2015-03

Cyber war: the next frontier for NATO

Jones, Ken M.

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/45201

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBER WAR: THE NEXT FRONTIER FOR NATO

by

Ken M. Jones

March 2015

Thesis Advisor:	Dorothy Denning
Second Reader:	Wade Huntley

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
March 2015

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE
CYBER WAR: THE NEXT FRONTIER FOR NATO

5. FUNDING NUMBERS

6. AUTHOR(S) Ken M. Jones

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. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Defining and understanding what constitutes a cyber-attack is a complicated matter, largely due to the fact that there has not yet been a large-scale cyber-attack upon any nation. With the help of Michael Schmitt's *Tallinn Manual*, published in 2013 by Cambridge University Press, it is possible to gain an understanding, although no policy expectations, of what elements need to be met for a cyber-attack to warrant a NATO response.

This study analyzes and explores the unique position that NATO operates in and the duty of NATO to protect its alliance members, and member states to protect each other. Topics discussed include how cyber-attacks are defined and identified, the particular challenges of NATO when addressing cyber-attacks, the severity of cyber-attacks, and what would need to occur in order for a victim-state to ask NATO to invoke Article 5.

This thesis discusses the readiness of NATO to respond to a cyber-attack and what the conditions necessary for an Article 5 response, and what that response would potentially look like. Finally, this work provides recommendations for actions that NATO could take to both prevent and confront cyber attacks.

14. SUBJECT TERMS
NATO, Article 5, cyber-attack, Tallinn Manual

15. NUMBER OF PAGES
71

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

THIS PAGE INTENTIONALLY LEFT BLANK

CYBER WAR: THE NEXT FRONTIER FOR NATO

Ken M. Jones
Lieutenant, United States Navy
B.A.S., Wayland Baptist University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
March 2015**

Author: Ken M. Jones

Approved by: Dr. Dorothy Denning
Thesis Advisor

Dr. Wade Huntley
Second Reader

Dr. Cynthia Irvine
Chair, Department of Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Defining and understanding what constitutes a cyber-attack is a complicated matter, largely due to the fact that there has not yet been a large-scale cyber-attack upon any nation. With the help of Michael Schmitt's *Tallinn Manual*, published in 2013 by Cambridge University Press, it is possible to gain an understanding, although no policy expectations, of what elements need to be met for a cyber-attack to warrant a NATO response.

This study analyzes and explores the unique position that NATO operates in and the duty of NATO to protect its alliance members, and member states to protect each other. Topics discussed include how cyber-attacks are defined and identified, the particular challenges of NATO when addressing cyber-attacks, the severity of cyber-attacks, and what would need to occur in order for a victim-state to ask NATO to invoke Article 5.

This thesis discusses the readiness of NATO to respond to a cyber-attack and what the conditions necessary for an Article 5 response, and what that response would potentially look like. Finally, this work provides recommendations for actions that NATO could take to both prevent and confront cyber attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

9/11	September 11
CASIC	China Aerospace Science and Industry Corporation
CCDOE	Cooperative Cyber Defense Center of Excellence
CDMA	Cyber Defense Management Authority
CDMB	Cyber Defense Management Board
DDoS	distributed denial of service
ENISA	European Network and Information Security Agency
EU	European Union
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NCI	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCO	noncommissioned officer
RMM	resilience management model
SACEUR	Supreme Allied Commander Europe
SCADA	supervisory control and data acquisition
SHAPE	Supreme Headquarters Allied Powers Europe
U.S.	United States

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would never have been able to finish my thesis without the guidance of my advisors and the continued support from my family and friends, especially my wife.

I would like to express my deepest gratitude to my advisor, Dr. Dorothy Denning, for her excellent guidance, encouragement, patience, and providing me with a ton of material that greatly assisted me with my academic research. She steered me when I was confused and, most certainly, is the most knowledgeable on this subject matter. Her knowledge and academic guidance were invaluable to me. I would also like to thank Dr. Wade Huntley, my second reader, who pushed me to be a better writer and critical thinker and challenged me to my fullest potential. I would also like to thank Dr. Duane Davis for being a voice of reason throughout the entire master’s program. I would also like to thank the chair of the Cyber Academic group, Dr. Cynthia Irvine, who created an outstanding Cyber Systems and Operations curriculum from which the military will benefit for years to come. A special thank you goes to all the professionals who work at the Naval Postgraduate School Thesis Processing Office. I would like to specifically thank Sue Hawthorne, who works tirelessly to ensure students graduate with a professionally formatted and edited thesis. She is an invaluable asset to NPS.

Finally, I would again like to thank my beautiful wife, Rachel. She was always there by my side, encouraging me to never give up and keep pressing forward.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Mark Twain wrote, “From the ‘London Times’ of 1904” in 1898, a science fiction tale that describes a marvelous invention called a “telelectroscope.” This amazing device is hooked to the telephone system (a fairly new invention at the time) whereupon the user of the device can view and talk to people all over the world. Unbeknownst to him, in his short story Mark Twain imagined the Internet into existence a century before it was to become a reality.[1] Albert Einstein is quoted as saying, “Imagination is more important than knowledge,” a statement that has never held more weight than it does when applied to the cyber world, a place where nearly anything is possible, so long as the user or creator can imagine it. In both Mark Twain’s and Albert Einstein’s time, the Internet was nothing more than science fiction; an imaginary device that an author invented to make a story interesting, and not something that could ever legitimately exist. Now, the Internet and the cyber-world therein is not only a reality, it is used in almost every aspect of human life from recreational to entertainment to professional use, and it would be nearly impossible to imagine living in a world without it.

With the increase in the use of the Internet and the easy access for individuals around the world to computers and the Internet, it is easier than ever for nations to utilize cyber warfare against their enemies. This leads to the primary question of this thesis, how should North American Treaty Organization (NATO) respond to a cyber-attack against a member country? NATO is a collection of about two dozen countries dedicated to working together and collaborating to ensure the safety and defense of each nation, and available to support militarily member states in need. Knowing that cyber-attacks are on the rise, the secondary focus of this thesis is to determine if NATO is prepared to respond to a cyber-attack on a member state, and if not, what policy changes are needed to be made in order for NATO to be better prepared.

[1] Crawford Kilian, “Mark Twain, Father of the Internet,” The Tyee, January 8, 2007, http://thetyee.ca/Books/2007/01/08/MarkTwain/.

