NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPLEMENTATION OF ACTIVE CYBER DEFENSE MEASURES BY PRIVATE ENTITIES: THE NEED FOR AN INTERNATIONAL ACCORD TO ADDRESS DISPUTES

by

Isaac A. Barnes

December 2018

Thesis Advisor: Shannon A. Brown
Second Reader: Lynda A. Peters (contractor)

Approved for public release. Distribution is unlimited.

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 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE IMPLEMENTATION OF ACTIVE CYBER DEFENSE MEASURES BY PRIVATE ENTITIES: THE NEED FOR AN INTERNATIONAL ACCORD TO ADDRESS DISPUTES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Isaac A. Barnes	
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)

Cybersecurity is a national security issue. Passive cyber defense measures are no longer sufficient. This thesis uses options analysis to consider different courses of action for the employment of active cyber defense measures. The Active Cyber Defense Certainty Act, with minor changes, will strengthen the collective cybersecurity posture of entities worldwide by increasing the identification of those perpetrating cyberspace acts. Alone, it does not address the legitimate concerns of proponents and opponents alike. It needs to be coupled with the Cyber Diplomacy Act of 2017, which creates an office within the Department of State to negotiate cyber matters globally on behalf of the United States. While these two acts are stronger together, no single entity within the United States fully addresses America's cybersecurity policy. As the attacks on the World Trade Center in 2001 necessitated the creation of a Director of National Intelligence to coordinate the intelligence community, the current state of cybersecurity necessitates the creation of a national director of cybersecurity. The three concepts create a holistic approach to U.S. cybersecurity, but an entity must mitigate disputes between nations. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) facilitated the writing of the *Tallinn Manual 2.0*. Coupled with the Budapest Convention on Cybercrime as a framework, the CCDCOE has the ability to serve as the entity to mitigate those disputes.

14. SUBJECT TERMS Active Cyber Defense Certainty Act, ACDC Act, Cyber Diplomacy Act of 2017, Cyber Diplomacy Act, Representative Tom Graves, Representative Kyrsten Sinema, Representative Edward Royce, NATO, CCDCOE, National Director of Cybersecurity, active cyber defense, cyberspace, cyber diplomacy, cybersecurity, active cyber defense measures, implementation, cyber-attacks, cybercrime, Budapest Convention on Cybercrime	**15. NUMBER OF PAGES** 85
	16. PRICE CODE

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

IMPLEMENTATION OF ACTIVE CYBER DEFENSE MEASURES BY PRIVATE ENTITIES: THE NEED FOR AN INTERNATIONAL ACCORD TO ADDRESS DISPUTES

Isaac A. Barnes
Assistant to the Special Agent in Charge, U.S. Secret Service
Department of Homeland Security
BS, U.S. Military Academy, 1994

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 2018**

Approved by: Shannon A. Brown
Advisor

Lynda A. Peters
Second Reader

Erik J. Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cybersecurity is a national security issue. Passive cyber defense measures are no longer sufficient. This thesis uses options analysis to consider different courses of action for the employment of active cyber defense measures. The Active Cyber Defense Certainty Act, with minor changes, will strengthen the collective cybersecurity posture of entities worldwide by increasing the identification of those perpetrating cyberspace acts. Alone, it does not address the legitimate concerns of proponents and opponents alike. It needs to be coupled with the Cyber Diplomacy Act of 2017, which creates an office within the Department of State to negotiate cyber matters globally on behalf of the United States. While these two acts are stronger together, no single entity within the United States fully addresses America's cybersecurity policy. As the attacks on the World Trade Center in 2001 necessitated the creation of a Director of National Intelligence to coordinate the intelligence community, the current state of cybersecurity necessitates the creation of a national director of cybersecurity. The three concepts create a holistic approach to U.S. cybersecurity, but an entity must mitigate disputes between nations. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) facilitated the writing of the *Tallinn Manual 2.0*. Coupled with the Budapest Convention on Cybercrime as a framework, the CCDCOE has the ability to serve as the entity to mitigate those disputes.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....1
B. RESEARCH QUESTION....3
C. RESEARCH DESIGN....3
D. CHAPTER OVERVIEW....5

II. LITERATURE REVIEW....7
A. DEFINING ACTIVE CYBER DEFENSE....8
B. CYBER THREAT LANDSCAPE....9
C. ACTIVE AND PASSIVE CYBER DEFENSE MEASURES....12
D. EXISTING AND PROPOSED LEGISLATION....18
E. LEGAL ANALYSIS....20
1. Domestic Legal Analysis....21
2. International Legal Analysis....23
3. Law of Armed Conflict....25
F. DETERRENCE THEORY....26
G. CONCLUSION....29

III. COURSES OF ACTION....31
A. COURSE OF ACTION A: STATUS QUO....31
B. COURSE OF ACTION B: NO INTERNATIONAL DISPUTE MITIGATION BODY....31
C. COURSE OF ACTION C: INTERNATIONAL BODY TO ADDRESS CYBER DISPUTES....32
1. National Director of Cybersecurity....32
2. Cyber Diplomacy Act of 2017 Passed....36
3. Possible Bodies to Mitigate Disputes....37
4. Selecting a Mitigation Body to Handle Dispute Resolution....38

IV. OPTIONS ANALYSIS USING A CYBER SCENARIO....43
A. CRITERIA....44
1. Domestic Legality....44
2. International Legality....44
3. Deterrence....45
B. COURSE OF ACTION A: DISCUSSION....46
C. COURSE OF ACTION B: DISCUSSION....47
D. COURSE OF ACTION C: DISCUSSION....48

V. RECOMMENDATIONS AND CONCLUSION 51
A. RECOMMENDATIONS 51
1. Legislative Branch 52
2. Executive Branch 53
3. NATO 54
4. Private Sector 54
B. AREAS OF FUTURE STUDY 55
C. CONCLUSION 56

LIST OF REFERENCES 57

INITIAL DISTRIBUTION LIST 63

LIST OF FIGURES

Figure 1. Active Cyber Defense Measures.....16

Figure 2. Active Cyber Defense Measures Defined.....17

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Options Analysis 46

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACDC	Active Cyber Defense Certainty (Act)
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDPC	European Committee on Crime Problems
CFAA	Computer Fraud and Abuse Act
CIKR	critical infrastructure and key resources
DNI	director of national intelligence
DoS	Department of State
EC3	European Cybercrime Centre
FBI	Federal Bureau of Investigation
IC	intelligence community
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organization
NPS	Naval Postgraduate School
NSA	National Security Agency

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

News reports about cyber-attacks against corporations are commonplace. A search of Google News on July 31, 2017, for cyber-attacks yielded eight articles from the same day on the first page of the search return. To address this problem, organizations such as George Washington University's Center for Cyber and Homeland Security and the Heritage Foundation have proposed the implementation of active cyber defense measures by the private sector to increase the collective cybersecurity posture of all entities.[1] (For clarity, both the Center for Cyber and Homeland Security and Professor Dorothy Denning from the Naval Postgraduate School have limited the definition of active cyber defense to measures that do not involve hacking a threat actor to recover material by the private sector.)[2] These proposals have brought forth differing opinions on the legality of active cyber defense; however, proponents and opponents of these measures agree that cybersecurity is a national security issue for the nations of the world.

To address the legal objections, Representatives Tom Graves (R-GA) and Kyrsten Sinema (D-AZ) proposed the Active Cyber Defense Certainty (ACDC) Act on October 13, 2017, which creates an affirmative defense for private entities that use active measures external to their networks to determine the location of persistent attacks on their networks and to address the limitations of passive cyber defense measures.[3] This proposed legislation has reshaped the conversation to include the application of deterrence theory in cyberspace across the geopolitical boundaries between nation states, organizations, individuals, and cyber threat actors, yet it does not address the global nature of cyberspace and the ease in which entities can cross geopolitical borders.

---

[1] Dennis C. Blair et al., eds., *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats* (Washington, DC: George Washington University, Center for Cyber and Homeland Security, 2016); and Paul Rosenweig, Steven P. Bucci, and David Inserra, "Next Steps for US Cybersecurity in the Trump Administration: Active Cyber Defense," *Backgrounder*, no. 3188 (May 5, 2017): 11.

[2] Blair et al., *Into the Gray Zone*, 9; and Dorothy E. Denning, "Framework and Principles for Active Cyber Defense" (Monterey, CA: Naval Postgraduate School, December 2013), 3.

[3] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong., 1st sess. (2017), https://www.congress.gov/bill/115th-congress/house-bill/4036.

Representative Edward Royce (R-CA) introduced the Cyber Diplomacy Act of 2017, a law that would create an office within the Department of State to negotiate cyber matters on behalf of the United States abroad and "to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against deception, fraud, and theft."[4] The Cyber Diplomacy Act of 2017 creates a mechanism to address the concerns surrounding the use of active cyber defense measures by American companies in cyberspace. Combining these two pieces of legislation promotes U.S. interests in cyberspace globally while allowing private entities to engage in active cyber defense measures external to their networks with the goal of deterring cyber-attacks; however, it still leaves a gaping hole in U.S. cybersecurity. There is no single entity charged with creating a coherent cybersecurity policy. In fact, numerous executive branch agencies in the intelligence community (IC), law enforcement, the military, and the Department of Homeland Security are charged with various aspects of cybersecurity policy creation and implementation.

The U.S. government, due to the 9/11 Commission's findings, created a director of national intelligence in 2005 to address IC shortfalls in the aggregation of intelligence to prevent terrorist attacks. Likewise, the threat to national security created by the number of diverse and disparate executive branch entities with roles in the creation and implementation of America's cybersecurity policy necessitates the creation of a national director of cybersecurity. This director needs regulatory authority over private-sector critical infrastructure and key resources (CIKR) to ensure that best practices are followed and that the U.S. government issues a standard for the CIKR sectors to follow in cybersecurity matters. Furthermore, the national director of cybersecurity can serve as the coordination point for the private sector's implementation of active cyber defense measures as required by the ACDC Act. Combining the ACDC Act and the Cyber Diplomacy Act of 2017, in conjunction with the creation of an empowered national director of cybersecurity, creates a holistic policy for the United States, but an international body is

[4] Cyber Diplomacy Act of 2017, H.R. 3776, 115th Cong., 1st sess. (2017), https://www.congress.gov/bill/115th-congress/house-bill/3776/text.

still needed to manage and mitigate the disputes that will inevitably arise between nations with the use of active cyber defense measures.

The Council of Europe and the United States recognized a need for an international accord to homogenize global laws on cyber matters in the late 1990s. The resultant 2001 treaty, the Budapest Convention on Cybercrime, states in summary that nations should homogenize their laws in cyberspace to increase cooperation in enforcement matters as criminals can conduct cyber-attacks globally.[5] The North Atlantic Treaty Organization (NATO) created the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, in 2008 "to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation."[6] The CCDCOE played a key role in authoring the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, which outlines the myriad of international laws in cyberspace.[7] Given this expertise, the CCDCOE should use the Budapest Convention on Cybercrime as a framework for disputes arising from the implementation of the ACDC Act. The CCDCOE's 29 centres provide the infrastructure necessary to mitigate disputes in a variety of locales.[8] The United States should petition NATO to change the charter of the CCDCOE, so it can be the international agency to mitigate cyber disputes between nations.

The legislative branch, the executive branch, NATO, and the private sector all have a role to play in the implementation of active cyber defense measures. As there is at least ambiguity surrounding the employment of active cyber defense measures, the U.S. Congress needs to make at least some facets of active cyber defense legal. The executive branch needs to develop a policy surrounding the legalization of active cyber defense. NATO should explore a role in the mitigation of disputes arising between nations from the

---

[5] Convention on Cybercrime, November 23, 2001, E.T.S. 185.

[6] "Home Page," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), accessed May 28, 2018, https://www.ccdcoe.org.

[7] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

[8] CCDCOE, "Home Page."

employment of active cyber defense measures. The private sector needs to develop the implementation techniques.

Cybersecurity experts agree the current state of global cybersecurity needs improvement. Though there is significant disagreement about the employment of active cyber defense measures, this thesis concludes that to raise the collective cybersecurity of all, active cyber defense measures need to be legalized and employed. They will deter cyber threat actors and change their cost–benefit analysis for conducting illicit activities in cyberspace. Creating a national director of cybersecurity to unify and coordinate the cybersecurity policy of the United States will only strengthen the employment of active cyber defense. Likewise, empowering NATO's CCDCOE to mitigate disputes between nations will facilitate information sharing between countries, making it harder for faceless enemies to remain anonymous.

Cybersecurity is a collective issue. It is not limited to the government, nor is it limited to the private sector. Only through the cooperation and mutual support outlined in this thesis can the United States raise the collective security of all. Active cyber defense is a facet of that collaboration. It is naïve for an entity to rely on passive cyber defense measures to protect its crown jewels.[9] The time for collective action is now. The bipartisan legislation legalizing active cyber defense in conjunction with the other measures presented in this thesis is the first step.

[9] *Crown jewels* are the key pieces of data and information a company has that make its business viable. The loss of this information generally means a company no longer exists. Among cybersecurity professionals, it is a common term and concept in describing what information a company must protect so that the proper tools can be put into place. *Misidentification* generally means the company is spending money to protect something that, if lost, is not critical to its business model. For an investment company, this would include both its client account information and trading strategy, which makes it different from other investment companies.

ACKNOWLEDGMENTS

I would like to thank my wife for her forbearance and perseverance as I worked on this master's program through the Naval Postgraduate School's Center for Homeland Defense and Security. In what is already a hectic full-time work schedule, the addition of academe to the mix has caused her to pick up even more responsibilities raising our children and running the household. Without her patience and incredible strength, I would not have been able to complete this program. She is truly the yin to my yang, and I look forward to many more years together.

Likewise, I would like to thank my children for their support through this journey. Their interest in academics inspires me. I pray that they can use my periods of inattentiveness—from being absorbed in the development of this thesis—as motivation toward their own academic endeavors.

I would like to thank my parents for instilling in me the discipline necessary to juggle work, family, and academia. Their own intellectual pursuits provided me a model to follow. Their words of encouragement during times when the task seemed insurmountable were invaluable.

Professor Shannon Brown helped me shape, scope, and craft this study. Without his big-picture guidance, I would still be floundering. I hope our academic journey together has enriched him as much as it has me.

Thank you, Lynda Peters, your guidance in ensuring the completeness of my arguments was worth its weight in gold. Similarly, Professor Lauren Wollman's teaching, mentoring, and incessant nudging during the formulation of the proposal made this thesis possible. To the unsung hero, Greta Marlatt, I could not have finished this thesis without your tutelage on research and proper citations, and your help in weaving them into a coherent narrative. The rest of the staff and faculty at CHDS also deserve special mention. Their classes and mentorship built the tools to complete both the program and the thesis. Thank you. One last member of the CHDS team, Scott Martis, deserves a specific thank

you. He provided the operational and logistical support for the cohort, enabling us to focus on academics. His work enabled us to concentrate entirely on learning.

To the Cohortians of 1703/1704, thank you. I enjoyed getting to know each and every one of you. I loved our spirited debates both inside and outside the classroom. I probably learned as much from each of you as I did from the classroom. I look forward to our continued friendships.

Finally, I would like to thank the Department of Homeland Security, FEMA, and the U.S. Secret Service for the opportunity to pursue this endeavor. DHS and FEMA's funding made it all possible. The U.S. Secret Service allowed me to travel two weeks per quarter for the in-residence portion, often during times of high operational tempo, and I sincerely appreciate it. I hope the agency can take pride in the results.

