effectiveness of National Cyber Policy to Strengthen the Security and Resilience of Critical Infrastructure Against Cyber Attacks." Master's thesis, Naval Postgraduate School, 2020. http://hdl.handle.net/10945/66140.

Slater, Daniel. "The Imperatives of Customer-Centric Innovation." Amazon Web Services, Inc. Accessed September 28, 2023. https://aws.amazon.com/executive-insights/content/the-imperatives-of-customer-centric-innovation/.

Strategic Command. "Reserves Day: Our Joint Cyber Reserve Force." GOV.UK. Accessed October 6, 2023. https://www.gov.uk/government/news/reserves-day-our-joint-cyber-reserve-force.

Sullivan, John P., and James J. Wirtz. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, 29–38, 2015. https://hdl.handle.net/10945/59143.

Tallinn University of Technology. "CR14 and TalTech Signed an Agreement to Promote Estonian Youth Cyber Defense Competitions | TalTech." Tallinn University of Technology. Accessed October 7, 2023. https://taltech.ee/en/news/CR14-and-TalTech-signed-an-agreement-to-promote-Estonian-youth.

Taylor, Ahiah. "There's a Huge Surge in Hackers Holding Data for Ransom, and Experts Want Everyone to Take These Steps." *Fortune*, February 17, 2022. https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/#:~:text=Governments.

Theohary, Catherine. *Defense Primer: Cyberspace Operations*. CRS Report No. IF10537. Washington, DC: Congressional Research Service, 2022. https://crsreports.congress.gov/product/details?prodcode=IF10537.

Underwood, Kimberly. "CISA's Cybersecurity Advisory Committee Pivots to Meet the Threat." AFCEA International, June 1, 2023. https://www.afcea.org/signal-media/cyber-edge/cisas-cybersecurity-advisory-committee-pivots-meet-threat.

United States Space Force. "Space Force Begins Transition into Field Organizational Structure." July 24, 2020. https://www.spaceforce.mil/News/Article/2287005/space-force-begins-transition-into-field-organizational-structure/

———. *Spacepower: Doctrine for Space Forces*. Washington, DC: United States Space Force, 2020. https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

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

Vaughan, Ann. "Hacking for Defense Turns 5 – USAASC." United States Army Acquisition Support Center, May 21, 2021. https://asc.army.mil/web/news-hacking-for-defense-turns-5/.

Vergun, David. "App Aims to Match Reserve, Guard Talent With DOD Needs." DOD News, June 29, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2675967/app-aims-to-match-reserve-guard-talent-with-dod-needs/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F2675967%2Fapp-aims-to-match-reserve-guard-talent-with-dod-needs%2F.

Vest, Bonnie M. "'I Am a Citizen Soldier': Negotiating Civilian and Military in the Post-9/11 National Guard." Ph.D., State University of New York at Buffalo, 2012. ProQuest.

Wartman, Katie, and Trent He. "What Would Be Some Ways to Promote a Learning Culture and Drive Employee Engagement in Continuous Learning?," Cornell University Library, November 1, 2019. https://hdl.handle.net/1813/74577.

White House. "Fact Sheet: The Biden-Harris Administration's National Security Strategy," 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/.

———. *National Cybersecurity Strategy*. Washington, DC: White House, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Zadelhoff, Marc van. "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It." *Harvard Business Review*, May 4, 2017. https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California