A. DEFINE THE PROBLEM

The Internet has made the world a substantially smaller place and more connected in ways that were seemingly impossible before now. However, with all the positive things that exist thanks to the Internet and technology, there is also a sinister, unwholesome side that exists simultaneously. As in the physical world, the cyber world breeds criminals looking to make a quick buck through fraudulent means, hackers looking for fun, hacktivists looking to make a political or social point, terrorists looking to recruit new members, and finally, government organizations looking to advance their country's power or position in the global hierarchy. Individuals, states, and non-state actors use cyber-attacks as a way to advance their agenda. Common examples of cyber-attacks include computer viruses, worms, malware, and distributed denial of service (DDoS) attacks.

The 2007 cyber-attack on the nation of Estonia illustrates the potential for a serious cyber-attack and the long-lasting effects of one. For a three-and-a-half week period starting on April 27, 2007, and finally ending on May 18, 2007, parts of the nation's Internet-based infrastructure were targets of powerful DDoS attacks.[2] Government websites were shut down, as were those of two major banks holding the accounts of thousands of citizens and several political parties.[3] Like many nations, Estonia relies on its cyber infrastructure and, therefore, the 2007 attack created a major headache for millions of Estonians, which led some professionals to refer to it as "Web War I," while others have called it a "cyber-riot."[4] The cyber-attack was even more damaging due to the fact that Estonia is extremely reliant on the Internet and Internet connections. In response to the attacks, NATO created the Centre of Excellence for Cyber Defense, located in Tallinn, Estonia.[5] NATO also created the Cyber Defence Management Authority. In creating both these organizations, NATO recognized the need

[2] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49–60, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.

[3] Ibid.

[4] "War in the Fifth Domain," July 3, 2010, http://www.economist.com/node/16478792.

[5] Ibid.

to prepare for, and respond accordingly to, any future cyber-attacks of this magnitude on alliance members. In addition, NATO produced a document known as the *Tallinn Manual* that, while non-binding, applies international law and NATO policies to cyber warfare.

B. OVERVIEW

NATO as an organization is designed to protect and assist member states. Though it had a very loose cyber policy, it did not have a clear protocol for how to respond to a cyber-attack against a member country. However, the attack against NATO served as a wake-up call and the following year NATO held its first meeting on the topic, known as the Bucharest Summit, to formally address the issue of cyber-attacks.[6] Two divisions were created, the Cyber Defense Management Authority and the Cooperative Cyber Defense Centre of Excellence. This led to the creation of the *Tallinn Manual*. Produced by a team of international law experts led by Professor Michael Schmitt and published in 2013, it offers guidelines on how to treat cyber warfare within international law.

C. THESIS PROPOSAL QUESTIONS

The central focus of the thesis is to perform a thorough analysis using three guiding questions to narrow the scope of the investigation of how NATO is coping with the potential of cyber-attacks on a member state and how the organization should respond to a cyber-attack. First, is NATO prepared to respond to a cyber-attack? Second, under what conditions would a cyber-attack trigger a NATO Article 5 response? Third and final is the question how would NATO respond to a cyber-attack under Article 5?

Due to the fact that there has yet to be a cyber-attack that has forced NATO to respond, NATO is working to get a clearer understanding of when it would, or *should*, respond to a cyber-attack and under what conditions it would be reasonable to respond

[6] NATO, “Bucharest Summit Declaration,” last modified May 8, 2014, http://www.nato.int/cps/en/natolive/official_texts_8443.htm.

with a response under Article 5.[7] Article 5 of the Washington Treaty provides for several expectations of NATO in the event of a kinetic attack against a member state, which is now also considered to include a cyber-attack.[8] The core of Article 5 revolves around collective defense against an aggressor state on behalf of a member state, but would be reviewed on a case-by-case basis.[9] NATO has left criteria for invoking Article 5 for a cyber-attack purposefully vague, possibly because there has not yet been an attack on an alliance member state that caused significant damage similar to that of a significant kinetic attack, with states mindful not to create dangerous precedent. The only substantial cyber-attack event that could help to understand what NATO might do is the cyber-attack on Estonia in 2007. Although that attack did not result in an Article 5 response, this does not mean there was not the possibility of retaliation. Then Minister of Defense, Jaak Aaviksoo reportedly contemplated seeking out NATO assistance in helping his country overcome the attack, suspected to have been committed by Russia or non-state Russian actors.[10] Since the Estonia attack, the closest that NATO has moved toward defining when an Article 5 response would occur was at the recent 2014 summit in Wales when it was announced that if there were to be a cyber-attack on a member state, Article 5 could be invoked and lead to a response.[11]

D. METHODOLOGY

This thesis uses descriptive and analytical approaches to answer the thesis questions. Through a careful review of Articles 4 and 5 of the Washington Treaty, as well as past and current responses to cyber-attacks by NATO, this thesis will outline the strategies that NATO employs to protect member states. Starting with a detailed analysis

[7] Article 5 is part of the Washington Treaty and provides for the ability for the United States to aid its allies in Europe but was first invoked by Europe to offer aid to America following the 9/11 attacks. The Article is meant to offer automatic support to a member state, but allows the particular state to decide how that aid would be defined. Hannes Krause, “Invocation in Context,” *NATO Review*, 2006, http://www.nato.int/docu/review/2006/issue2/english/summaries.html.

[8] Ibid.

[9] Ibid.

[10] Josephine Wolff, “NATO’s Empty Cybersecurity Gesture,” *Slate Magazine*, September 10, 2014, http://www.slate.com/articles/technology/future_tense/2014/09/nato_s_statement_on_cyberattacks_misses_some_fundamental_points.html.

[11] Ibid.

of NATO and what thresholds have needed to be passed in order for NATO to organize a ground offensive, the thesis will draw parallels to suggest when cyber-attacks might evoke an Article 5 NATO response. In support of what type of events might need to occur in order for there to be an Article 5 response following a cyber-attack, there will be comparative case studies and review of the first time NATO invoked an Article 5 response, following the September 11, 2011 terror attacks. Through a review of the prevailing literature and available information, inferences can be drawn as to when or how NATO should respond to a cyber-attack against a member country and when it would be appropriate to invoke an Article 6 response against a cyber-attack. The descriptive and analytical pieces of this thesis rely on official statements from NATO, experts in the field of cyber defense, and information published in official NATO sources. This thesis utilizes primary and secondary sources to provide a complete and current picture of how NATO policy has evolved and where current challenges still exist.