There is no doubt that I have neglected to mention others—no slight is intended. All should note that the opinions contained within this thesis are mine alone and do not represent the position of the U.S. government. The same applies to any mistakes. Though this thesis has undergone a robust review process, all errors are mine and mine alone.

I. INTRODUCTION

A. PROBLEM STATEMENT

News reports about cyber-attacks against corporations are commonplace. A search of Google News on July 31, 2017, for cyber-attacks yielded eight articles from the same day on the first page of the search return. Newsmax proclaims, "Costly cyber-attacks are having a bigger impact on corporate earnings and are becoming a fact of life for companies."[1] Verizon contends that 1,935 cyber-attacks occurred in 2016.[2] Symantec adds that 1.1 billion identities were exposed as a result of those breaches.[3] Nuix reports that 88 percent of self-identified hackers can breach a network in less than 12 hours.[4] CNBC reports, "In 2016, cybercrime cost the global economy over $450 billion."[5] Additionally, 7.1 billion identities have been exposed over the last eight years as a result of cyber-attacks.[6]

If cyber-attacks against corporations are "a fact of life" and self-identified hackers can penetrate most networks in fewer than 12 hours—resulting in 1,935 breaches with 1.1 billion identities exposed and costing the economy more than $450 billion—the current practices for cybersecurity are inadequate, and a new paradigm for cybersecurity should be sought. Currently, protective measures for cybersecurity are passive. Cybersecurity professionals rely on firewalls, anti-virus software, and other passive measures to protect networks from intrusion by various threat actors. The threat actors—criminals, activists, and spies (nation-states, terrorists, and business competitors)—need only defeat those

---

[1] "Cyber 'Worm' Hurts Corporate Earnings, Sparks $850 Million in Damage," Newsmax, August 2, 2017, http://www.newsmax.com/Finance/StreetTalk/cyber-worm-notpetya-earnings/2017/08/02/id/805374/.

[2] Verizon, *2017 Data Breach Investigations Report*, 10th ed. (New York: Verizon Enterprise Solutions, 2017), 11.

[3] Symantec, *Internet Security Threat Report* (Mountain View, CA: Symantec, 2017), 22:9.

[4] Chris Pogue, *The Black Report*, ed. Josh Mehlman (Herndon, VA: Nuix, 2017), 15.

[5] Luke Graham, "Cybercrime Costs the Global Economy $450 Billion: CEO," CNBC, February 2, 2017, https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

[6] Symantec, *Internet Security Threat Report*, 22:9.

passive measures to penetrate corporate networks.[7] The cybersecurity professional must defeat every attack while the cyber threat actor need only one success to penetrate the network. Further exacerbating the ease with which threat actors gain access to networks, these actors often use insiders' credentials to penetrate networks. Eighty-four percent of hackers use social engineering of some kind to obtain user credentials to penetrate networks.[8] This is an indictment of cybersecurity professionals relying on single-factor authentication—passwords—as opposed to multi-factor authentication—both something the user knows and a physical token the user has in one's possession. Regardless, the number of publicized breaches in a one-year period demonstrates the ease with which cyber threat actors penetrate networks.

With passive cyber defense measures in place, cyber threat actors averaged more than five breaches per day in 2016.[9] To deter cyber-attacks, can other, more active measures be employed by cybersecurity professionals to identify the source of the attack more easily? Representatives Tom Graves (R-GA) and Kyrsten Sinema (D-AZ) proposed the Active Cyber Defense Certainty (ACDC) Act on October 13, 2017, creating a permissive legal framework for affirmative defense for private entities that use active measures external to their networks to determine the location of persistent attacks on their networks, and to address the limitations of passive cyber defense measures.[10] Proponents and opponents of Graves and Sinema's legislative proposal almost immediately began publishing articles, blogs, and podcasts either supporting or excoriating the ACDC Act; however, both sides question whether such an act could be created in a vacuum by one

[7] Verizon, *Data Breach Investigations Report*, 6.

[8] Pogue, *The Black Report*, 15.

[9] Verizon, *Data Breach Investigations Report*, 11. This is figure was derived from the 1,935 attacks in 2016 (1,935 attacks/365 days = 5.3 attacks per day).

[10] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong., 1st sess. (2017), https://www.congress.gov/bill/115th-congress/house-bill/4036.

nation given the ease of transiting geopolitical boundaries in cyberspace because of the myriad of international laws.[11]

Approximately one month earlier, Representative Edward Royce (R-CA) introduced the Cyber Diplomacy Act of 2017, a law that would create an office within the Department of State (DoS) to negotiate cyber matters on behalf of the United States abroad. Its goal is "to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against deception, fraud, and theft."[12] The Cyber Diplomacy Act of 2017 creates a mechanism to address the concerns regarding the global activities of American companies in cyberspace. Combining these two pieces of legislation promotes U.S. global interests in cyberspace while allowing private entities to engage in active cyber defense measures external to their networks with the goal of deterring cyber-attacks.

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* outlines the myriad of international laws in cyberspace. Given the ease with which operations in cyberspace, both nefarious and legitimate, cross geopolitical boundaries, is it plausible for America to pass the ACDC Act, which—if an entity engages in those legally authorized behaviors—may be illegal in another nation without an international accord? Thus far, the literature does not explore this aspect of active cyber defense.

B. RESEARCH QUESTION

Can the United States implement an active cyber defense policy without an international body to mitigate disputes?

C. RESEARCH DESIGN

This thesis is a policy proposal document that explores the possible implementation of active cyber defense measures by private entities as proposed by the pending ACDC

[11] Chris Cook, "Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act," *Just Security* (blog), November 20, 2017, https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act/.

[12] Cyber Diplomacy Act of 2017, H.R. 3776, 115th Cong., 1st sess. (2017), https://www.congress.gov/bill/115th-congress/house-bill/3776/text.

Act. Specifically, it examines whether those measures can be authorized by one nation without an international accord or body to address the inevitable disputes that will arise because cyberspace does not respect geopolitical boundaries. Consequently, an entity could run afoul of the laws of one nation while being entirely within the bounds of the laws of another. This thesis concludes with policy recommendations on the feasibility of implementing both the ACDC Act and the Cyber Diplomacy Act and shaping an international accord or body to mitigate disputes.

The research was limited to the deployment of active cyber defense measures in cyberspace by private entities, whose stated purpose is identifying cyber threat actors that penetrate those networks. Building on this research, the thesis explores a potential framework for addressing active cyber defense in the international arena. It discusses the concept of deterrence theory in cyberspace and its application among nation-state, corporate, individual, and cyber threat actors.

To do so, this study considered alternative courses of action, including the concept of deterrence theory in cyberspace, and the plausibility of private entities implementing active cyber defense measures. This process involved comparing often-contradictory sources of literature and employing options analysis to evaluate the courses of action. The options analysis considered the following three courses of action: the status quo (no passage of the ACDC Act), the passage of the ACDC Act without an international accord or body to discuss cybersecurity matters, or the passage of the ACDC Act with an international accord or body. The criteria were as follows: legality in the United States, international legality, and deterrence theory application in cyberspace.

The thesis presents a policy options matrix measuring each criterion as either "yes" or "no" as described in Paul Pitman's lecture notes on policy options analysis.[13] As active cyber defense measures are possibly illegal, as demonstrated in the literature review, a fictional scenario depicting the use of active cyber defense measures by a private U.S. entity is used to facilitate the options analysis. The scenario portion of the analysis assumes

[13] Paul M. Pitman, "Research Methods, Part II: Policy Options Analysis" (lecture module, Center for Homeland Defense and Security, 2017), https://www.chds.us/coursefiles/NS4081/lectures/methods_policy_options_analysis_v02/methods_policy_options_lec_v02.pdf.

that one nation has authorized active cyber defense measures while others have not and predicts the resulting tensions caused by differing laws. It does not seek to explore the laws of the world regarding cyberspace as other works have done, nor does it seek to recommend which, if any, active cyber defense measures private entities should employ.

Bounded by those guidelines, this thesis makes a series of actionable recommendations, including the identification of any gaps in the ACDC Act as written, on the implementation of an international body or accord to address potential disputes between nations as a result of the employment of active cyber defense measures by private entities. This thesis does not address the international framework of laws as the *Tallinn Manual 2.0* explains the laws of various nations. Likewise, it does not explore the technical employment of active cyber defense measures as seminal works like the Center for Cyber and Homeland Security's *Into the Gray Zone* discuss and define active cyber defense measures.

D. CHAPTER OVERVIEW

To facilitate the analysis, this thesis explores the literature on active cyber defense, examines three different courses of action, and performs an options analysis, which concludes with a series of policy recommendations for the legislative branch, the executive branch, NATO, and the private sector. The literature review in Chapter II defines active cyber defense, reviews the cyber threat landscape, and details the differences between active and passive cyber defense measures. The chapter also delves into cybersecurity expert opinions, explores the legal feasibility of active cyber defense measure employment in the domestic and international legal environments, and considers the passage of the ACDC Act in the United States. It ends with a discussion on the Law of Armed Conflict and deterrence theory as they relate to cyberspace. Chapter III considers the possible courses of action, and Chapter IV evaluates them using the aforementioned options analysis criteria. Chapter V concludes with a series of recommendations for policymakers and the private sector alike.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A review of the literature on active cyber defense yields four broad categories: the cyber threat landscape, the pursuit of active cyber defense measures, U.S. and international laws on cyber defense, and opinions on the legality of active cyber defense measures. In 2017, Representatives Graves and Sinema proposed to legalize active cyber defense measures undertaken by private entities in the United States via the ACDC Act, which has reshaped the conversation to include the application of deterrence theory in cyberspace across geopolitical boundaries between nation-states, organizations, individuals, and cyber threat actors.

The literature review first discusses the debate over the definition of active cyber defense to help the reader appreciate the nuanced or contradictory positions on active cyber defense measures. It continues with a portrayal of the cyber threat landscape from both the news media and cybersecurity companies like Nuix, TrendMicro, Trustwave, Symantec, and Verizon Enterprise Solutions. Each of these entities publishes articles and papers detailing cyber-attacks and outlining the threat actors and their motives. This second category shapes the public discussion around the cyber threat, cyber threat actors, their motives, and the most common types of attacks.

In the third section, public and private consortia examine cyber defense measures, both passive and active, and either call for additional (i.e., more active) cyber defense measures while making policy recommendations or submit that current passive cyber defense measures are adequate to combat the cyber threat actors if implemented correctly and completely. The fourth section details existing and proposed legislation in the United States that codifies permissible actions both internal and external to an entity's network. The proposed ACDC Act applies recommendations, made in works such as *Into the Gray Zone* by the Center for Cyber and Homeland Security, to change the laws of the United States, so private entities may engage in active cyber defense measures outside their networks. The act creates an affirmative defense to the Computer Fraud and Abuse Act (18 U.S.C. § 1030) when those entities attempt to identify "persistent" attackers of their

networks.[14] A different U.S. legislative proposal by Representative Royce seeks to create an office within the Department of State to negotiate cyber matters on behalf of the United States.[15]

The fifth section discusses global legal frameworks and weighs in on whether active cyber defense measures exceed statutory authority internationally or are permissible given current laws and court decisions. This includes organizations like NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and its examination of "154 'black letter' rules governing cyber operations."[16] The final section discusses the relevance of deterrence theory in examining the proposed ACDC Act. Simply put, while some posit mutually assured destruction worked well in the nuclear age but does not translate to the cyber age, others claim that cyber threat actors will limit their cyber-attacks if reasonable certainty of attribution exists.[17]

A. DEFINING ACTIVE CYBER DEFENSE

Proponents and opponents characterize active cyber defense measures differently. Proponents of active cyber defense specifically limit the definition to measures that harm no external networks. Opponents of active cyber defense make the term synonymous with "hacking back." To demonstrate, in the proponent category, both George Washington University's Center for Cyber and Homeland Security and Naval Postgraduate School (NPS) Professor Dorothy Denning limit the definition of active cyber defense to measures that do not involve hacking a threat actor to recover material.[18] Siobhan MacDermott builds

---

[14] Active Cyber Defense Certainty Act.

[15] Cyber Diplomacy Act of 2017.

[16] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), i.

[17] Joshua Tromp, "Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-Attacks," *Small Wars Journal* 12, no. 1 (January 28, 2016), http://smallwarsjournal.com/jrnl/art/law-of-armed-conflict-attribution-and-the-challenges-of-deterring-cyber-attacks; and Jim Chen, "Cyber Deterrence by Engagement and Surprise," *PRISM* 7, no. 2 (December 21, 2017): 101–7.

[18] Dennis C. Blair et al., eds., *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats* (Washington, DC: George Washington University, Center for Cyber and Homeland Security, 2016), 9; and Dorothy E. Denning, "Framework and Principles for Active Cyber Defense" (Monterey, CA: Naval Postgraduate School, December 2013), 3.

on aforementioned definitions and includes all measures just short of preemptive offense.[19] In the opponent category, a news article describes Representatives Graves and Sinema's proposed ACDC Act is entitled "U.S. Congress Mulls First 'Hack Back' Revenge Law. And Yup, You Can Guess What It'll Let People Do."[20] This stark contrast continues throughout the literature.

B. CYBER THREAT LANDSCAPE

News articles keep cyber-attacks in the forefront of the public's mind on a nearly daily basis. An internet news search on a single day in 2017 yielded eight articles. The internet news site Deadline broke the story of HBO's breach in which a hacker stole unpublished videos and scripts and attempted to extort payment from HBO so as not to release them.[21] The *Financial Times* wrote of Merck downwardly modifying its annual performance guidance due to the breach of its networks in June 2017, which temporarily halted production of some products.[22] An article in *The Scotsman* described how businesses fail to take measures to defend networks against cyber-attacks despite their increasing number annually.[23] A similar article on IT Pro Portal describes a study that found small and medium-sized enterprises "are not yet heeding the warnings provided by large attacks on global businesses [despite] more than 875,000 small and medium-sized businesses . . . being hit by at least one cyber-attack . . . in the past twelve months."[24] *The Sun* in London

---

[19] Siobhan MacDermott, *The Folded Paper: Inventing Cyberdiplomacy* (North Charleston, SC: CreateSpace Independent Publishing Platform, 2018), 89.

[20] Iain Thomson, "US Congress Mulls First 'Hack Back' Revenge Law. And Yup, You Can Guess What It'll Let People Do," Register, October 13, 2017, https://www.theregister.co.uk/2017/10/13/us_hack_back_law/.

[21] Denise Petski, "HBO Confirms It Was Hit by Cyber Attack," Deadline, July 31, 2017, http://deadline.com/2017/07/hbo-confirms-cyber-attack-hack-1202139202/?utm_source=dlvr.it&utm_medium=twitter.

[22] Pan Kwan Yuk and Mamta Badkar, "Merck Updates Guidance to Reflect June Cyber Attack," *Financial Times*, July 31, 2017, https://www.ft.com/content/3d7ac341-1742-3329-9a15-2dc269522d10.

[23] Scott Reid, "Hundreds of Thousands of SMEs Hit by Cyber-attacks," *The Scotsman*, July 31, 2017, http://www.scotsman.com/business/companies/tech/hundreds-of-thousands-of-smes-hit-by-cyber-attacks-1-4518376.