E. THESIS ORGANIZATION

This thesis is organized into six chapters. Chapter I is the introduction, providing all of the pertinent background information regarding this thesis and its purpose. Chapter II is a brief literature review, offering background information for the reader unfamiliar with the topic and its importance. Chapter III pertains to NATO, the history of the organization, the creation, drafting, and publishing of the *Tallinn Manual*, and a discussion on Articles 4 and 5 of the Washington Treaty, including why both articles are important and their invocation following 9/11. Chapter IV focuses on cyber-attacks, what they are, major international cyber-attacks, and the problems that NATO is facing in terms of responding to a cyber-attack. Chapter V explores the question of whether NATO is prepared to respond to a cyber-attack, investigates what conditions would be necessary for a cyber-attack to trigger a NATO Article 5 response and studies how NATO would respond to a cyber-attack under Article 5. Chapter V explores what conditions would need to exist if NATO were to go outside of Article 5 to respond and provides recommendations on how NATO should respond to future cyber-attacks. Chapter VI is the conclusion, including areas of understanding and unresolved issues in the current research, areas of agreement and understanding, and a discussion of unresolved issues.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Defining and understanding what makes up a cyber-attack appears to be a simple task, until the topic is delved into, at which point the difficulty of the topic is realized. Authors have tried to create scenarios that could play out in the event of a cyber-attack, but often the scenarios have been perceived as alarmist and reactive, and not based on events that are actually likely to occur. Other authors have taken a more proactive approach, looking at the various laws that dictate domestically, and how those laws would handle cyber-attacks, which are often classified as terror attacks within the cyber realm.

In the book, *Cyber War*, Clarke and Knake use what reads as hysterical overreaction to stress their point regarding the threat of cyber-attacks on the United States. The authors arrange the book well, hitting upon topics in a methodological order while also providing detailed technical analysis of the issue of cyber war, particularly in relation to China and Russia.[12] While providing a good historical background on American policy on the topic of cyber warfare, the book is more of an opinion piece, providing their thoughts and logic on why more has not been done in order to protect the American people from an attack.[13] Even with the questions regarding the validity of their beliefs, and the alarmist stance that they take, the book offers the reader substantial information regarding cyber warfare.

In "Perspectives for Cyber Strategists on Law for Cyberwar," Charles Dunlap takes a look at the legal issues and requirements in relation to international law and treaties that have been ratified.[14] An essential question that Dunlap attempts to describe and answer is what the parallels are between a conventional military attack and a cyber-attack, specifically in terms of the Law of Armed Conflict.[15] The Law of Armed Conflict

[12] Richard A. Clarke and Robert K. Knake, *Cyber War* (New York City: Harper Collins, 2011).

[13] Ibid.

[14] Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly Spring 2011* (2011), http://www.au.af.mil/au/ssq/2011/spring/dunlap.pdf.

[15] Ibid.

is a principle element of international law that seeks to limit all unnecessary violence and unwarranted military action. Dunlap also introduces the idea that cyber-warfare and cyber-crime are two substantial threats facing the West right now and that there need to be more preventative measures introduced in order to address the threat.[16] According to Dunlap, the introduction of the Stuxnet virus and the WikiLeaks document drop have led some to believe that all-out cyber war is inevitable, if not already underway but undetected.[17]

Hathaway et al. also address the issue of law and cyber-attacks, stressing the importance of the international legal system while also providing tangible steps that can be taken in order to shore up American security and NATO partner states.[18] They claim that cyber-attacks are becoming more and more sophisticated, agreeing with Dunlap regarding their strength and danger, and capable of shutting down nuclear centrifuges, electric grids, or air defense systems.[19] They argue that it is important for cyber-attacks to be treated with the sense of urgency that is needed, and in some cases should be treated as acts of war.[20] Hathaway et al. introduce many ways that laws already in place can be applied to cyber-attacks, while making it a point to define cyber-attacks, which many scholars struggle to do.[21] The most effective suggestion made by Hathaway et al. is for the United States to use its ability to strengthen domestic law by making cyber-attacks extraterritorial and adopting very limited countermeasures to fight against cyber-attacks, which do not qualify as an appropriately comparable kinetic attack to trigger an armed response.[22]

[16] Dunlap Jr., “Perspectives for Cyber Strategists on Law for Cyberwar.”

[17] Ibid.

[18] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, “The Law of Cyber-Attack,” *Yale Law Review 100* (2012), http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Ibid.

Henry S. Kenyon, in "Cyber Attacks Reveal Lessons," reviews the Estonia cyber-attacks that took place in April and May 2007 and introduced to the public the new cyber-attack: hard to track, hard to fight, hard to detect, and a threat to international security.[23] Kenyon claims that the attacks were so damaging to Estonia that they nearly paralyzed the government and almost forced a complete shutdown of services as the country relies extensively on e-commerce and online transactions, two areas of infrastructure that were targeted.[24] The attacks on Estonia were likely perpetrated by Russia, but that is determined largely by using context clues, with Kenyon pointing out that there were political and social events taking place with the government removing a war memorial of the Red Army out of a town center and into a cemetery.[25] The statue caused a substantial amount of civil unrest with many Estonians believing that the statue was a negative symbol of their oppression during the Soviet years and their time living as part of the Soviet Union, while ethnic Russians felt slighted and believe that the statue is a monument of Russian sacrifice.[26] The attacks against Estonia, Kenyon points out, are unique in that it was not a single, sustained attack but several attacks aimed at different infrastructure, with the denial-of-service attacks debilitating due to the e-commerce society Estonia is so proud of.[27]

Herzog writes on the same topic as Kenyon, the Estonian cyber-attacks and the effect of the attacks, as well as the multinational responses. Making Estonia unique is the fact the government relies on digital infrastructure, which also makes Estonia an easy target for denial-of-service attacks.[28] According to Herzog, there are only a small handful of advanced cyber-warfare states, including China, the United States, Russia, and Israel, leading these countries, and their adversaries, to investigate further their own cyber-

[23] Henry S. Kenyon, "Cyber Attacks Reveal Lessons," *Signal* 63, no. 11 (2009), http://www.afcea.org/content/?q=cyber-attacks-reveal-lessons.

[24] Ibid.

[25] Ibid

[26] Ibid

[27] Ibid

[28] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49–60.

attack capabilities.[29] NATO, unable to truly point a finger because there was no trail, stated rather clearly that the attack on Estonia was the concentrated efforts of a single state, and due to the geopolitics at the time, that state was likely Russia.[30] Unlike Kenyon, and the other authors reviewed here, Herzog jumps into NATO Article 5 headfirst, stating that had Russia attacked Estonia using conventional means, such as tanks and bombs, NATO would have had to invoke Article 5, yet NATO did not mount such a response.[31] An attack or attempt to stop Russia could have had serious detrimental effects against Russia, particularly pertaining to their valuable and economically necessary energy, which provides much of Russia's wealth.[32] Then, Herzog delves into the multinational response to the Estonia cyber-attack, labeling the attack a "mild version of a new form of digital violence," and highlighting the seriousness of the issue.[33]

Keiran Hardy questions what affect that post-9/11 lawmaking had on the issue of cyber-terrorism, looking at the issue by comparing U.S. laws to commonalities in laws of four Commonwealth states: Australia, New Zealand, Canada, and the United Kingdom. Hardy attempts to provide a framework of debate by critiquing the legislation that was passed following 9/11 and could be utilized in prosecuting cyber-attacks.[34] Hardy calls the U.S. legislation draconian and exceptional, but refrains from calling it unlawful, stating that the Americans save the harshest penalties for when cyber-attacks cause or attempt to cause death.[35] The four Commonwealth countries, in an attempt to truly attack the problem of cyber-attacks, instead proffer a low threshold of harm and high penalties up to life in jail for any act of terrorism focusing on the digital or electronic systems or

[29] Ibid.

[30] Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," 49–60.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Keiran Hardy, "WWWMDs: Cyber-Attacks Against Infrastructure in Domestic Anti-Terror Laws," *Computer Law & Security Review* 27, no. 2 (April 2011): 152–161, http://dx.doi.org/10.1016/j.clsr.2011.01.008.

[35] Ibid.

infrastructure.[36] Australia, New Zealand, Canada, and the United Kingdom hold the crimes to a much lower standard when compared to the United States, with Hardy subtly hinting that maybe the United States should better focus anti-terrorism laws to include true cyber-attacks, and offer penalties for acts of cyber-terrorism less extreme than death-inducing.[37]

In "NATO: Defending Against the Known Unknowns," Tony Morbin focuses on the 200-person cyber security NATO team that is responsible for protecting NATO's networks, and providing and implementing cyber-security solutions.[38] Morbin states there are, every single day, more than 200 million potential cyber-attacks against NATO's systems by states, crime syndicates, terrorist organizations, and hacktivists.[39] While acknowledging that some of those are falsely reporting as cyber-attacks, this does highlight the scope of the issue of security and the need for organizations, NATO included, to take cyber-security extremely serious. According to Chief of Cyber Security for the NATO Communications and Information Agency (NCI), Ian West, interviewed by Morbin, the goal is to get the number of attempted attacks needing intervention down to ten per day, which is a reasonable goal with careful programming.[40] Morbin's article highlights the true capabilities of NATO today, and the fact that NATO is prepared to handle a cyber-attack if one is launched against it, just leaving open the issue of what NATO would do if one of the alliances' member states were to suffer a cyber-attack. West, in highlighting the singular goal of NATO, to defend NATO, points out that all of their work in the cyber-world is based around defending against a cyber-attack.[41] While this is a logical and necessary approach, NATO could also share its technology and

[36] Ibid.

[37] Hardy, "WWWMDs: Cyber-Attacks Against Infrastructure in Domestic Anti-Terror Laws," 152–161.

[38] Tony Morbin, "NATO: Defending Against the Known Unknowns," *SCMagazine UK*, 2015, http://www.scmagazineuk.com/nato-defending-agains-the-known-unknowns/article/400190/.

[39] Ibid.

[40] Ibid.

[41] Ibid.

knowledge with member states to help them be better protected from cyber-attacks as well.

Jeffrey Caton authored a substantial and thorough document, “Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications,” for *The United States Army War College*. Caton immediately addresses the fact that there is no internationally accepted definition of what a hostile action is in cyberspace.[42] The intended purpose of his manuscript is to provide policy makers, politicians, military leaders, and decision makers a foundational background in the issue of cyber-attacks and hostile actions in cyberspace for the formation of cyber policy.[43] Caton not only provides policy considerations, but he also provides detailed assessment criteria utilizing information from international bodies, such as the United Nations.[44] Finally, Caton provides the reader with courses of action that can be taken while addressing the various influences that have an effect on decision makers and the ways to overcome them.[45] While seeming to make great promises in the information he is going to offer, Caton admits that it would be impossible for him to come up with the perfect solution. Instead, he offers various options and ideas, supported by data and international law. Caton remains honest in his discussion of each topic, admitting that there is no international legal definition of what a cyber-attack would look like, but then offers his own definition of the concept for the reader, even if it is broad.[46]

There is a remarkable void in the literature addressing cyber-attacks and Article 5, but this may be because there has not yet been a cyber-attack of sufficient severity to trigger an Article 5 response, or perhaps scholars are focused more on legality under the UN Charter, particularly Articles 2(4) on use of force and Article 51 on armed attacks (plus international humanitarian law). Since NATO’s Article 5 is based on UN Article

[42] Jeffrey L. Caton, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications* (Carlisle Barracks, PA: The United States Army War College, Strategic Studies Institute, 2014).

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

51, what is determined for 51 also applies to Article 5. There are a few articles that handle the issue in the abstract, but they are filled with conjecture. While there is no international definition of what a cyber-attack is, academics and policymakers do believe they have an understanding of what a cyber-attack would look like. Similarly, academics seem to agree that when there is a cyber-attack worthy of an Article 5 response, it will be obvious and comparable to a kinetic attack. With all of the questions regarding what a cyber-attack would need to look like in order to garner a response, there is consensus that such a picture is hard to draw until there is an event. The cyber-attack on Estonia is the only cyber-attack that might have warranted an Article 5 response, but did not result in any type of response, leaving the people of Estonia exposed until the attacks were finally thwarted.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NATO

A. HISTORY OF NATO

NATO was officially created on April 4, 1949, in Washington, DC, with the United States, the United Kingdom, France, Canada, Belgium, the Netherlands, Luxembourg, Iceland, Denmark, Norway, Italy, and Portugal signing what became known as the Washington Treaty.[47] NATO was unique upon its official creation due to the fact it was the first peacetime military-based alliance that the United States had ever entered into that did not focus on the Western Hemisphere.[48] NATO was formed for three overarching purposes, in the words of Lord Ismay, the first NATO Secretary General, "to keep the Russians out, the Americans in, and the Germans down."[49]

Of the Washington Treaty's fourteen articles, Article 5 provides NATO's core collective defense commitment and is the most significant for the purpose of this thesis. Article 5 states that:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.[50]

[47] "Milestones: 1945–1952; North Atlantic Treaty Organization (NATO), 1949," accessed March 12, 2015, https://history.state.gov/milestones/1945-1952/nato.

[48] Ibid.

[49] David Reynolds, *The Origins of the Cold War in Europe: International Perspectives* (New Haven, CT: Yale University Press, 1994), 13.

[50] "North Atlantic Treaty," accessed March 13, 2014, http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

Article 4 precedes Article 5 and states:

> The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.[51]

Article 4 is not difficult to understand. It clearly states that alliance members will meet, talk about the problem facing one or all of them, and then decide as a group what the best course of action should be. In practice, Article 4 would bring together the members of NATO, and Article 5 provides the capability for member states to support, militarily, NATO member states under attack or requiring defense.