[24] Sead Fadilpašić, "Nearly a Million UK SMEs Hit by Cyber-Attacks," IT Pro Portal, July 31, 2017, http://www.itproportal.com/news/almost-a-million-smes-victims-to-cyber-attacks-in-the-last-year/.

summarized five large-scale attacks.[25] *The Christian Science Monitor* published an essay detailing a couple's recovery from a cyber-attack and their regimen of prayer to God, in addition to other cyber hygiene measures, as an additional layer of defense.[26] Dubai Media extolled the virtues of the United Arab Emirates' Computer Emergency Response Team and the "289 cyber-attacks [it prevented] during the first quarter of 2017."[27] RCR Wireless News offered mitigation techniques for network function virtualization and software-defined networking vulnerabilities.[28]

Beyond these news stories, which help form public sentiment and opinion by reporting the scope of the cyber threat issue, several companies publish (at least) annual reports that discuss the cyber threat entities facing all critical infrastructure and key resource (CIKR) sectors.[29] Chief Information Security Officer Chris Pogue of Nuix, a global cybersecurity firm, has authored a report on hackers and their methodologies to help organizations understand the psychology of the cyber threat actors behind cyber-attacks.[30] TrendMicro publishes research papers on a variety of vulnerabilities to the cyber infrastructure and the mitigation techniques that cyber defenders should employ to successfully defend against specific threats. One such report discusses "sinkholing," which

---

[25] Dan Elsom, "Five of the Worst Cases of Cybercrime the World Has Ever Seen – from Stealing Data from One Billion Yahoo Users to Crippling the NHS," *The Sun* (London), July 31, 2017, https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/.

[26] Kevin Graunke, "Shielded from Cyberattacks," *Christian Science Monitor*, July 31, 2017, https://www.csmonitor.com/Commentary/A-Christian-Science-Perspective/2017/0731/Shielded-from-cyberattacks.

[27] "Telecommunications Regulatory Authority Prevents 289 Cyber-Attacks in Q1 2017," Dubai Media, July 31, 2017, http://www.emirates247.com/news/emirates/telecommunications-regulatory-authority-prevents-289-cyber-attacks-in-q1-2017-2017-07-31-1.656939.

[28] Nathan Cranford, "How to Protect NFV and SDN from Cyber Attacks," RCR Wireless News, July 31, 2017, http://www.rcrwireless.com/20170731/nfv/how-to-protect-nfv-and-sdn-from-cyber-attacks-tag27-tag99.

[29] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: DHS, 2013), 9. The U.S. government defines the CIKR sectors.

[30] Pogue, *The Black Report*.

redirects malicious internet traffic to an internet address that hosts no content.[31] Another report outlines 11 different attacks between May 2016 and August 2017. That report details instances of attackers using misconfigurations in security settings to penetrate systems, causing disruption and harm to the intelligent transportation system and the mitigation techniques its operators should employ.[32] Trustwave's 2017 annual security report details cyber-attacks of the previous year, arguing that cyber-security professionals need to shift from passive measures to active ones.[33] Symantec's 2017 *Internet Security Threat Report* outlines the 2016 attack vectors and threat actors—including espionage, email attacks, and the underground economy enabled by cybercrime—and offers recommendations for mitigating the cyber threat. Symantec's report briefly discusses new attack vectors the internet of things introduces to the cyber realm.[34] Verizon's 2017 *Data Breach Investigations Report* details the threat to each of the CIKR sectors, the attack vectors that threat actors pursue, and mitigation techniques that entities need to employ to combat those cyber threats.[35] Each of the aforementioned documents by cybersecurity companies helps shape the public understanding of various cyber threat actors, the methods they use, and the CIKR sector or sectors they will most likely attack.

A description of the threat is not limited to news articles and publications by cybersecurity firms. Cybersecurity author Roger Grimes has written eight books about his experiences as a penetration tester by describing methods he and cyber threat actors employ to penetrate networks. Grimes recommends mitigation techniques for cybersecurity

---

[31] David Sancho and Ranier Link, "Sinkholing Botnets" (technical paper, TrendMicro, 2011); and Margaret Rouse and Matthew Haughn, "What Is Botnet Sinkhole?" Tech Target, June 2014, http://whatis.techtarget.com/definition/botnet-sinkhole.

[32] Numaan Huq, Rainer Vosseler, and Morton Swimmer, "Cyberattacks against Intelligent Transportation Systems: Assessing Future Threats to ITS" (research paper, TrendMicro, 2017), 4. Many global locales are implementing aspects of ITS to improve traffic flow and the efficiency of public transportation (e.g., by adjusting schedules to accommodate usage) and to decrease the response time of emergency vehicles to calls for service. Disruptions to these networks may cause gridlock. Even worse, they may lead to false calls for emergency response. Securing these networks as they continue to come online is a public safety concern.

[33] Trustwave, *2017 Trustwave Global Security Report* (Chicago: Trustwave Holdings, 2017), 1.

[34] Symantec, *Internet Security Threat Report*, 22:64.

[35] Verizon, *Data Breach Investigations Report*.

professionals in his work.[36] Other works describe the cybersecurity threat, as exemplified by M. Mitchell Waldrop's article in *Nature* that suggests individuals and organizations need to understand the psychology of cyber threat actors to better defend against them.[37] These and other similar works focus public conversation on the ease with which cyber threat actors attack entities, public and private alike, which calls for more—or different—cybersecurity measures.

C. ACTIVE AND PASSIVE CYBER DEFENSE MEASURES

The aforementioned documents detail the undeniable fact that there is a multitude of cyber threats across all CIKR sectors. These documents also offer a glimpse into the havoc cyber-attacks cause in CIKR sectors as well as possible mitigation techniques. The next set of documents presents research into passive and active cyber defense measures and offers recommendations for policymakers. A healthy debate among cybersecurity professionals regarding various recommendations permeates the worldwide discussion. The recommendations are either to permit more active measures by private entities or to restrict their usage to government entities and limit private entities to passive cyber defense measures. Proponents of allowing private entities to engage in active cyber defense measures in the United States often cite a 2006 Government Accountability Office report that states "about 85 percent of the nation's critical infrastructure is owned by the private sector."[38] Those citing this statistic often use it to demonstrate the decentralized nature of CIKR sector and argue that control of implemented cybersecurity measures is beyond the U.S. government.

Published in 2011, an NPS thesis by Tiong Pern Wong was one of the first scholarly works to address active cyber defense measures. Wong's seminal work limits the proposed

---

[36] Roger A. Grimes, *Hacking the Hacker: Learn from the Experts Who Take Down Hackers* (Indianapolis: Wiley, 2017).

[37] M. Mitchell Waldrop, "How to Hack the Hackers: The Human Side of Cybercrime," *Nature* 533, no. 7602 (May 12, 2016): 164, https://doi.org/10.1038/533164a.

[38] Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors Characteristics* (Washington, DC: GAO, October 2006), 2.

implementation of active cyber defense measures to nation-states.[39] In doing so, Wong avoids considering the legal implications of private entities engaging in active cyber defense measures.

Dorothy Denning's 2013 work expands on Wong's limited framework for nation-states to engage in active cyber defense measures. Denning offers a framework for public and private entities alike to engage in active cyber defense based on the military construct of missile defense. This is one of the first works calling for private entities to engage in active cyber defense. To frame the discussion, she proposes four characteristics to consider prior to engaging in active cyber defense activities: "scope of effects, degree of cooperation, type of effects, and degree of automation."[40] To illustrate these principles, Denning explores different air defense shields, including the Patriot Missile System and Israel's Iron Dome, as well as the Coreflood botnet takedown.[41] Clearly, missile defense is rooted in the construct of deterrence. The capability of intercepting missiles limits the effectiveness of launching them. More devastating still is the ability to accurately identify the launch point of missiles and immediately deploy a counter-attack. Such an ability deters individuals from locating themselves at the launch site. Similarly, in cyberspace, certain attribution of an attack limits an individual's willingness to engage by changing the value proposition. The increased likelihood of identification deters nefarious behavior in cyberspace. Deterrence theory is discussed more fully toward the end of the literature review.

In 2015, Michael Amao expanded on Denning's work with his thesis for Utica College. Amao proposes that active cyber defense measures have the potential to mitigate cybercriminal activity.[42] Without explicitly exploring the concept of deterrence theory in cyberspace, Amao's thesis posits that active cyber defense measures can blunt

---

[39] Tiong Pern Wong, "Active Cyber Defense: Enhancing National Cyber Defense" (master's thesis, Naval Postgraduate School, 2011), 41.

[40] Denning, "Framework and Principles for Active Cyber Defense," 3.

[41] Denning.

[42] Michael Amao, "Active Cyber Defense to Fight Cybercrime" (master's thesis, Utica College, 2015), 45.

cybercriminal activity because previously anonymous activity may become attributable. This shift in technology explores one of the potential benefits of allowing private entities to engage in active cyber defense to reduce cybercriminal activity.

In 2016, George Washington University's Center for Cyber and Homeland Security gathered a large group of professionals, academics, and cyber experts to discuss active cyber defense measures, the legality thereof, and which (if any) measures should be included in an active cyber defense framework. Former Secretary of Homeland Security Michael Chertoff partnered with Former Director of National Intelligence Admiral Dennis Blair to lead this effort. It resulted in the publication of a report that examines internal and external measures private entities could undertake and offers a series of recommendations to the executive branch, the legislative branch, and the private sector to create more robust defense mechanisms to deter cyber threat actors.[43] Some of the key recommendations are as follows:

- The President should direct executive branch agencies to research active cyber defense measures, issue guidance for their deployment under current laws, and negotiate with foreign entities to develop standards and procedures for the employment of active cyber defense measures.

- The legislative branch should update the CFAA to ensure the legality of active cyber defense measures.

- The private sector should develop best practices and policies for the employment of active cyber defense measures.[44]

Rodrigo Nieto-Gómez disagrees with these recommendations, positing that the government engages in fear-mongering when it comes to the cyber threat as it screams for

[43] Blair et al., *Into the Gray Zone*.

[44] Blair et al., 31–33.

more security and criminalization of behavior.[45] Many of Nieto-Gómez's examples describe the criminalization of intellectual-property fraud; however, this narrow focus does not address the legitimate concern of cyber threat actors either penetrating critical infrastructure for nefarious reasons or stealing data. Essentially, he says hacking is behavior consistent with the American entrepreneurial spirit; instead of criminalizing it, he suggests the government should reward and incentivize the behavior for improvements in critical infrastructure protection.[46] Most private entities engage in the sort of "bug bounty" program proposed by Nieto-Gómez. Grimes outlines one such program from Microsoft.[47]

From an international perspective, the Center for Security Studies offers recommendations to employ active cyber defense measures to bring a "holistic approach to cyber defense and cybersecurity policy."[48] The Center for Security Studies also directly contradicts Nieto-Gomez's proposition that the government engages in fear-mongering related to attacks against the CIKR sector. Writing for the center, Robert Dewar details several attacks against the CIKR sector and the impact those attacks have had on the populace.[49]

This thesis does not explore the different technologies across the gamut of active cyber defense. Rather, it focuses on the possible implementation of active cyber defense measures in a global setting. The following two figures from Blair et al. summarize the topic well. Figure 1 depicts the spectrum from passive cyber defense measures to increasingly active measures, sorted by risk.

---

[45] Rodrigo Nieto-Gómez, "Cyber-Geopolitics: Geopolitical Rivalries behind the Cyber-Threat Narratives in the United States," *Medium* (blog), August 20, 2014, https://medium.com/homeland-security/cyber-geopolitics-a45fc698a3a1. This blog post was originally published as follows: Rodrigo Nieto Gómez, "Cybergéopolitique: De l'utilité Des Cybermenaces," *Journal Hérodote*, no. 1 (2014): 98–122.

[46] Nieto-Gómez.

[47] Grimes, *Hacking the Hacker*, 268.

[48] Robert S. Dewar, *CSS Cyber Defence Trend Analysis 1: Active Cyber Defense* (Zurich: Center for Security Studies, 2017), 16.

[49] Dewar, 4–22.

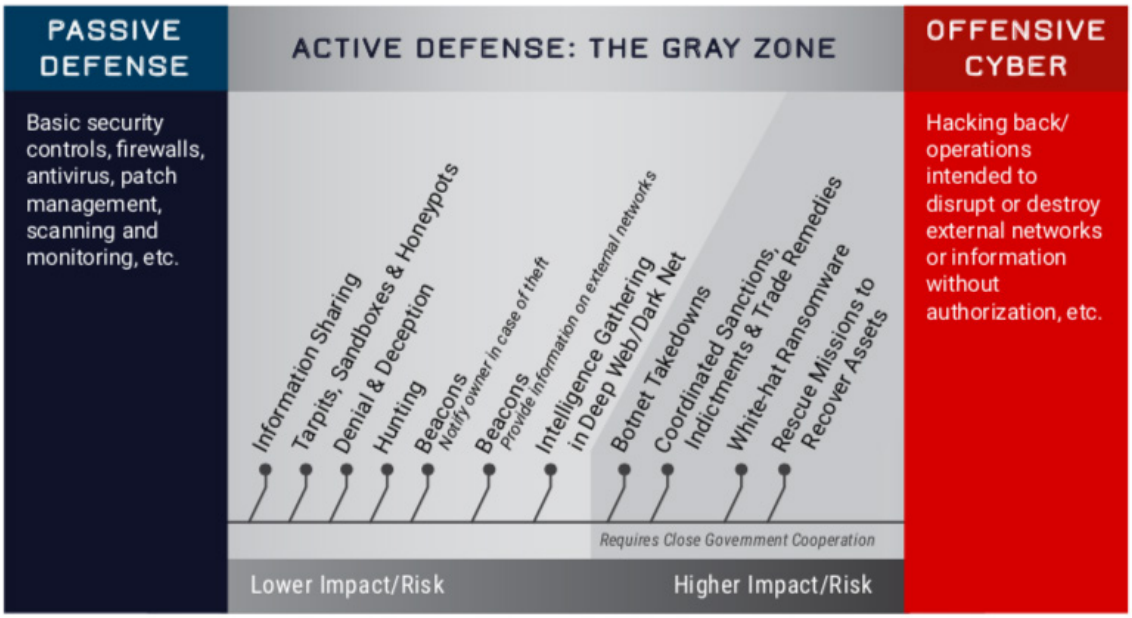

Figure 1. Active Cyber Defense Measures[50]

Figure 1 depicts the range of active cyber defense measures in order of increasing risk, while Figure 2 provides a short definition of each measure, again sorted by increasing risk. This study does not delve into the different measures included in either figure but merely uses them to demonstrate some of the different measures included in active cyber defense.

[50] Source: Blair et al., *Into the Gray Zone*, 26.