During the first several decades of NATO's existence, this collective defense commitment was focused on ensuring that the Soviet Red Army did not advance further through Europe. Article 5 provided the European states with the reassurance they needed that the United States would intervene on their behalf in the event of Soviet attack.

This reassurance generally sufficed despite serious questions regarding the ability of the Americans to act because of U.S. constitutional constraints. The European NATO members did not just want reassurance that the United States would intervene on their behalf, but they wanted the United States to do so automatically, and without having to seek approval from a potentially hostile Congress.[52] This was complicated by the U.S. Constitution, which provides Congress the sole authority to declare war; through negotiations it was written that the United States would be able to seek approval from Congress for any large-scale military incursion.[53] There were also issues when it comes to the need of the European countries to have the United States provide military assistance in an attempt to rebuild the decimated defense system following the close of the Second World War.[54] The European states each wanted unconditional grants for the process of rebuilding and refocusing their defense systems, but the United States, as the largest funder of NATO, wanted the aid to be based on, and contingent upon, regional

[51] "North Atlantic Treaty."

[52] Ibid.

[53] Ibid.

[54] Ibid.

coordination.[55] The all-encompassing negotiations ended with the signing of the Treaty and led to the declaration that an attack on a member state was like an attack on each state and should be treated as such.[56]

Surprisingly, it was the communist uprising and outbreak of the Korean War that led to NATO fully developing into the organization that it is today. Thirteen months following the official creation of NATO, war broke out on the Korean Peninsula, and member states were once again forced to recognize the increasing threat of communism around the globe.[57] The Korean War saw the Supreme Headquarters Allied Powers Europe (SHAPE) form to help direct and disperse forces throughout Europe; this was overseen by Dwight D. Eisenhower, Supreme Allied Commander.[58] During this same period of time, there was an increase in the number of troops on the ground, in order to match what the Soviet's had lined up, waiting patiently for the allies to act; NATO was forced to create military plans that would be adhered to when in a state of war.[59]

France struggled with the dominant role that the United States took within NATO and the close relationship between The United States and the United Kingdom. When President Eisenhower and Prime Minister Harold Macmillan did not respond to France in the way that President Charles de Gaulle had hoped, de Gaulle sought out other allies in the event that East Germany invaded West Germany.[60] De Gaulle pulled back the Mediterranean Fleet, banned all nuclear weapons from French soil, and removed all fleets from NATO Command. As a result, SHAPE move from a Paris suburb to Casteau, Belgium.[61] De Gaulle's infuriating move complicated the Cold War alliances and would

[55] "Milestones: 1945–1952; North Atlantic Treaty Organization (NATO), 1949."

[56] Ibid.

[57] David C. Isby, and Charles Kamps, Jr., *Armies of NATOs Central Front* (New York City, NY: Jane's Information Group, 1985), 14.

[58] Ibid.

[59] Ibid.

[60] National Defense University, *Allied Command Structures in the New NATO* (Collingdale, PA: Diane Publishing, 1997), 50.

[61] Ibid., 53.

go on for 43 years.[62] France would finally fully rejoin NATO under President Nicolas Sarkozy, highlighting the changing conditions of French security.[63] Sarkozy made it a point to reunite with NATO as part of his plan to strengthen ties to the United States, and helping to redefine the mission of NATO in the 21st century.[64]

During the Cold War, NATO's primary function was to defend Europe against the Warsaw Pact nations led by the Soviet Union. Because much of this defense relied on U.S. nuclear deterrence, a substantial amount of the Cold War involved showing strength, though not through military incursions. The goal of NATO to maintain the security of the member nations with nuclear deterrence unintentionally resulted in a nuclear arms race between the United States and the Soviet Union.[65] Later in the Cold War, the U.S.-led policy of détente was in part meant to ensure that NATO states could match the defenses of Warsaw Pact states while curbing nuclear buildups and stabilizing relations. When non-nuclear NATO states signed the Nuclear Non-Proliferation Treaty in 1968, the United States held on to its nuclear weapons in part because maintaining extended deterrence guarantees to these NATO allies was a condition of their own nuclear forbearance.[66]

At the end of the Cold War, NATO had to reevaluate its position now that the Soviet Union had fallen and the organization was no longer needed to protect against an aggressive communist regime. The November 1991 Rome Summit saw the approval of a new strategic concept that realigned the purpose of NATO in the new, communist-free Europe.[67] The new concept saw the need for smaller and more flexible forces, not a massive buildup of troops waiting for the invasion of the multi-million strong Soviet Army; it also called for a focus on the traditional defense mission and not, just the Soviet

[62] Edward Cody, "After 43 Years, France to Rejoin NATO as Full Member," *Washington Post*, March 12, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/11/AR2009031100547.html.

[63] Ibid.

[64] Ibid.

[65] Raymond L. Garthoff, *Détente and Confrontation: American-Soviet Relations from Nixon to Reagan* (Washington, DC: Brookings Institute Press, 1994), 661.

[66] Ibid., 657–664.

[67] "Milestones: 1993–2000; North Atlantic Treaty Organization (NATO), 1949," accessed March 12, 2015, https://history.state.gov/milestones/1993-2000/evolution-of-nato.

enemy.[68] Through the Rome Summit, there were important discussions and decisions made regarding the European Union and NATO's role in the growing body, and for the first time NATO truly took part in the discussion regarding the strategic architecture of Europe and became a partner with other European-based groups.[69] This was further cemented following the 1994 Brussels Summit and the creation of a Combined Joint Task Force, as well as discussions over enlargement of NATO.[70]

Enlargement was an issue that was hotly debated and contested with policymakers concerned about the cost and implications of introducing more states into the alliance. In late 1996, NATO finally announced that they were going to expand and invite new member states in July 1997 after a summit that was to be held in Madrid.[71] The dominant concern was with Russia, and how the Russian government would feel about an expanded NATO, and what effect that would have on the delicate balance of democracy that had been embraced. President Boris Yeltsin and President Bill Clinton would discuss this issue face-to-face in March 1997 at a summit in Helsinki, Finland.[72] The meeting went exceptionally well, and it was agreed upon that both countries, while in disagreement over the expansion of NATO, would consult and make joint decisions whenever possible in regards to Russia and NATO security.[73]

B. NATO AND THE *TALLINN MANUAL*

The *Tallinn Manual*, prepared by the Cooperative Cyber Defense Center of Excellence and published by Cambridge University Press, is an attempt to apply customary international law to generate legal principles for the developing field of cyber warfare.[74] The Cyber Defense Center is an International Military Organization accredited

[68] "Milestones: 1993–2000; North Atlantic Treaty Organization (NATO), 1949."

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Ibid.

[73] Ibid.

[74] Michael N. Schmitt, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal Online* 54 (December 2012): 13.

by the North Atlantic Council (NAC), NATO's top political decision making arm. The *Tallinn Manual*, though written by a panel of experts on international law, does not hold legal authority. Nevertheless, it can be used to help guide a response following a cyber-attack on a member nation. In the newly developing field of cyber warfare, it is important that what constitutes an armed attack be defined, since this threshold triggers the right to utilize self-defense. Part A, Chapter II, Section 2 deals specifically with self-defense in the *Tallinn Manual* and is the focus of this section. Rules 13 through 17 apply to responses that use force.

The task of understanding when a cyber-attack qualifies as a true attack on another state is difficult due to the lack of an agreed-upon definition for such an attack. That being said, there are not firm globally-agreed definitions for "use of force" or "armed attack" either. It is in NATO's best interest, at least while the field of cyber warfare is still developing, to remain ambiguous to ensure states can act with their own best interests without limitation or legal hindrance. The information provided in the *Tallinn Manual* is largely written in the abstract, possibly because it seeks to frame an ethics for cyber conflict in a world that is only now starting to get to the point at which significant harm can be caused via a cyber-attack. The potential for damage has most recently been displayed by North Korea in attacking Sony Entertainment over the release of a movie it found repugnant.[75] November 2014 saw North Korea hack into Sony's computers, destroy data, and steal a substantial amount of information, which was then released to the public in a series of humiliating data dumps.[76] As the field becomes more developed, and as more attacks, such as the one by North Korea occur, it will be in the NATO member states' best interest to better define cyber warfare as it is experienced and the damage caused can be evaluated.

[75] Oliver Laughland, "FBI Director Stands by Claim that North Korea Was Source of Sony Cyber-Attack," *The Guardian*, January 7, 2015, http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey.

[76] Ibid.

Rule 13, “Self-Defense Against Armed Attack,” focuses on the right that all states have to defend themselves in the event of a cyber-attack.[77] For an attack to constitute an armed action, a trans-border element is essential, which results when one state attacks another, or when a state targets another by utilizing a non-state actor to behave in such a way that it would conduct an attack in the name of that state.[78] This definition becomes more convoluted when the attack occurs by a non-state actor not acting under the direction of the state.[79] There are many questions raised when it comes to the very core of the NATO alliance and the promise that states have made to come to the defense of one another when they are attacked. Understanding the role of a cyber-attack in providing a response is important and will slowly develop, as there is more experience with cyber-attacks.

Much like kinetic attacks, when a state is attacked via the cyber-world, the right to use force as a means of self-defense is extended to the cyber realm.[80] The International Group of Experts that created the *Tallinn Manual* agreed that a cyber-attack could be significant enough to warrant classifying as an armed attack. They also agreed that labeling it as such would be in accordance with the *Nuclear Weapons Advisory*[81] opinion of the International Court of Justice, which concluded that the means of attack is immaterial to its classification.[82] For a state to exercise its right of self-defense, the consequences of the cyber-attack would need to have resulted in serious suffering or death, similar to what would warrant self-defense in a kinetic attack.[83] The *Manual* also states that “armed” does not have to include “weapons,” and that emphasis should be placed upon the effects caused in the attack.[84]

[77] Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2013), 53.

[78] Schmitt, *Tallinn Manual*, 54.

[79] Ibid.

[80] Ibid.

[81] Ibid.

[82] Ibid.

[83] Ibid.

[84] Ibid.

Rule 13 includes criteria that would delineate an armed attack, namely the scale and effect of the attack.[85] Although the rule is ambiguous, because it fails to define scale and effect of an attack, it is drawn from the *Nicaragua*[86] judgment that stated a difference must exist between the worst types of use of force and the less grave types of force.[87] While situations occur in which this difference is very clear, for instance, when people are killed, instances could also occur when the consequences of the attack are less obvious, which makes it difficult to know if the attack meets the scale and effect requirement.[88] The Group of Experts stated that if the cyber-attack merely gathered intelligence information, engaged in cyber theft, or resulted in other non-essential information being gathered, characterizing it as an armed attack would be inappropriate.[89] They noted that the question of whether cyber-attacks that did not cause death, injury, damage, or destruction could be considered armed attacks was unsettled and that there were no clear lines delineating such attacks. They considered a cyber-attack on the New York Stock Exchange that caused the market to crash. Although no one would be physically hurt, some argued that the attack could be considered an armed attack owing to its possibly catastrophic effects.[90]

The *Tallinn Manual* states in Rules 14 and 15 that the right to use force in self-defense depends on necessity, proportionality, imminence, and immediacy.[91] The Group of Experts also expects that the victim-state will demand that the aggressor-state stop the

[85] Ibid.

[86] The Nicaragua judgment comes from *Nicaragua v. United States* that was heard by the International Court of Justice and decided in 1986. The judgment came following the U.S.' support of the Contras during the rebellion against the Nicaraguan government with judgment falling in favor of Nicaragua. The holding of the judgment found that the United States had interfered with state sovereignty and intervened in the affairs of Nicaragua, which helped to create clarification in the area of acting in self-defense by creating a concept of the threshold of force necessary to retaliate. International Court of Justice, "Military and Paramilitary Activities In and Against Nicaragua," June 1986, http://www.icjcij.org/docket/?sum=367&p1 =3&p2=3&case=70&p3=5.

[87] Schmitt, *Tallinn Manual*, 54.

[88] Ibid.

[89] Ibid.

[90] Ibid., 55.

[91] Ibid., 58.

activities comprising the attack.[92] Rule 14 deals specifically with necessity and proportionality, which must be met to apply force in self-defense, and were first introduced into the discourse of self-defense during the Nuremberg trials.[93] The principle of necessity requires that force be used only when non-forceful means would be insufficient. It is expected that non-forceful means will be attempted to end the situation, with the necessity to escalate to force always judged from the perspective of the victim-state.[94] Non-forceful means would typically manifest through diplomatic channels, talks between embassies, and resolutions passed by the United Nations. Proportionality is how much force is permitted, including in a cyber-attack that can be used in self-defense.[95] Proportionality limits the scope, scale, duration, and intensity to the minimum amount necessary to stop the situation and return to the status quo.[96]

There are several sections of the *Tallinn Manual* that NATO member states can refer to in determining if a cyber-attack warrants a NATO response. Rule 15 of the *Tallinn Manual* considers requirements for imminence and immediacy. Article 51[97] of the United Nations Charter does not explicitly grant permission to act defensively when it is merely believed that an armed attack will occur, but that does not mean that a potential victim-state should wait to be attacked.[98] In reality, a state should have the ability to protect its people; a potential victim-state has the ability to participate in anticipatory

[92] Ibid., 59.