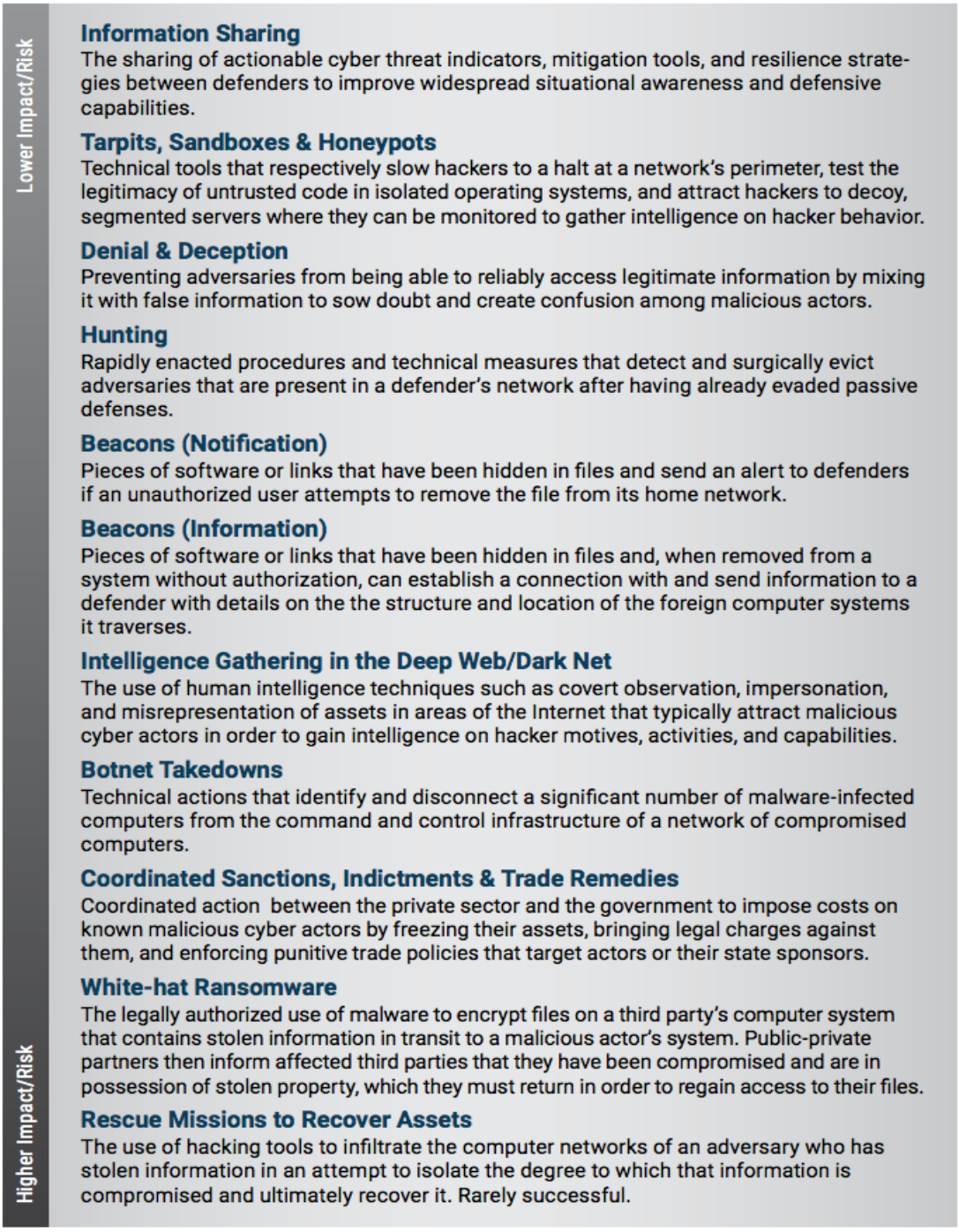

Figure 2. Active Cyber Defense Measures Defined[51]

[51] Source: Blair et al., 27.

D. EXISTING AND PROPOSED LEGISLATION

Shortly before President Trump was inaugurated, the Heritage Foundation published a policy recommendation for the new administration to allow private-sector employment of active cyber defense measures because "the failure of the government to provide adequate protection has led many cybersecurity analysts, scholars, and policymakers to suggest that there is a need for private-sector self-help."[52] The policy recommendations follow from work begun by George Washington University's Center for Cyber and Homeland Security.[53] These calls for action prompted Representatives Graves and Sinema's legislative activity. Prior to discussing their proposed legislation, a background of the legal discussion around the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is in order.

Individuals and entities within the United States are bound by the CFAA, which makes it illegal to improperly access computers and computer systems.[54] Several U.S. appellate court decisions provide additional guidance. One of the first cases involved Robert Tappan Morris, who wrote and released a computer worm that infected thousands of computers. He had released the worm on the internet for the express purpose of showing the security flaws of a commonly used protocol that computers used to communicate. The computer worm self-replicated as it moved across different networks on the internet.[55] Cultural lore credits Morris with crashing the internet. The Second Circuit ruled that Morris exceeded his level of authorized access on the infected computer systems when he released the self-propagating worm because he did not have permission to modify the systems and, therefore, was guilty of violating the CFAA.[56]

In a more recent case, Andrew Joseph Workman appealed his conviction related to the distribution and possession of child pornography because he said the U.S. government

---

[52] Paul Rosenweig, Steven P. Bucci, and David Inserra, "Next Steps for US Cybersecurity in the Trump Administration: Active Cyber Defense," *Backgrounder*, no. 3188 (May 5, 2017), 1.

[53] Blair et al., *Into the Gray Zone*.

[54] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1984).

[55] *United States v. Robert Tappan Morris*, 928 F.2d 504, 505–506 (2nd Cir. 1991).

[56] *Morris*, 928 F.2d at 505.

exceeded its level of authorized access during the execution of a lawful search warrant when it installed beaconing technology on the pornographic images of children. The beaconing technology notified the U.S. government of the locations of computers that housed the images after they left the government-controlled server. The 10th Circuit Court of Appeals, affirming the conviction, ruled that due to the good faith doctrine, the U.S. government has authority pursuant to a search warrant to install beaconing technology regardless of the validity of the search warrant.[57] The Department of Justice's Computer Crimes and Intellectual Property Section publishes guidance for the U.S. attorney based on statutes and court decisions to assist with prosecuting violations and suspected violations of the CFAA.[58]

Representatives Graves and Sinema proposed a modification to the CFAA that permits private entities to use beaconing (or phone-home) technology in cooperation with law enforcement—specifically the Federal Bureau of Investigation (FBI)—as part of the ACDC Act. The proposal is as follows: For those concerned with entities falsely accusing another of penetrating their networks, the ACDC Act creates liability for the private entity that falsely attributes data loss in a report to law enforcement; law enforcement must provide an annual report to Congress on entities using beaconing technology; and the modification to the CFAA has a two-year sunset clause.[59] This legislative proposal sparked intense debate. Stanford legal scholar Kristen Eichensehr opposes the proposed legislation and raises concerns about the possible international ramifications: "The FBI's participation in the review process may trigger the U.S. government's international legal responsibility for private actors."[60] Legal scholars Bobby Chesney and Herb Lin support the proposed legislation; however, both raise concerns over the limiting factor of cooperation with the

[57] *United States v. Andrew Joseph Workman*, 863 F.3d 1313, 1317–1318 (10th Cir. 2017).

[58] Department of Justice, *Computer Crimes and Intellectual Property Section: Prosecuting Computer Crimes* (Washington, DC: Office of Legal Education, 2015).

[59] Active Cyber Defense Certainty Act.

[60] Kristin E. Eichensehr, "Would the United States Be Responsible for Private Hacking?," *Just Security* (blog), October 17, 2017, https://www.justsecurity.org/46013/united-states-responsible-private-hacking/.

FBI.[61] Additionally, both question whether some of the undefined terms in the proposed legislation, e.g., "persistent attacker," and the nebulousness surrounding them may adversely limit the implementation of the act.[62]

To address the concerns raised by Eichensehr and others regarding international ramifications, a piece of legislation proposed independently of the ACDC Act by Representative Royce—the Cyber Diplomacy Act of 2017—creates the Cyber Issues Office within DoS to create consensus on actions within the international arena.[63] This act creates a U.S. government body with the authority to work with other nations to address the actions of U.S. private entities exercising their authority under the ACDC Act to identify cyber threat actors who penetrate their networks. Combining the two acts blunts the aforementioned concerns regarding unilateral actions undertaken by U.S. private entities in the international arena in cyberspace, which often ignores geopolitical boundaries.

Because the internet does not recognize geopolitical boundaries, individuals and entities routinely circumvent the globe in their interactions with others. Therefore, the *Tallinn Manual 2.0* is an invaluable document for an entity engaged internationally in any form of cyber activity. It describes 154 laws from around the globe.[64]

E. LEGAL ANALYSIS

Three facets of the legal discussion on active cyber defense appear in the literature. The first centers on the legality of employing active cyber defense measures in the United States using the CFAA and case law as the basis for discussion. The second centers on how other nations' laws view active cyber defense measures. The third, included within the

---

[61] Robert Chesney, "Legislative Hackback: Notes on the Active Cyber Defense Certainty Act Discussion Draft," *Lawfare* (blog), March 7, 2017, https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft; and Herb Lin, "More on the Active Defense Certainty Act," *Lawfare* (blog), March 24, 2017, https://www.lawfareblog.com/more-active-defense-certainty-act.

[62] Chesney, "Legislative Hackback"; and Lin, "More on the Active Defense Certainty Act."

[63] Cyber Diplomacy Act of 2017.

[64] Schmitt, *Tallinn Manual 2.0*, i.

international analysis but substantial enough to receive its own section, is the Law of Armed Conflict (LOAC).

1. Domestic Legal Analysis

Under the CFAA as currently written—but without considering passage of the ACDC Act in its current or proposed form—University of Southern California Law Professor Orin Kerr argues active cyber defense measures are illegal because the basis for interpretation of the CFAA centers on the level of authorized access. As defined by *U.S. v. Morris*, the owner or operator of a network authorizes every user's access level on the network. Kerr's position is that active cyber defense measures exceed the level of authorized access on external networks and are, thus, illegal.[65] Josh Goldfoot and Aditya Bamzai take a similar position.[66]

Shane McGee, Randy Sabett, and Anand Shah disagree with Kerr's interpretation of case law. They claim that an entity's active cyber defense measures to defend its networks and/or identify the perpetrators of an attack are legal under both U.S. and international self-defense law and common law.[67] They offer a caveat: using active cyber defense measures is illegal if they are employed against a misattributed entity.[68] Finally, they posit that a private entity cannot use active cyber defense measures against nation-states because doing so may violate the Neutrality Act.[69]

On a blog for the law firm Steptoe & Johnson, Eugene Volokh adds to the argument regarding self-defense. He explains self-defense does not need to be explicitly authorized for it to be legal under U.S. and international law. On the same blog, former National Security Agency (NSA) general counsel Stewart Baker proposes licensing private entities

---

[65] Orin Kerr, "Norms of Computer Trespass," *Columbia Law Review* 116 (May 1, 2016): 1143.

[66] Josh Goldfoot and Aditya Bamzai, "A Trespass Framework for the Crime of Hacking," *George Washington Law Review* 84, no. 6 (December 2016): 1499.

[67] Shane McGee, Randy V. Sabett, and Anand Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Journal of Business & Technology Law* 8, no. 1 (2013): 13–20.

[68] McGee, Sabett, and Shah, 37.

[69] McGee, Sabett, and Shah, 44.

to perform active cyber defense measures to ensure that only trained professionals engage in the identification of cyber threat actors who penetrate networks and to promote accountability in those using the tools.[70]

Siobhan MacDermott's 2018 book greatly expands Volokh's concept of self-defense and argues all Americans have authority under the Second Amendment to the U.S. Constitution to form a cyber-militia. MacDermott implores individuals to exercise those rights to increase the collective defense of the nation.[71] This cyber-militia construct as authorization for private individuals and entities to employ active cyber defense measures is similar to the argument made that active cyber defense measures are authorized by the "castle doctrine."[72]

Raymond Collin's master's thesis from Utica College echoes the objections raised by Kerr and others regarding the legality of such measures and posits that the law should change to allow private entities to use them. Collins adds that fully developing a capability to conduct active cyber defense measures will also require a corporate cultural shift and an investment in infrastructure.[73] Jautau White's 2017 dissertation asserts 85 percent of cybersecurity professionals will employ active cyber defense measures if they are feasible and legal. Thus, the shift in corporate culture may have already occurred.[74]

Clearly, no consensus exists on the legality of private entities employing active cyber defense measures under the CFAA as currently written. This debate becomes moot if the U.S. Congress passes the ACDC Act. The next section explores the international framework for cybersecurity laws and the discussion surrounding the use of active cyber defense measures.

---

[70] Steptoe & Johnson, "The Hackback Debate," *Steptoe Cyberblog*, November 2, 2012, http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

[71] MacDermott, *The Folded Paper*, 116.

[72] McGee, Sabett, and Shah, "Adequate Attribution," 15.

[73] Raymond Martin Luther Collins, "Proactive Cybersecurity through Active Cyber Defense" (master's thesis, Utica College, 2017), 29.

[74] Jautau Kelton White, "Impact of Protection Motivation Theory and General Deterrence Theory on the Behavioral Intention to Implement and Misuse Active Cyber Defense" (PhD diss., Capella University, 2017), 83.

2. International Legal Analysis

The debate over the international legality of active cyber defense measures is as varied as the domestic debate. To understand the common framework for the debate, the Council of Europe and the United States recognized a need for an international accord to homogenize global laws on cyber matters in the late 1990s. The resultant 2001 treaty, the Budapest Convention on Cybercrime, states in summary that nations should formulate their laws governing cyberspace along the following guidelines:

- Every network has a base level of authorized access. Entities that exceed that level of authorized access violate the law.
- Preventing access to or damaging data and/or computer networks is counterproductive to the free sharing of information and should be punished appropriately.
- Although digital devices allow the ubiquitous copying of intellectual property, they do not obliterate intellectual property protections. Nations should ensure entities respect intellectual property rights.
- Illicit images of children are inherently wrong. Nations should prosecute entities that publish and distribute such images.
- Parties that subscribe to the treaty shall cooperate with other nations to enforce these principles and share information pursuant to the appropriate legal measure to allow the extradition and prosecution of perpetrators of acts contrary to those provisions.
- Criminal liability does not attach to measures used for the protection of computers and computer networks.

- The European Committee on Crime Problems (CDPC) shall settle disputes between signatories.[75]

The effectiveness of the Budapest Convention on Cybercrime is hotly debated. Seger praises the common standards created because they form a common framework for nations to create and enforce cybersecurity laws.[76] Owens, Dam, and Lin argue the international agreement "increase[s] the effectiveness of [international] criminal laws in dealing with cyberattacks."[77] Goldsmith laments its effectiveness because only 67 nations have signed it, and he details the weak enforcement mechanism of the CDPC.[78] Lindsay builds on Goldsmith's view, adding that almost all countries agree cybersecurity is a global problem; however, the Budapest Convention on Cybercrime's nebulous definitions, poor enforcement, and voluntary compliance measures make it ineffective.[79] Lindsay adds that major global cyber players, such as China, are not signatories.[80] MacDermott adds to Lindsay's and Goldsmith's comments that nations should not expect others to comply with "unenforceable global conventions" and that NATO should become involved in creating meaningful global cyber defense mechanisms.[81] Borghard and Lonergan concur with this assessment—that global agreements are ineffective in the cyber realm whereas they did prove effective in the conventional and nuclear weapons era.[82] The difference lies in the

---

[75] Convention on Cybercrime, November 23, 2001, E.T.S. 185.

[76] Alexander Seger, "The Budapest Convention on Cybercrime: A Framework for Capacity Building," *Global Cyber Expertise Magazine*, vol. 2, November 2016, 40.

[77] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 34.