[93] Schmitt, *Tallinn Manual*, 59.

[94] Ibid., 59–60.

[95] Ibid., 60.

[96] Ibid.

[97] Article 51 of the United Nations Charter states that when an armed attack occurs against a Member State there is nothing that prohibits the right of self-defense until the Security Council addresses the issue in order to restore peace and security. “Charter of the United Nations, art. 51,” ch. VII. 1945, http://www.un.org/en/documents/charter/chapter7.shtml.

[98] Schmitt, *Tallinn Manual*, 60.

self-defense, which is provided for following the *Caroline*[99] incident in the 19th century.[100] The Group of Experts acknowledged that some commentators believe it is never permissible to act in anticipatory self-defense, that use of force is only acceptable following an actual attack.[101] Regardless, the Group of Experts rejects the strict temporal analysis resulting in self-defense being triggered only after being attacked and agrees that an armed attack needs to be imminent to result in anticipatory use of force in self-defense.[102] The aggressive state needs to be preparing an attack, not just merely gaining the ability to launch an attack sometime in the future, which can be difficult to define due to the changing set of circumstances as each situation unfolds.[103]

Immediacy is what distinguishes an act of self-defense from an act of retaliation, with acts of retaliation never being permissible.[104] An even more difficult issue than differentiating between retaliation and self-defense is assessing the period of time that determines how long a state can wait before using force in self-defense following an armed attack against it.[105] Cyber warfare makes determining immediacy difficult because of the nature of a cyber-attack, which is important for NATO due to the expectation that member states will support each other when they become victims. Complicating matters even more, a victim-state might not even be aware that an attack is occurring on its systems, or the person committing the attack might not be known until following the attack when the damage is discovered and finally understood.[106]

[99] The aftermath of the *Caroline* Incident introduced into international law the concept of preemptive military force. A United States ship, the *Caroline*, attempted to provide aid to Canada in 1837 while Canada was engaging in an anti-British insurrection, which resulted in British troops crossing from Canada into American waters, boarding the *Caroline*, murdering several Americans, and then setting the ship on fire before sending it over Niagara Falls. The British claimed their actions were legal and in self-defense, but following diplomatic tensions between the United Kingdom and the United States Secretary of State, Daniel Webster, the United Kingdom would eventually apologize for its actions. Anthony Clark Arend, “International Law and the Preemptive Use of Military Force,” *The Washington Quarterly* 26, no. 2 (2003): 89–103.

[100] Schmitt, *Tallinn Manual*, 60.

[101] Ibid., 61.

[102] Ibid.

[103] Ibid., 62.

[104] Ibid.

[105] Ibid., 62–63.

[106] Ibid., 63.

Rule 16 covers collective self-defense, reiterating the need for necessity, proportionality, imminence, and immediacy in the exercise of such.[107] Rule 17 invokes Article 51 of the UN Charter, which states that when it is discovered that a cyber-attack is underway or has already occurred, the violation of Article 51 should be reported to the United Nations Security Council immediately.[108] At this point, if the situation is enough to be referred to the UN Security Council, it should be assumed that it is extensive enough for NATO to respond in defense of a members state under cyber-attack.

The *Tallinn Manual* uses expert opinion and imagined scenarios in its development of rules, which have yet to be applied in any serious "real-life" scenario as it relates to a cyber-attack. However, the publication of the *Tallinn Manual* is a step forward in cyber defense.

C. ARTICLES 4 AND 5, AND THE SEPTEMBER 11, 2001 ATTACKS

Some indications of how NATO might invoke Article 5 in response to a cyber-attack may be found by examining the only time Article 5 has been invoked at all. On September 11, 2001 the worst terrorist attack ever to occur on American soil resulted in about 3,000 murdered civilians in New York City, Washington, DC, and a field in western Pennsylvania. Four hijacked planes were turned into powerful weapons, killing thousands at the World Trade Center in Towers 1 and 2, and at the Pentagon. Article 5, which provides the basis for the NATO alliance and which holds the true power of the entire organization, was invoked following the 9/11 attacks due to the extraordinary nature of the attack. On September 12, 2001, for the first time since the Washington Treaty was signed, NATO invoked Article 5, with Secretary General Lord Robertson subsequently informing the United Nations of NATO's decision.[109] The NAC, in their subsequent statement on deliberations on deciding to invoke Article 5, stated, "if it determined that the attack was directed from abroad against the United States, it would be

[107] Ibid.

[108] Schmitt, *Tallinn Manual*, 64.

[109] "Collective Defense," accessed March 14, 2015, http://www.nato.int/cps/en/natohq/topics_110496.htm.

regarded as an action covered by Article 5."[110] Three weeks later, on October 2, 2001 NATO determined that the United States was attacked by enemy combatants and that the attacks were covered by the provisions of the Washington Treaty and Article 5.[111]

The alliance agreed that the attack on the United States was significant enough to invoke Article 5 for the following reasons:

- The attack was extremely severe that resulted in the loss of many lives and extreme damage to property
- The attack was executed with the use of improvised missiles (i.e., commercial planes) and therefore constituted "armed attack."[112]
- The attacks were conducted by a foreign enemy
- The attacks were planned
- The attacks were unprovoked
- In his statement following the September 11th attacks that explained the process leading to NATO's decision, Lord Robertson stated that in nearly six hours of considerations and conversations with distressed Prime Ministers, Foreign Ministers, and other officials, there was unanimous agreement in supporting the United States through Article 5.[113] Lord Robertson, who had to engage EU leadership, as well as the NATO Council, knew that Article 5, when written, had other circumstances in mind, not a terror attack of the magnitude of September 11th, but that he understood the entire world had changed, and NATO was going to have to transform in order to be effective.[114]

By invoking Article 5, NATO members offered statements in support of the United States, while also proffering statements condemning the terror attacks in the strongest possible way.[115] This was followed by several consultations among NATO members on what collective action should be taken with the understanding that the United States could also act unilaterally under the rights afforded to states that have been

[110] Ibid.

[111] Ibid.

[112] Edgar Buckley, "Invoking Article 5," *NATO Review*, Summer 2006, http://www.nato.int/docu/review/2006/issue2/english/art2.html.

[113] Lord George Robertson, "Being NATOs Secretary General on 9/11," *NATO Review*, accessed March 14, 2015, http://www.nato.int/docu/Review/2011/11september/Lord_Robertson/EN/index.htm.

[114] Ibid.