[78] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View," in *Future Challenges in National Security and Law*, ed. Peter Berkowitz (Palo Alto, CA: Hoover Institution Task Force on National Security and Law, Stanford University, February 2011), 2.

[79] Jon. R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (Winter 2014): 42, https://doi.org/10.1162/ISEC_a_00189.

[80] Lindsay, 41.

[81] MacDermott, *The Folded Paper*, 89–94.

[82] Erica D. Borghard and Shawn W. Lonergan, "Why Are There No Cyber Arms Control Agreements?," Defense One, January 18, 2018, http://www.defenseone.com/ideas/2018/01/why-are-there-no-cyber-arms-control-agreements/145289/.

nature of cyberspace vis-à-vis the physical nature of conventional weapons. There are limited places to hide conventional weapons and munitions. Conversely, because weaponized software can be hidden virtually anywhere, adversaries must have complete access to a nation's networks to verify compliance with agreements, thus preventing a nation from having secrets whatsoever.[83]

Regardless of the debate, the Budapest Convention on Cybercrime creates a common framework for the international discussion of cyberlaws. Augmented with the CCDCOE's *Tallinn Manual 2.0*, international laws generally follow the concept of exceeding levels of authorized access; however, the Budapest Convention on Cybercrime allows activities to defend networks, which give credence to the idea that at least in some circumstances, active cyber defense measures are allowable.

3. Law of Armed Conflict

LOAC is the internationally recognized framework for nations to conduct wars. It protects combatants and non-combatants alike.[84] It further defines regular and irregular troops and outlines the protections (or lack thereof) for interactions between the different elements found on the battlefield.[85] William Taft argues in the *Yale Law Review* that terrorists engaged in nefarious activities lack protections provided to regular soldiers. [86] Similarly, this thesis posits those engaged in activity that violates conventions, such as the international treaty, the Budapest Convention on Cybercrime, also lack some of the protections provided under LOAC as they do not meet the definition of regular troops.

Owens, Dam, and Lin propose that active cyber defense measures are permitted under LOAC because it is a self-defense activity, which is explicitly permitted.[87] Building on this theme, the cyber threat actors who engage in cyber-attacks commit actions

---

[83] Borghard and Lonergan.

[84] William H. Taft IV, "The Law of Armed Conflict after 9/11: Some Salient Features," *Yale Journal of International Law* 28, no. 2 (2003): 319.

[85] Taft, 319.

[86] Taft, 320–21.

[87] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 244.

previously limited to nation-states because of the ease by which lesser entities can develop weapons, which when compared to conventional arms, are capable of delivering tremendous devastation to both governmental and non-governmental organizations. As such, a combination of both LOAC and the criminal statutes apply.[88] Owens, Dam, and Lin call for explicit authorization to use active cyber defense measures through a modification to the CFAA, which the proposed ACDC Act provides.[89]

Tromp's views of LOAC strongly differ from those of Owens, Dam, and Lin. Tromp argues the same low barriers to entry, which they view as authorizing activities, prohibit action.[90] Tromp maintains that active cyber defense measures violate the theory of neutrality because attacks and attributional actions routed through innocent parties or neutral bystanders violate the sovereignty of those trespassed. Therefore, any counter-actions, which Owens, Dam, and Lin argue are authorized, are violations of LOAC.[91] From Tromp's perspective, the proposed ACDC Act is not feasible.

As Owens, Dam, and Lin demonstrate, both LOAC and national cybersecurity laws apply to matters in cyberspace. Cyber threat actors, given their tactics and lack of identifiable markings, may meet the definition of terrorists as Taft discusses regarding the war on terror.[92] As Taft astutely recognizes, this does not mean these actors have no protections under LOAC, but it does mean they can be treated differently. Nonetheless, legislation like the ACDC Act and the Cyber Diplomacy Act of 2017 can help sort through the ambiguity of the current legal framework and settle the debate.

F. DETERRENCE THEORY

Just as scholars disagree on the legality of active cyber defense measures employed under the current legal framework, they also disagree on the concept of deterrence in

---

[88] Owens, Dam, and Lin, 22.

[89] Owens, Dam, and Lin, 72.

[90] Tromp, "Law of Armed Conflict."

[91] Tromp.

[92] Taft, "The Law of Armed Conflict after 9/11," 323.

cyberspace. Joshua Tromp argues deterrence does not apply to cyberspace because the barriers to entry are virtually non-existent—in contrast to an entity attempting to develop a chemical or nuclear weapon for which the barriers are numerous. Consequently, almost anyone can attempt to compromise a network.[93] Tromp adds that because attribution is extremely difficult in cyberspace given the ease with which traffic can be routed through different networks, no deterrence can exist.[94] Tromp concludes that nearly every active cyber defense measure violates the theory of proportionality in law, which states the punishment should fit the crime.[95]

Jim Chen disagrees with Tromp's assessment of deterrence in cyberspace. Chen argues that because active cyber defense measures can help attribute not only the source of the cyber-attack but also the specific perpetrator of the attack in a timely manner, a tremendous deterrence exists. Chen demonstrates his theory with the example of an entity causing a sound to play on a cyber threat actor's computer as part of an active cyber defense response and the unnerving effect it would have on the perpetrator.[96] Josh Higgins counters Tromp's argument on deterrence, stating the employment of active cyber defense increases the attribution of attacks in a "more effective and timely manner," thus deterring cyber threat actors.[97]

Mariarosaria Taddeo echoes the same concerns as Tromp. Her concern centers primarily around the limited barriers to entry and success in the cyber weapons realm that if countered by a more powerful force engaged in active cyber defense, would pose a serious threat of escalation.[98] Similar to Tromp, she maintains that the difficulties associated with attribution limit the deterrent effect of active cyber defense and that the

---

[93] Tromp, "Law of Armed Conflict."

[94] Tromp.

[95] Tromp.

[96] Chen, "Cyber Deterrence by Engagement and Surprise," 105.

[97] Joshua Higgins, "Industry: New House Bill Lays Groundwork for Policy Dialogue on Active Cyber Defense," *Inside Cybersecurity*, March 7, 2017, http://libproxy.nps.edu/login?url=https://search.proquest.com/docview/187507644 5?accountid=12702.

[98] Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace," *Philosophy & Technology* 31, no. 3 (September 2018): 339, https://doi.org/10.1007/s13347-017-0290-2.

relative difficulty of demonstrating capabilities in cyberspace—holding a military parade in the conventional sense—limits the effectiveness of deterrence.[99] Taddeo's analysis falls short in acknowledging how active cyber defense measures will help increase attribution, as Chen articulates.

Richard Andres believes the United States generally self-deters from retaliating against cyber-attacks due to a lack of political will in the nation.[100] He uses the examples of the public's inability to grasp the loss and the difficulty in attribution as reasons.[101] As other scholars have demonstrated about improvements in technology, the ability of cyber defenders to attribute cyber-attacks to threat actors will continue to improve, which lessens Andres' concern. Furthermore, Herath and Rao discuss that the will to enforce rules or laws has a tremendous deterrent effect on poor behavior in cyberspace.[102]

Hoffman and Levite discuss how most governments treat their responsibility for security of the private sector differently in cyberspace than in the physical realm, which has encouraged the behavior of cyber threat actors.[103] Thus, if governments allow private entities to engage in active cyber defense, the cumulative effect is deterrence of poor behavior because it will reduce the benefits derived by the cyber threat actors because they are unsure of the attributional capabilities of cybersecurity professionals.[104] Hoffman and Levite call for governments worldwide to allow private entities to engage in active cyber defense, which will result in increased security for everyone.[105]

Although almost everyone agrees the world has an increasing cyber threat problem and that more needs to be done to combat the issue, the method to solve the problem brings

---

[99] Taddeo, 342.

[100] Richard Andres, "Cyber Gray Space Deterrence," *PRISM* 7, no. 2 (December 21, 2017): 92.

[101] Andres, 97.

[102] Tejaswini Herath and H. Raghav Rao, "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* 18, no. 2 (2009): 112, https://doi.org/10.1057/ejis.2009.6.

[103] Wyatt Hoffman and Ariel E. Levite, *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* (Washington, DC: Carnegie Endowment for International Peace, 2017), 3.

[104] Hoffman and Levite, 18.

[105] Hoffman and Levite, 41.

widely varying techniques to the forefront. Some suggest current passive cybersecurity techniques need to be employed more effectively by shoring up basic cyber hygiene processes. Others propose that current passive cybersecurity techniques are inadequate, and laws need to change to allow the employment of active cyber defense measures by private entities. Representatives Graves and Sinema's proposed ACDC Act has brought to light an entirely new discussion on whether deterrence is even possible in cyberspace. Deterrence theory in cyberspace differs from deterrence theory in the nuclear age, wherein mutually assured destruction ensured nations did not employ their nuclear arsenals against one another. As several scholars have indicated, the barriers to entry into the cyber realm are almost non-existent, which changes the players and the dynamic in which they interact. To argue there can be no deterrence in cyberspace discounts how the smallest of actions impact behavior, as Herath and Rao as well as Chen detail in their respective works.

G. CONCLUSION

In reviewing the literature, all parties agree cybersecurity is a national security issue for America and the world. Cyber incidents increase year after year as demonstrated in the publications of cybersecurity firms. The proposed techniques to address the issue vary from the better implementation of passive cyber defense measures to calls for more active measures. Legal scholars argue over the legality of active measures domestically and internationally as well as the efficacy of the measures and their ability to deter cyber threat actors. Representatives Graves and Sinema proposed legislation to create a positive defense through the employment of active cyber defense measures under the CFAA, which reframes the discussion. Coupling the ACDC Act with Representative Royce's Cyber Diplomacy Act of 2017 may reduce many of the objections. The remainder of this thesis explores different courses of action for the implementation of active cyber defense measures to increase the common defense.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COURSES OF ACTION

As discussed in Chapter I, this thesis uses three distinct courses of action to facilitate the analysis. In the first course of action, the thesis assumes the laws of both America and the world exist as currently written. In the second course of action, it assumes the U.S. passes the ACDC Act; however, the state of affairs in the rest of the world remains unchanged. In the third course of action, it assumes the U.S. passes the ACDC Act and the Cyber Diplomacy Act of 2017. It further assumes that an international, multilateral organization emerges to become the cyber dispute mitigation entity.

A. COURSE OF ACTION A: STATUS QUO

This course of action leaves everything as it currently stands. The ACDC Act has not passed the U.S. Congress, nor has similar legislation passed the legislative branch of any other nation. Active cyber defense measures, which exceed authorized levels of access, are at least arguably illegal as detailed in U.S. legal debate and the *Tallinn Manual 2.0.* Furthermore, this course of action assumes civil and possibly criminal actions will increase against entities engaged in active cyber defense measures—using logic proposed by MacDermott and others—as they shore up their cyber postures.

B. COURSE OF ACTION B: NO INTERNATIONAL DISPUTE MITIGATION BODY

This course of action assumes only the ACDC Act is passed; there are no other changes to U.S. legislation or the international legislation detailed in the *Tallinn Manual 2.0*. This course of action assumes the U.S. Congress passed and the President signed the ACDC Act, which creates an affirmative defense for private entities to employ active cyber defense measures external to their networks upon notification to federal law enforcement.[106]

[106] Active Cyber Defense Certainty Act.

C. COURSE OF ACTION C: INTERNATIONAL BODY TO ADDRESS CYBER DISPUTES

This course of action assumes the ACDC Act is passed, the U.S. creates a national director of cybersecurity as detailed in this chapter, and the Cyber Diplomacy Act of 2017 is passed. It further explores different bodies to mitigate disputes and makes a recommendation as to which body should mitigate any disputes that will inevitably arise as a result the ACDC Act's passing.

1. National Director of Cybersecurity

The U.S. government created a director of national intelligence in 2005 due to the 9/11 Commission's findings. Despite the model to have the various intelligence community (IC) members report to a single authority to facilitate a unified national intelligence plan, there is no single authority in the executive branch responsible for creating a unified cybersecurity policy. The head of the Department of Defense's U.S. Cyber Command is dual-hatted as the director of the NSA (an IC member). The Department of Homeland Security's National Protection and Programs Directorate oversees both the Office of Cybersecurity and Communications and the Office of Cyber and Infrastructure Analysis. The Department of Commerce's National Institute of Standards and Technology publishes and maintains the Cybersecurity Framework, which is mandated for use by the Department of Health and Human Services for the healthcare industry. The Department of Justice's criminal division oversees the Computer Crimes and Intellectual Property Section. In the federal law enforcement arena, the U. S. Secret Service is responsible for investigating crimes against the financial infrastructure committed by individuals; the Federal Bureau of Investigation enforces laws pertaining to both crimes committed by individuals and those for the purpose of espionage; U.S. Immigration and Customs Enforcement's Homeland Security Investigations division is responsible for investigating intellectual property fraud, which includes child pornography; and the Internal Revenue Service, among other agencies, has a cyber-crimes division. Those are a small sampling of federal law enforcement agencies with an interest in cybersecurity. The Federal Reserve Bank, a quasi-government entity, regulates a large percentage of America's banks and requires the

banking industry utilize the Federal Financial Institutions Examination Council's cybersecurity framework.

Each of the aforementioned entities has an impact on America's cybersecurity policy; however, as demonstrated by the differing cybersecurity frameworks required in two different critical infrastructure and key resource (CIKR) sectors, requirements conflict. With 85 percent of critical U.S. infrastructure owned by the private sector and the approximately 2,000 cyber-attacks that occurred in 2016 against the United States, the private sector also has a role in defending critical U.S. infrastructure given the potential impact to daily life in the event of an incident.[107] Owens, Dam, and Lin echo this sentiment when they call for an overarching national cybersecurity policy and one entity in charge to ensure the whole of U.S. government coordinates actions appropriately.[108] National security implications indicate the current model poses a risk to America's critical infrastructure.[109]

a. Cyber Threat Actors

The lack of a cohesive cybersecurity policy is also attributed to the cyber threat landscape. Nation-states, criminal syndicates, and hacktivist organizations all occupy the cyber threat space and have different motives and targets. Criminal syndicates attempt to steal easily monetized data. Hacktivist organizations generally try to embarrass organizations to correct a perceived wrong. Nation-state attacks may be offensive, gather intelligence, or involve monetary motivations.[110] Each group uses different attack vectors and methodologies; however, the most common attack vector for all groups involves the

---

[107] Government Accountability Office, *Critical Infrastructure Protection*, 2; and Verizon, *Data Breach Investigations Report*, 11.

[108] Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 56.

[109] Other homeland security professionals are increasingly arriving at the same conclusion as evidenced by articles like the following: David H. Petraeus and Kiran Sridhar, "The Case for a National Cybersecurity Agency," Politico, September 5, 2018, https://politi.co/2MOCnMh.

[110] Jim Finkle, "North Korea Likely behind Taiwan SWIFT Cyber Heist: BAE," Reuters, October 16, 2017, https://www.reuters.com/article/us-cyber-heist-north-korea-taiwan/north-korea-likely-behind-taiwan-swift-cyber-heist-bae-idUSKBN1CL2VO.

use of stolen credentials.[111] Because of the differing motivations, organizations that properly identify crown jewels can ascertain which protective measures to employ to mitigate attack vectors.[112] Consequently, the differing motivations of cyber threat actors should not prevent a cohesive national policy. Furthermore, one of the advantages in the cyber threat landscape can be information sharing between entities (e.g., public, private, and academic) about the differing attack vectors. Entities can implement specific controls to thwart attacks.

b. The National Director of Cybersecurity and the Private Sector

Assuming a national director of cybersecurity position comes to fruition, and given the preponderance of the CIKR sectors owned and operated by the private sector in the United States, what will the relationship be between the director and the private sector in a republican form of government? An attack against the power grid—to cite one example—is arguably an act of war. What role, if any, should a privately owned electrical company have in countering the attack? Should the government be responsible for mitigating all attacks? Given the civil liberty concerns with the U.S. government repairing any privately owned systems, mitigation by the government should be limited to identifying the attack vector and sharing best practices for mitigation. The appropriate sector of government—law enforcement for prosecutorial matters or the military for offensive matters—can then use the evidence gathered to pursue its stated goals. Nonetheless, the private sector must be responsible for mitigating the cyber-attack and implementing best practices. In a similar manner, the regulated CIKR sectors, such as the banking industry, must implement the Federal Financial Institutions Examination Council's cybersecurity framework or be held liable by the Federal Reserve Bank for preventable exploited measures that resulted in the

---

[111] Verizon, *Data Breach Investigations Report*, 16.

[112] *Crown jewels* are the key pieces of data and information a company has that make its business viable. The loss of this information generally means a company no longer exists. Among cybersecurity professionals, it is a common term and concept in describing what information a company must protect so that the proper tools can be put into place. *Misidentification* generally means the company is spending money to protect something that, if lost, is not critical to its business model. For an investment company, this would include both its client account information and trading strategy, which makes it different from other investment companies.

successful attack. This regulatory model is a framework to formulate the relationship between the national director of cybersecurity and the private sector, which controls 85 percent of America's critical infrastructure.[113]

c. The Dual-Hatted Role of U.S. Cyber Command and National Security Agency

The commander of U.S. Cyber Command also serves as the director of the National Security Agency. In addition to the elements directly under his or her control, each of the branches of the U.S. Armed Forces has a cyber component for offensive and defensive capabilities. Furthermore, the Defense Criminal Investigative Service, the U.S. Army's Criminal Investigative Division, the Naval Criminal Investigative Service, and the U.S. Air Force's Office of Special Investigations all have a dedicated cyber unit. Given the membership of the NSA in the IC, it is possible the goals of U.S. Cyber Command and the NSA may be at odds with one another. Without questioning the professionalism or the capability of the dual-hatted individual, is it possible for a single person to mediate between the two organizations on those occasions? Separating the roles of the commander of the U.S. Cyber Command and the director of the NSA seems a prudent place to begin with the creation of a national director of cybersecurity.

d. Conclusion

Considering the aforementioned items, the threat to national security created by the number of diverse and disparate executive branch entities with a role in the creation and implementation of America's cybersecurity policy necessitates the creation of a national director of cybersecurity. Furthermore, the director needs regulatory authority over private-sector CIKR entities to ensure best practices are followed, and the U.S. government issues a standard for the sectors to follow in cybersecurity matters. This will eliminate duplication of effort among the executive branch because policy matters will be implemented by a single entity. It should also have the added benefit of cost savings through the elimination of jobs. Like the director of national intelligence's budgetary authority over IC agencies,

[113] Government Accountability Office, *Critical Infrastructure Protection*, 2.

the national director of cybersecurity should have a similar authority to ensure policy matters in the executive branch are followed. Furthermore, as a co-equal to the director of national intelligence, the new position can help coordinate America's cybersecurity policy among the IC, the military, law enforcement, and the other executive branch entities engaged in cybersecurity activities. Finally, as with the director of national intelligence, the national director of cybersecurity should have some budgetary control over those entities to ensure compliance with the overarching policy. Just as the attacks on September 11, 2001, necessitated the creation of a director of national intelligence, the number of cyber-attacks occurring annually necessitates a unifying cybersecurity policy under a national director of cybersecurity.

2. Cyber Diplomacy Act of 2017 Passed

Given the concerns addressed in Chapter II of this thesis, Representative Royce's Cyber Diplomacy Act of 2017 works toward international consensus on actions in cyberspace. This course of action assumes the act passes the U.S. Congress and is signed by the President. Briefly, the Cyber Diplomacy Act of 2017 enacts the following:

- Creates a U.S. cyberspace policy to work with international partners to secure an open, free cyberspace,
- Creates a DoS Cyber Issues Office to negotiate on behalf of U.S. entities,
- Directs the executive branch to notify Congress of all existing international cyber arrangements, and
- Directs the executive branch to create an international strategy for cyberspace.[114]

[114] Cyber Diplomacy Act of 2017.

3. Possible Bodies to Mitigate Disputes

This thesis considers three possible entities to mitigate international disputes, which will arise unavoidably should the ACDC Act become law. The United States and 67 other nations are signatories to the Budapest Convention on Cybercrime, which provides a framework for countries to base cyber laws.[115] NATO's Cooperative Cyber Defence Center of Excellence (CCDCOE) is an expert in the laws of nations by virtue of its involvement with the *Tallinn Manual 2.0*.[116] Europol's European Cybercrime Centre (EC3) is a law enforcement information-sharing entity created for the worldwide reduction in cybercrime.[117]

a. Budapest Convention on Cybercrime

The Council of Europe and the United States realized a need for consistent legislation to address cyberspace worldwide in the late 1990s. Consequently, they gathered representatives in Budapest to discuss the various laws of the nations to establish a framework for permitted and prohibited activities in cyberspace. The negotiations created the Budapest Convention on Cybercrime treatise in 2001.[118]

b. Cooperative Cyber Defence Centre of Excellence

NATO created the CCDCOE in Tallinn, Estonia, in 2008 "to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation."[119] Currently, 20 of NATO's member countries are also members of the CCDCOE. To increase information sharing with the private sector, in 2009, the CCDCOE partnered with SEB—a Scandinavian banking institution—to study cyber threat activities.

---

[115] Convention on Cybercrime.

[116] "Home Page," NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), accessed May 28, 2018, https://www.ccdcoe.org.

[117] "European Cybercrime Centre - EC3," Europol, accessed May 28, 2018, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[118] Convention on Cybercrime.

[119] CCDCOE, "Home Page."

It conducts cyber table-top exercises for both the public and private sectors to help entities shore up cyber defenses. Finally, it contributed to the development of the *Tallinn Manual 2.0*, a one-stop resource for public and private entities alike to understand the various—and often conflicting—cyber laws of all nations.[120]

c. European Cybercrime Centre

In 2013, Europol created EC3 to bolster law enforcement's response to cybercrime globally by fostering increased cooperation through forensics education, outreach, and intelligence information sharing.[121] Conceptually, this increased law enforcement capability enhances cybersecurity for all sectors because it has an increased ability to identify nefarious actors. To accomplish its objectives, EC3 created three branches. The strategy branch supports outreach and prevention through threat awareness. The forensics branch helps educate law enforcement and creates best practices for cyber forensic techniques. The operations branch facilitates criminal investigations on child pornography, financial fraud, and other computer crimes by sharing information with members.[122]

4. Selecting a Mitigation Body to Handle Dispute Resolution

If the United States or another nation passes a law similar to the ACDC Act, a mechanism for mitigating international disputes must exist to address the inevitable disagreements between nation-states.

a. Dispute Resolution

The Budapest Convention on Cybercrime, the CCDCOE, and EC3 all have mechanisms for sharing information with members and non-members. The Budapest Convention on Cybercrime has a specific entity—the European Committee on Crime Problems (CDPC)—for mitigating disputes between members. The education wing of the CCDCOE and the strategy section of EC3 have outreach mechanisms embedded in their

---

[120] CCDCOE, "Home Page"; and Schmitt, *Tallinn Manual 2.0*.

[121] Europol, "European Cybercrime Centre."

[122] Europol.

core, which could be used by nations to facilitate dispute mitigation. Each of the aforementioned organizations has strengths and weaknesses in mitigating disputes.

The CDPC's mechanism for resolving disputes has been criticized for its lack of use and enforcement mechanisms by the signatories. Goldsmith cites the Budapest Convention on Cybercrime, which explicitly allows for the defense of computer networks as a justification for violating other protections under the treatise.[123] Goldsmith argues that a nation could attempt to justify its interests as a defensive measure in allowing for the attack on a sector or infrastructure otherwise protected by the treatise.[124] The Budapest Convention on Cybercrime further allows nations to express their reservations about any of the clauses as they become signatories.[125] Thus, as one signatory nation expresses reservations over a clause and a subsequent dispute arises, the CDPC would honor those expressed concerns in any subsequent dispute mitigation. Furthermore, if a nation asserts the violation was a defensive response to an offensive attack, it could be exempted from censure.[126] This defense may work in favor of a nation or its private entities employing active cyber defense measures; however, dispute mitigation may consequently be less than satisfactory.

The outreach mechanism embedded in each of the CCDCOE's various branches could prove beneficial to any dispute resolution. Specifically, the legal branch, with its work on the *Tallinn Manual 2.0* and the on-going seminars and classes it teaches on international law, is in the unique position of having learned all the facets of various nations' laws. The acquired knowledge base of the CCDCOE makes it uniquely positioned to engage in dispute resolution. Its sponsorship by NATO is both a strength and a weakness. The threat of military force behind a cyber violation on a member-nation both lends extreme credibility to any decisions made in dispute resolution and raises concern that a relatively minor dispute between nations could lead to a full-scale kinetic conflict. Thus,

[123] Convention on Cybercrime, art. 6, para. 2.

[124] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 5.

[125] Convention on Cybercrime, art. 42.

[126] Convention on Cybercrime, art. 6.

the threat of military force, whether perceived or actual, may limit the willingness of nations to bring disputes before the CCDCOE for mitigation.

Europol's EC3 is a law enforcement model for the enhancement of cybersecurity through increased cooperation among the members. Consequently, it relies solely on the laws of its member nations, which may or may not be aligned with the Budapest Convention on Cybercrime and the information sharing and mutual assistance provisions outlined in that document. Law enforcement does not lend itself to dispute mitigation; it enforces the rule of law as it is written. Therefore, though members and non-members alike cooperate with EC3 on crime enforcement matters, it would not be a good choice for dispute mitigation.

b. Implementation Possibilities

EC3, as a law enforcement entity, is not suited for dispute mitigation. Both the CDPC and the CCDCOE provide the knowledge of a legal framework or is itself a legal framework, which could be used as the foundation for dispute mitigation between nations. The advantage of using the CDPC arises from the fact that the Budapest Convention on Cybercrime is a framework for nations to create their cyber laws. The inherent weakness of the Budapest Convention on Cybercrime is the ability of nations to exempt themselves from several of the clauses while still being signatories. The CCDCOE's strength lies in its extensive study of international laws, and by extrapolation, it can articulate how an active cyber defense measure may infringe on the sovereignty of another.

The concern of the CCDCOE adjudicating a dispute is the threat of kinetic force by NATO if the losing nation does not abide by the imposed corrective measures. The only example from which any lessons can be drawn is in the Russian–Ukrainian conflict, which is both cyber and kinetic. The kinetic attacks on Ukraine by Russia began in 2014. The cyber-attacks most notably occurred in 2015 and 2017.[127] The kinetic warfare predates the cyber warfare, and the later cyber-attacks are more likely extensions of the kinetic war. Therefore, no reliable indicator exists. Certainly, nations will preserve the right to wage a

[127] Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: CCDCOE, 2015), 8.

kinetic war in response to a cyber-attack, as outlined in Air Marshal Phil Collins' UK Ministry of Defence May 28, 2018, speech to the Royal United Services Institute in the United Kingdom.[128]

The charters of both the Budapest Convention on Cybercrime and the CCDCOE need to be modified to become an effective mitigatory agency for disputes. The Budapest Convention on Cybercrime would need to empower the CDPC to mitigate disputes, which requires a change to the treatise, and ideally, nations should not be allowed to exempt themselves from clauses to become signatories, which requires an additional change to the treatise. If those fundamental changes were made, one can reasonably infer some nations would withdraw from the treaty, thereby limiting its effectiveness as a tool for mediation. The charter of the CCDCOE would need to be expanded to allow for it to serve as a mitigation agency.

The United States does not have any organization like either the CDPC or the CCDCOE in existence which could mitigate disputes between nations on cyber matters, which will arise with the implementation of the ACDC Act. As a signatory to both NATO and the Budapest Convention on Cybercrime, the United States could petition for either to serve as a mediator between nations for disputes. Representative Royce's proposed legislation—the Cyber Diplomacy Act of 2017—creates an entity within the DoS to negotiate cyber matters on behalf of the United States and, if passed, could liaise with the identified mitigation entity.[129]

c. Conclusion

The United States should petition NATO to change the charter of the CCDCOE, so it can be the international agency to mitigate cyber disputes between nations. The CCDCOE should use the Budapest Convention on Cybercrime as a framework for disputes arising from the implementation of the ACDC Act. As reflected in the literature, the CDPC

[128] Kevin Townsend, "UK Warns That Aggressive Cyberattack Could Trigger Kinetic Response," Security Week, May 25, 2018, https://www.securityweek.com/uk-warns-aggressive-cyberattack-could-trigger-kinetic-response.

[129] Cyber Diplomacy Act of 2017.

does not have the international regard of the CCDCOE, nor does it have the backing of NATO as a peacemaker—similar to the 1990 wars in the Balkans where NATO forces pacified the regional conflict. The CCDCOE's legal expertise with its work on the *Tallinn Manual 2.0* will help with its dispute mitigation because it has the perspective of the claimed affronts to a nation's laws. The CCDCOE's 29 centres provide the infrastructure necessary to mitigate disputes in a variety of locales.[130] Thus, with the infrastructure and the expertise in place, a slight expansion of the CCDCOE's mission by NATO would enable it to fulfill this role.

[130] CCDCOE, "Home Page."

IV. OPTIONS ANALYSIS USING A CYBER SCENARIO

Facilitating the evaluation of the courses of action presented in this thesis, the options analysis uses the following scenario, which replicates common cyber-attack patterns. An external cyber threat actor hacks a multi-national U.S. corporation, Cody's Haberdashery. During the hack, the cyber threat actor performs reconnaissance on the network, installs keystroke logger malware on the chief financial officer's computer, and successfully exfiltrates Cody's Haberdashery's banking account credentials. Subsequently, the cyber threat actor transfers a significant majority of Cody's Haberdashery's funds into a bank account in the People's Democratic Republic of Krasnovia—a non-signatory to the Budapest Convention on Cybercrime.[131] The criminals then convert the stolen funds into digital currency using a cryptocurrency exchanger that does not recognize U.S. legal proceedings. The cybercriminals further process their ill-gotten gains through an anonymizer. Cody's Haberdashery notifies U.S. federal law enforcement of the breach and its intent to use active cyber defense measures to track the internet protocol (IP) and media access control (MAC) addresses to identify the threat actor. During the deployment of active cyber defense measures, Cody's Haberdashery follows the cybercriminal's digital evidence trail and transits the networks of RiverBend Zachary, a company located in the Republic of Mojave—a signatory to the Budapest Convention on Cybercrime—without causing damage and discovers the IP and MAC addresses of the threat actor located in the People's Democratic Republic of Krasnovia.[132] Upon realizing a third party accessed its networks, RiverBend Zachary notifies law enforcement in the Republic of Mojave, which identifies the IP and MAC addresses of a computer from Cody's Haberdashery. The Republic of Mojave subsequently indicts the chief executive officer (CEO) of Cody's

[131] "National Training Center Scenarios," Global Security, accessed October 20, 2018, https://www.globalsecurity.org/military/ops/ctc-ntc-scenario.htm. Both the People's Democratic Republic of Krasnovia and the Republic of Mojave are fictional countries created by the U.S. Army for training scenarios at the National Training Center, Fort Irvin, CA. They are used here for representational purposes.

[132] Global Security, "National Training Center Scenarios."

Haberdashery and obtains an arrest warrant, which is filed with INTERPOL as a red notice.[133]

A. CRITERIA

For the options analysis criteria, this thesis considers the legality of the courses of action both within the United States and internationally as pivotal to any evaluation. Entities concerned about the legality of their actions usually do not employ questionable practices for fear of being held either criminally or civilly liable for their actions. Thus, deterrence can be a strong motivator for behavior, as Herath and Rao's 2009 study indicates.[134] As such, deterrence is included as the third and final evaluative criteria for this thesis.

1. Domestic Legality

Despite disagreement between various legal scholars on the legality or illegality of employing active cyber defense measures, the proposed ACDC Act changes the CFAA by expressly creating an affirmative defense for entities that use active cyber defense measures. Thus, for the purposes of the options analysis, without the passage of the ACDC Act, all active cyber defense measures used outside an entity's network are illegal under the CFAA. Therefore, in the absence of legislative action on the ACDC Act, any active cyber defense measures employed are deemed domestically illegal and represented by a "no" in Table 1. Active cyber defense measures employed after the assumed passage of the ACDC Act are deemed domestically legal and represented by a "yes" in Table 1.

2. International Legality

Because the *Tallinn Manual 2.0* definitively explores the laws of nations, which are outside the scope of this thesis, stating how different nations would judge active cyber defense measures is nearly impossible. This thesis uses the standards of the Budapest

[133] An INTERPOL red notice is used by member nations to notify other countries of extraditable warrants for wanted persons.

[134] Herath and Rao, "Protection Motivation and Deterrence," 112.

Convention on Cybercrime to evaluate international legality. As previously explored, the Budapest Convention on Cybercrime uses a similar standard of exceeding the level of authorized access in a network as the CFAA does. Kerr argues that by definition, active cyber defense measures exceed levels of authorized access.[135] As previously noted, the Budapest Convention on Cybercrime permits external defensive measures for the express purpose of protecting "a computer system."[136] Thus, without an international body to mitigate disputes, any employed active cyber defense measures are deemed illegal and annotated as a "no" in Table 1. Conversely, with the empowerment of an international body to mitigate disputes, any employed active cyber defense measures are deemed legal and reflected as a "yes" in Table 1.

3. Deterrence

As Hoffman and Levite propose, employment of active cyber defense measures has a deterrent effect on cyber threat actors as it reduces the illicit gains from stolen data because some of the tools employed potentially remove the anonymity currently enjoyed in cyberspace.[137] Using this framework, this thesis records a "yes" for the employment of active cyber defense measures and a "no" for course of actions which do not permit active cyber defense measures.

Using these definitions for the options analysis, Table 1 presents the findings, which are discussed and analyzed further following the table.

[135] Kerr, "Norms of Computer Trespass," 1143.

[136] Convention on Cybercrime, art. 6, para. 2.

[137] Hoffman and Levite, *Private Sector Cyber Defense*, 18.

Table 1. Options Analysis

	Domestic Legality	International Legality	Deterrence
Course of Action A	No	No	No
Course of Action B	Yes	No	Yes
Course of Action C	Yes	Yes	Yes

B. COURSE OF ACTION A: DISCUSSION

When the CEO of Cody's Haberdashery authorizes the use of active cyber defense measures external to his network, he permits both domestic and foreign illegal activity. In doing so, he runs afoul of the CFAA in the United States and the equivalent law in the Republic of Mojave by permitting his corporation to exceed its level of authorized access to RiverBend Zachary's network. After the Republic of Mojave subsequently indicts the CEO of Cody's Haberdashery and seeks an INTERPOL red notice, the United States should extradite him. Additionally, after he voluntarily provides evidence against himself to U.S. law enforcement of his illegal activities, the local U.S. Attorney's Office should also indict him for violating the CFAA, further adding to his legal woes. Finally, despite the identification of the cybercriminals in the People's Democratic Republic of Krasnovia and despite the lack of applicability of the exclusionary rule of evidence—because it was collected by a private entity not acting on the government's behalf—those cyber threat actors are not indicted. Therefore, course of action A does not deter the Krasnovian cyber threat actors because the evidence collected against them most likely will not be used in a court of law. Though not reflected in Table 1, the actual deterrence likely occurred with other U.S. corporations from using active cyber defense measures as they observed the legal proceedings against Cody's Haberdashery.

As demonstrated in the scenario, a private entity's use of active cyber defense measures external to its network is problematic. Given the lack of clear authorization to use these measures, it is unlikely a CEO would authorize such an action. Furthermore, the current system, a disincentive to report such breaches to law enforcement. Shareholders hold CEOs and other executives accountable for breaches, as evidenced in NeSmith's

Forbes article in June 2018, entitled "CEOs: The Data Breach Is Your Fault."[138] Given the lack of reporting for those reasons results in fewer prosecutions of cyber threat actors occur, which further reinforces the illegal behavior. Clearly, the status quo scenario does not improve global cybersecurity given the negative consequences for all except the cyber threat actor.

C. COURSE OF ACTION B: DISCUSSION

If the United States passes the ACDC Act without addressing the international concerns raised by such opponents as former Department of Justice cybersecurity prosecutor Luke Dembosky, no international body exists to negotiate on behalf of the CEO of Cody's Haberdashery.[139] Once the United States receives the red notice from INTERPOL, it is on a firm legal footing to exercise Chapter 1, Article 6, paragraph 2, of the Budapest Convention on Cybercrime, which permits external defensive measures to protect data because the actions of Cody's Haberdashery were expressly permitted under U.S. law. Likewise, it is more probable that a U.S. attorney will charge the perpetrators in the People's Democratic Republic of Krasnovia based on evidence provided by Cody's Haberdashery.

Course of action B does not alleviate the international legal woes faced by Cody's Haberdashery, but it does provide for a positive defense to any prosecution for violation of the CFAA, and the Budapest Convention on Cybercrime seems to support the corporation's actions. Because the Republic of Mojave is a signatory to the treaty, Cody's Haberdashery would have to mount a vigorous criminal defense in that country; however, because the outcome of the hypothetical criminal trial cannot be predicted, the international legality of this scenario is recorded as "no." Given the increased likelihood of criminal prosecution of the cyber threat actors in the United States, the deterrence of such behavior increases. Over time, identifying cyber threat actors and a corresponding increase in criminal indictments will deter illegal behavior in cyberspace.

---

[138] Brian NeSmith, "CEOs: The Data Breach Is Your Fault," *Forbes*, June 26, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/06/26/ceos-the-data-breach-is-your-fault/.

[139] Steven Nelson, "'Active Cyber Defense' or Vigilantism?," *Examiner*, February 7, 2018, https://search.proquest.com/docview/1999668841?accountid=12702.

D. COURSE OF ACTION C: DISCUSSION

A fuller range of options is available at the governmental and organizational levels in this scenario. Entities are free to use active cyber defense measures; the U.S. government has a national director of cybersecurity and an office within the Department of State (DoS) to interact with the CCDCOE; and the CCDCOE, backed by the power of NATO, is the international entity to mitigate disputes between nations. In the scenario, when Cody's Haberdashery coordinates with U.S. federal law enforcement, the information is passed to the national director of cybersecurity. Later, when the Republic of Mojave indicts the CEO of Cody's Haberdashery and requests that INTERPOL issue a red notice, the U.S. federal law enforcement already has evidence that identifies the cyber threat actors in the People's Democratic Republic of Krasnovia.

The Office of Cyber Issues under the DoS can present that evidence to the CCDCOE as mitigating factors, which demonstrate that the actions of Cody's Haberdashery were defensive in nature when it transversed the networks of RiverBend Zachary in the process of identifying the Krasnovian cyber threat actors. The Office of Cyber Issues can invoke Chapter 1, Article 6, paragraph 2, of the Budapest Convention on Cybercrime. The Republic of Mojave can then use that information to vacate the criminal indictment against the CEO of Cody's Haberdashery and issue a new indictment against the cyber threat actors in the People's Democratic Republic of Krasnovia. Additionally, the United States can unseal its earlier criminal indictment against those same actors from Krasnovia, who used the evidence uncovered by Cody's Haberdashery during the employment of the active cyber defense measures. The Krasnovian cybercriminals are then publicly identified. The United States, the Republic of Mojave, and the CCDCOE request extradition. Because a clause in the constitution of the People's Democratic Republic of Krasnovia forbids the extradition of its citizens to third nations, it does not comply; however, the veil of anonymity over the Krasnovian cybercriminals has been lifted, limiting their ability to operate and preventing them from traveling outside the country.

With course of action C, the Office of Cyber Issues presents the legally defensible actions of Cody's Haberdashery under U.S. law, made available through information sharing under the national director of cybersecurity to the CCDCOE by invoking the

defensive clause under the Budapest Convention on Cybercrime. This, in turn, causes the Republic of Mojave to vacate its warrant. In such a case, the actions are internationally legal. Finally, multiple governments issue arrest warrants for the cyber threat actors, creating a deterrence effect for others—as detailed in works like Herath and Rao's study—due to the increased opportunity cost for the illicit behavior.[140]

As demonstrated, the more holistic approach available under course of action C—through the passage of the ACDC Act and the Cyber Diplomacy Act of 2017, the creation of a national director of cybersecurity, and the empowerment of the CCDCOE to resolve the international dispute that arose from Cody's Haberdashery's employment of active cyber defense measures—enable two countries to indict the cybercriminals in the People's Democratic Republic of Krasnovia. As these types of measures continue, course of action C will have a deterrent effect on illegal cyber activities because it increases the opportunity cost over time when the perpetrators are identified.

Because cyber threat actors will not know the active cyber defense capabilities of their targets, globally cybersecurity can improve as a result. Opponents may argue the use of the information gleaned from active cyber defense measures in a public forum (e.g., criminal prosecutions) will enable the cyber threat actors to change their tactics. This may occur, but the abilities of cyber defenders will increase as well, which negates this objection. The continual increase in breaches demands that action be taken. The combination of actions in option C will help make cyberspace a more secure environment for all.

[140] Herath and Rao, "Protection Motivation and Deterrence," 112.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS AND CONCLUSION

Proponents and opponents of active cyber defense measures all agree cybersecurity is a national security issue for the nations of the world. For instance, on July 24, 2018, German interior minister Horst Seehofer called for the use of active cyber defense measures as he released the domestic intelligence service's report of cyber-attacks in Germany.[141] The time has come for authorization of active cyber defense measures by private entities, notwithstanding pithy quotes such as the following in *Computer Shopper*'s Zygote column:

> Although the new bill is full of good intentions, it is called the Active Cyber Defense Certainty act. This has been abbreviated by its sponsors to ACDC, once labelled by Rolling Stone magazine as the greatest rock'n'roll band of all time. However, Zygote reminds the U.S. House of Representatives that AC/DC's greatest hit was called Highway to Hell, which is what good intentions end up becoming.[142]

A. RECOMMENDATIONS

As many others have noted, the time has come for the U.S. government to enable the private sector the ability to engage in active cyber defense measures. The legislative branch, the executive branch, NATO, and the private sector all have a role to play in the implementation of active cyber defense measures. As there is some ambiguity surrounding the employment of active cyber defense measures, the U.S. Congress needs to make at least some facet of active cyber defense legal. The executive branch needs to develop the policy surrounding the legalization of active cyber defense. NATO should explore a role in the mitigation of disputes arising between nations from the employment of active cyber defense measures. The private sector needs to develop implementation techniques. More specifics follow in the next four sections.

---

[141] Andrea Shalal and Thomas Escritt, "In Cyber, Germany Needs to Counter-Attack, Minister Says," Reuters, July 24, 2018, https://www.reuters.com/article/us-germany-espionage-cyber/in-cyber-germany-needs-to-counter-attack-minister-says-idUSKBN1KE0X3.

[142] "Parting Shots," Zygote, *Computer Shopper*, February 2018.

1. Legislative Branch

This thesis was written as a U.S. congressional session nears its end, which means the proposed legislation discussed throughout may expire. Regardless, this or a subsequent session of Congress can incorporate the recommendations into current or future legislative proposals. To remove the ambiguity surrounding the employment of active cyber defense measures, the U.S. Congress needs to pass the ACDC Act with the following modifications:

- The legislative branch should combine the ACDC Act and the Cyber Diplomacy Act of 2017 to incorporate the explicit authorization of active cyber defense measures as a positive defense to the Computer Fraud and Abuse Act (CFAA) and the creation of an office to address cyber matters on an international stage on behalf of the United States.

- The legislative branch should create a national director of cybersecurity, a co-equal of the director of national intelligence (DNI), to unify the cybersecurity policy of America.

- The national director of cybersecurity should have limited budgetary authority and some operational control over all executive branch agencies with a role in cybersecurity, as the DNI has over the intelligence community, to ensure compliance with national policy.

- The national director of cybersecurity should have regulatory control over the private sector's employment of active cyber defense measures, similar to the Federal Reserve Board's authority over the banking sector, to help ensure best practices are followed.

- The legislative branch needs to amend the Cyber Diplomacy Act of 2017 to account for the creation of the national director of cybersecurity.

- The legislative branch must remove the limiting factor in the ACDC Act for the cooperation of the private sector with the Federal Bureau of Investigation

(FBI). It needs to be broadened to include any federal law enforcement agency with jurisdiction over the CFAA and the national director of cybersecurity as well as to account for the creation of the national director of cybersecurity and the statutory authorization of federal law enforcement agencies in the CFAA.

- The legislative branch needs to amend the ACDC Act further to define the concept of "persistent attack" as Lin and Chesney indicate.[143]

2. Executive Branch

The President should direct the executive branch to perform the following actions:

- The executive branch should create a National Cybersecurity Advisor, similar to the National Security Advisor, until such time as the legislative branch creates the national director of cybersecurity to unify the policy of various U.S. entities with a role in cybersecurity.

- The executive branch should create policies and a mechanism for the private sector to work with federal law enforcement and the national director of cybersecurity in their employment of active cyber defense measures.

- The executive branch should separate the roles of U.S. Cybercommand and the director of the National Security Agency to end the potential conflicts of interest between the two roles.

- The executive branch needs to work with international partners to develop a consensus on the employment of active cyber defense measures as defined by the ACDC Act.

[143] Chesney, "Legislative Hackback"; and Lin, "More on the Active Defense Certainty Act."

- The executive branch should work with NATO to change the charter of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) to enable it to mitigate disputes between nations on the employment of active cyber defense measures.

3. NATO

NATO and NATO's CCDCOE play an integral role in dispute mitigation. As such,

- NATO should explore whether its charter needs to be modified to allow for the CCDCOE to mitigate cyber disputes between nations.
- The CCDCOE should examine methods to implement the dispute mitigation outlined in this thesis.
- The CCDCOE should continue the legal analysis that began in its *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

4. Private Sector

As the implementor of legalized active cyber defense measures, the private sector has a key role and should do the following:

- Develop best practices and policies for the employment of active cyber defense measures[144]
- Develop relationships with federal law enforcement, so it is known before the employment of active cyber defense measures whom to call and what response to expect
- To further develop these relationships, as well as cross-sector relationships, the private sector should join organizations such as the U.S. Secret Service's Electronic Crimes Task Forces and the FBI's InfraGard

[144] Blair et al., *Into the Gray Zone*; and Rosenweig, Bucci, and Inserra, "Next Steps for US Cybersecurity."

B. AREAS OF FUTURE STUDY

A suggested future area of study regarding active cyber defense measures is bounded by the Second Amendment to the U.S. Constitution. MacDermott raises the issue when she asserts the right granted within the Constitution around the concept of a militia.[145] The Second Amendment reads as follows: "A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed."[146] As discussed in the literature review's legal analysis, deterrence theory, and the Law of Armed Conflict sections, both proponents and opponents of active cyber defense measures compare the use of cyber measures to the use of arms. The breadth and scope of this concept demand a study of its own accord.

Another suggested future area of study is the use of artificial intelligence in conjunction with the deployment of active cyber defense measures. As cyber-attacks take nanoseconds to execute, would the employment of artificial intelligence to counter the cyber-attacks automatically increase the effectiveness of active cyber defense measures? Would the employment more rapidly identify the perpetrators of the attack? Would the employment of artificial intelligence remove some of the stigma related to the use of active cyber defense measures?

A third suggested area of study would be to develop more fully the employment of active cyber defense as recommended in this thesis. How specifically will the flow work between nations to resolve disputes? With the creation of a national director of cybersecurity, how will the different executive branch agencies work together toward a unified cybersecurity policy? How will the CCDCOE resolve the inevitable disputes between nation-states? What is the mechanism to bring the disputes before the CCDCOE? Much work remains in developing procedures for employing the recommendations from this thesis.

---

[145] MacDermott, *The Folded Paper*, 116.

[146] U.S. Const. amend. II, https://www.usconstitution.net/xconst_Am2.html.

C. CONCLUSION

All agree the current state of cybersecurity needs to be improved globally. Though there is significant disagreement on the employment of active cyber defense measures, this thesis concludes that to raise the collective cybersecurity of all, active cyber defense measures need to be legalized and employed. Doing so will deter cyber threat actors and change their cost–benefit analysis in conducting illicit activities in cyberspace. Creating a national director of cybersecurity to unify and coordinate the cybersecurity policy of the United States will only strengthen the employment of active cyber defense. Likewise, empowering NATO's CCDCOE to mitigate disputes between nations will also facilitate information sharing between nations, making it harder for faceless enemies to remain anonymous.

Cybersecurity is a collective issue. It is limited neither to the government nor to the private sector. Only through the cooperation and mutual support outlined in this thesis can the U.S. government raise the collective security of all. Active cyber defense is a facet of that collaboration. It is naïve for an entity to rely on passive cyber defense measures to protect its crown jewels. The time for collective action is now. The bipartisan legislation legalizing active cyber defense as proposed by Representatives Graves and Sinema in conjunction with the other measures presented in this thesis is the first step.

LIST OF REFERENCES

Amao, Michael. "Active Cyber Defense to Fight Cybercrime." Master's thesis, Utica College, 2015.

Andres, Richard. "Cyber Gray Space Deterrence." *PRISM* 7, no. 2 (December 21, 2017): 91–98.

Blair, Dennis C., Michael Chertoff, Frank J. Cilluffo, and Nuala O'Connor, eds. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: George Washington University, Center for Cyber and Homeland Security, 2016.

Borghard, Erica D., and Shawn W. Lonergan. "Why Are There No Cyber Arms Control Agreements?" Defense One. January 18, 2018. http://www.defenseone.com/ideas/2018/01/why-are-there-no-cyber-arms-control-agreements/145289/.

Chen, Jim. "Cyber Deterrence by Engagement and Surprise." *PRISM* 7, no. 2 (December 21, 2017): 101–7.

Chesney, Robert. "Legislative Hackback: Notes on the Active Cyber Defense Certainty Act Discussion Draft." *Lawfare* (blog), March 7, 2017. https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft.

Collins, Raymond Martin Luther. "Proactive Cybersecurity through Active Cyber Defense." Master's thesis, Utica College, 2017.

Computer Shopper. "Parting Shots." Zygote. February 2018.

Cook, Chris. "Hacking Back in Black: Legal and Policy Concerns with the Updated Active Cyber Defense Certainty Act." *Just Security* (blog), November 20, 2017. https://www.justsecurity.org/47141/hacking-black-legal-policy-concerns-updated-active-cyber-defense-certainty-act/.

Cranford, Nathan. "How to Protect NFV and SDN from Cyber Attacks." RCR Wireless News. July 31, 2017. http://www.rcrwireless.com/20170731/nfv/how-to-protect-nfv-and-sdn-from-cyberattacks-tag27-tag99.

Denning, Dorothy E. "Framework and Principles for Active Cyber Defense." Monterey, CA: Naval Postgraduate School, December 2013.

Department of Homeland Security. *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013.

Department of Justice. *Computer Crimes and Intellectual Property Section: Prosecuting Computer Crimes*. Washington, DC: Office of Legal Education, 2015.

Dewar, Robert S. *CSS Cyber Defence Trend Analysis 1: Active Cyber Defense*. Zurich: Center for Security Studies, 2017.

Dubai Media. "Telecommunications Regulatory Authority Prevents 289 Cyber-Attacks in Q1 2017." July 31, 2017. http://www.emirates247.com/news/emirates/telecommunications-regulatory-authority-prevents-289-cyberattacks-in-q1-2017-2017-07-31-1.656939.

Eichensehr, Kristin E. "Would the United States Be Responsible for Private Hacking?" *Just Security* (blog), October 17, 2017. https://www.justsecurity.org/46013/united-states-responsible-private-hacking/.

Elsom, Dan. "Five of the Worst Cases of Cybercrime the World Has Ever Seen – from Stealing Data from One Billion Yahoo Users to Crippling the NHS." *The Sun* (London), July 31, 2017. https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/.

Europol. "European Cybercrime Centre - EC3." Accessed May 28, 2018. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Fadilpašić, Sead. "Nearly a Million UK SMEs Hit by Cyber-Attacks." IT Pro Portal. July 31, 2017. http://www.itproportal.com/news/almost-a-million-smes-victims-to-cyber-attacks-in-the-last-year/.

Finkle, Jim. "North Korea Likely Behind Taiwan SWIFT Cyber Heist: BAE." Reuters. October 16, 2017. https://www.reuters.com/article/us-cyber-heist-north-korea-taiwan/north-korea-likely-behind-taiwan-swift-cyber-heist-bae-idUSKBN1CL2VO.

Geers, Kenneth, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: CCDCOE, 2015.

Global Security. "National Training Center Scenarios." Accessed October 20, 2018. https://www.globalsecurity.org/military/ops/ctc-ntc-scenario.htm.

Goldfoot, Josh, and Aditya Bamzai. "A Trespass Framework for the Crime of Hacking." *George Washington Law Review* 84, no. 6 (December 2016): 1477–99.

Goldsmith, Jack. "Cybersecurity Treaties: A Skeptical View." In *Future Challenges in National Security and Law*, edited by Peter Berkowitz. Palo Alto, CA: Hoover Institution Task Force on National Security and Law, Stanford University, February 2011.

Government Accountability Office. *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors Characteristics*. Washington, DC: GAO, October 2006.

Graham, Luke. "Cybercrime Costs the Global Economy $450 Billion: CEO." CNBC. February 2, 2017. https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html.

Graunke, Kevin. "Shielded from Cyberattacks." *Christian Science Monitor*, July 31, 2017. https://www.csmonitor.com/Commentary/A-Christian-Science-Perspective/2017/0731/Shielded-from-cyberattacks.

Grimes, Roger A. *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*. Indianapolis: Wiley, 2017.

Herath, Tejaswini, and H. Raghav Rao. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems* 18, no. 2 (2009): 106–25. https://doi.org/10.1057/ejis.2009.6.

Higgins, Joshua. "Industry: New House Bill Lays Groundwork for Policy Dialogue on Active Cyber Defense." *Inside Cybersecurity*. March 7, 2017. http://libproxy.nps.edu/login?url=https://search.proquest.com/docview/187507644 5?accountid=12702.

Hoffman, Wyatt, and Ariel E. Levite. *Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?* Washington, DC: Carnegie Endowment for International Peace, 2017.

Huq, Numaan, Rainer Vosseler, and Morton Swimmer. "Cyberattacks against Intelligent Transportation Systems: Assessing Future Threats to ITS." Research paper, TrendMicro, 2017.

Kerr, Orin. "Norms of Computer Trespass." *Columbia Law Review* 116 (May 1, 2016): 1143–84.

Lin, Herb. "More on the Active Defense Certainty Act." *Lawfare* (blog), March 24, 2017. https://www.lawfareblog.com/more-active-defense-certainty-act.

Lindsay, Jon. R. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39, no. 3 (Winter 2014): 7–47. https://doi.org/10.1162/ISEC_a_00189.

MacDermott, Siobhan. *The Folded Paper: Inventing Cyberdiplomacy*. North Charleston, SC: CreateSpace Independent Publishing Platform, 2018.

McGee, Shane, Randy V. Sabett, and Anand Shah. “Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense.” *Journal of Business & Technology Law* 8, no. 1 (2013).

NATO Cooperative Cyber Defence Centre of Excellence. “Home Page.” Accessed May 28, 2018. https://www.ccdcoe.org.

Nelson, Steven. “‘Active Cyber Defense’ or Vigilantism?” *Examiner*, February 7, 2018. https://search.proquest.com/docview/1999668841?accountid=12702.

NeSmith, Brian. “CEOs: The Data Breach Is Your Fault.” *Forbes*, June 26, 2018. https://www.forbes.com/sites/forbestechcouncil/2018/06/26/ceos-the-data-breach-is-your-fault/.

Newsmax. “Cyber ‘Worm’ Hurts Corporate Earnings, Sparks $850 Million in Damage.” August 2, 2017. http://www.newsmax.com/Finance/StreetTalk/cyber-worm-notpetya-earnings/2017/08/02/id/805374/.

Nieto-Gómez, Rodrigo. “Cyber-Geopolitics: Geopolitical Rivalries behind the Cyber-Threat Narratives in the United States.” *Medium* (blog), August 20, 2014. https://medium.com/homeland-security/cyber-geopolitics-a45fc698a3a1.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press, 2009.

Pan Kwan Yuk and Mamta Badkar. “Merck Updates Guidance to Reflect June Cyber Attack.” *Financial Times*, July 31, 2017. https://www.ft.com/content/3d7ac341-1742-3329-9a15-2dc269522d10.

Petraeus, David H., and Kiran Sridhar. “The Case for a National Cybersecurity Agency.” Politico. September 5, 2018. https://politi.co/2MOCnMh.

Petski, Denise. “HBO Confirms It Was Hit by Cyber Attack.” Deadline. July 31, 2017. http://deadline.com/2017/07/hbo-confirms-cyber-attack-hack-1202139202/?utm_source=dlvr.it&utm_medium=twitter.

Pitman, Paul M. “Research Methods, Part II: Policy Options Analysis.” Lecture module, Center for Homeland Defense and Security, 2017. https://www.chds.us/coursefiles/NS4081/lectures/methods_policy_options_analysis_v02/methods_policy_options_lec_v02.pdf.

Pogue, Chris. *The Black Report*. Edited by Josh Mehlman. Herndon, VA: Nuix, 2017.

Reid, Scott. “Hundreds of Thousands of SMEs Hit by Cyber Attacks.” *The Scotsman*, July 31, 2017. http://www.scotsman.com/business/companies/tech/hundreds-of-thousands-of-smes-hit-by-cyber-attacks-1-4518376.

Rosenweig, Paul, Steven P. Bucci, and David Inserra. “Next Steps for US Cybersecurity in the Trump Administration: Active Cyber Defense.” *Backgrounder*, no. 3188 (May 5, 2017): 11.

Rouse, Margaret, and Matthew Haughn. “What Is Botnet Sinkhole?” TechTarget. June 2014. http://whatis.techtarget.com/definition/botnet-sinkhole.

Sancho, David, and Ranier Link. “Sinkholing Botnets.” Technical Paper, TrendMicro, 2011.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Seger, Alexander. “The Budapest Convention on Cybercrime: A Framework for Capacity Building.” *Global Cyber Expertise Magazine*. Vol. 2. November 2016.

Shalal, Andrea, and Thomas Escritt. “In Cyber, Germany Needs to Counter-Attack, Minister Says.” Reuters. July 24, 2018. https://www.reuters.com/article/us-germany-espionage-cyber/in-cyber-germany-needs-to-counter-attack-minister-says-idUSKBN1KE0X3.

Steptoe & Johnson. “The Hackback Debate.” *Steptoe Cyberblog*, November 2, 2012. http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

Symantec. *Internet Security Threat Report*. Vol. 22. Mountain View, CA: Symantec, 2017.

Taddeo, Mariarosaria. “The Limits of Deterrence Theory in Cyberspace.” *Philosophy & Technology* 31, no. 3 (September 2018): 339–355. https://doi.org.libproxy.nps.edu/10.1007/s13347-017-0290-2.

Taft, William H., IV. “The Law of Armed Conflict after 9/11: Some Salient Features.” *Yale Journal of International Law* 28, no. 2 (2003): 319–23.

Thomson, Iain. “US Congress Mulls First ‘Hack Back’ Revenge Law. And Yup, You Can Guess What It’ll Let People Do.” Register. October 13, 2017. https://www.theregister.co.uk/2017/10/13/us_hack_back_law/.

Townsend, Kevin. “UK Warns That Aggressive Cyberattack Could Trigger Kinetic Response.” Security Week. May 25, 2018. https://www.securityweek.com/uk-warns-aggressive-cyberattack-could-trigger-kinetic-response.

Tromp, Joshua. “Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-Attacks.” *Small Wars Journal* 12, no. 1 (January 28, 2016). http://smallwarsjournal.com/jrnl/art/law-of-armed-conflict-attribution-and-the-challenges-of-deterring-cyber-attacks.

Trustwave. *2017 Trustwave Global Security Report*. Chicago: Trustwave Holdings, 2017.

U.S. Congress. House of Representatives. Active Cyber Defense Certainty Act. H.R. 4036. 115th Cong., 1st sess. (2017). https://www.congress.gov/bill/115th-congress/house-bill/4036.

———. Cyber Diplomacy Act of 2017. H.R. 3776. 115th Cong., 1st sess. (2017). https://www.congress.gov/bill/115th-congress/house-bill/3776/text.

Verizon. *2017 Data Breach Investigations Report*. 10th ed. New York: Verizon Enterprise Solutions, 2017.

Waldrop, M. Mitchell. "How to Hack the Hackers: The Human Side of Cybercrime." *Nature* 533, no. 7602 (May 12, 2016): 164–67. https://doi.org/10.1038/533164a.

White, Jautau Kelton. "Impact of Protection Motivation Theory and General Deterrence Theory on the Behavioral Intention to Implement and Misuse Active Cyber Defense." PhD diss., Capella University, 2017.

Wong, Tiong Pern. "Active Cyber Defense: Enhancing National Cyber Defense." Master's thesis, Naval Postgraduate School, 2011.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California