[115] "Collective Defense," accessed March 14, 2015, http://www.nato.int/cps/en/natohq/topics_110496.htm.

attacked in the United Nations Charter.[116] October 4, 2001 saw NATO agree to eight measures of support to the United States; the United States asked NATO for assistance, and NATO engaged in their first anti-terror mission, known as Eagle Assist, which lasted until May 2002.[117] This was followed by a second anti-terror operation, named Active Endeavor, with segments of NATO's naval forces being sent to the eastern Mediterranean Sea and working to deter and detect terror based activity.[118]

While NATO offered its full support to the United States, the United States selected its coalitions on a "case-by-case and mission-by-mission basis."[119] This led to significant speculation that the mission and purpose of NATO, even in invoking its most sacred and important article, had outlived its usefulness. There were questions about whether NATO could be successful as it was during the Balkans missions due to the United States choosing which coalitions it wanted to build instead of taking the whole of the NATO alliance.[120] There were also questions raised about the effectiveness in Iraq and Afghanistan of the ad hoc coalitions that the United States chose, and if there could have been a more positive, and shorter war, had NATO been fully included in the operations.[121]

In the years since the invocation of Article 5 following the 9/11 attacks, questions have been raised about the failure to invoke it before the attacks and in the years since.[122] In 1991, Article 5 was considered to assist with the First Gulf War, although Germany objected believing that the Iraqi missile attack on Turkey was not sufficient to invoke an Article 5 response.[123] Germany strongly believed that because the attack on Turkey had been in retaliation for the aggressive actions taken by Alliance members against Iraq, it

[116] Ibid.

[117] Ibid.

[118] "Collective Defense."

[119] Ellen Hallams, "The Transatlantic Alliance Renewed: The United States and NATO since 9/11," *Journal of Transatlantic Studies (Routledge)*, 7, no. 1 (Spring 2009): 41.

[120] Ibid., 44–46.

[121] Ibid., 49.

[122] Thomas Fedyszyn, "Saving NATO: Renunciation of the Article 5 Guarantee," *Orbis* 54, no. 3 (2010): 377.

[123] Ibid., 379.

was unacceptable for NATO to invoke Article 5 in response to Iraq's retaliation.[124] This issue was once again revisited in 2007 following the cyber-attack in Estonia, which likely originated in Russia, and which will be discussed later in this thesis.[125]

[124] Ibid.

[125] Ibid., 280.

IV. CYBER-ATTACKS

A. WHAT IS A CYBER-ATTACK?

There is some acknowledged difficulty in concretely defining what a cyber-attack is, at least in absolute terms. As our society has modernized, it has become more and more connected to the Internet, creating opportunity for enemies and criminals to take advantage of security holes and cause damage to computer systems, steal financial data, or acquire sensitive secrets. As technology becomes cheaper and cheaper to purchase, and access to the Internet expands, the barriers that might have otherwise prevented a terrorist organization or rogue state from gaining access to sensitive computer networks and servers are reduced. Today, anyone with a laptop, high-speed Internet connection, and the relevant knowledge could bring an organization or government to its knees.

When a hostile nation attacks another state by launching a rocket into their territory, it is generally obvious and easy to define who the perpetrator is. In cyber space, it can be a considerable challenge to know who the aggressive actor is. According to the *Tallinn Manual,* a cyber-attack is an offensive or defense cyber operation that is "reasonably" expected to either cause injury or death to people or destruction to objects.[126] While the *Tallinn Manual* is non-binding and does not qualify as international law, it does provide guidance to any state needing it. It is difficult, and perhaps unwise, to concretely define a cyber-attack as technology changes rapidly, and a narrow definition might prove too inflexible to remain useful.

B. MAJOR INTERNATIONAL CYBER-ATTACKS

There have been a handful of major international cyber-attacks, although none have been to the level that would have invoked an Article 5 response if suffered by a NATO country. Many of the attacks were on specific segments of the country. The December 2006 cyber-attack on NASA forced the agency to block and prevent all emails with attachments from being opened out of fear of causing harm to upcoming shuttle

[126] Schmitt, *Tallinn Manual*, 54.

launches.[127] A 2007 cyber-attack on Estonia will be detailed in the following section; another 2007 cyber-attack hit the U.S. Secretary of Defense and the Pentagon.[128] The year 2008 saw a cyber-attack in Georgia, likely perpetrated either by Russia, or a Russian proxy, that left graffiti on many government websites, but did not cause substantial harm.[129] The link to Russia was made as during this cyber-attack, Russia was engaged in military action against Georgia, a former Soviet bloc state. Perhaps one of the most damaging cyber-attacks, known as Stuxnet, employed malware that was released in October 2010 and aimed to harm the Iranian nuclear program.[130] A 2013 cyber-attack on South Korea affected financial institutions and broadcaster YTN, which was reported to be the work of North Korean hackers.[131]

C. NATO AND THE PROBLEM WITH CYBER-ATTACKS

To date, NATO, along with nearly every other nation on this planet, has had great difficulty in dealing with the problem of cyber-attacks. While cyber-attacks are hard to stop for many reasons, the biggest obstacle is the difficulty in tracing a cyber-attack back to the culprit. The Internet offers a realm for cyber-criminals, hacktivists, hackers, and government agencies to operate anonymously. How does an organization, such as NATO deal with a massive cyber-attack on an alliance member if it is unable to prove the identity of the attacker? NATO’s number one role is to protect their member states, with the hope of remaining peaceful, but being unafraid to intervene militarily if need be. It is not the role of NATO to accuse non-alliance members haphazardly of orchestrating a cyber-attack on a member country without proof.

Another problem with cyber-attacks and NATO’s role in dealing with them is to evaluate and determine when a cyber-attack meets the criteria set by NATO to intervene.

[127] “The History of Cyber Attacks—Timeline,” accessed March 20, 2015, http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

[128] Ibid.

[129] Ibid.

[130] Ellen Nakashima and Joby Warrick, “Stuxnet Was Work of U.S. and Israel, Officials Say,” *The Washington Post*,” June 1, 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[131] “The History of Cyber Attacks—Timeline.”

When looking at a cyber-attack, NATO needs to determine whether the attack crosses the threshold into an armed attack, which is extraordinarily difficult. Most small-scale attacks (the kind NATO would not consider for an Article 5 response) are a result of hobbyists experimenting with computer viruses and other malicious code and criminals looking for a way to steal cash. For example, organized crime groups use a variety of techniques to make money, such as "shady advertising schemes, online scams, and other attacks, to make money. Today worldwide criminal businesses are based on cyber-crime."[132] Some of the common attacks use spyware, botnets, spam and phishing, credit card fraud and identity theft, corporate information theft, and denial of service extortion.[133] For obvious reasons, small-scale attacks are not something NATO would necessarily be interested in, while large-scale attacks can be waged by nation-states or non-state actors seeking to cause widespread damage. Several methods can be used for a large-scale attack including DDoS floods exploiting infrastructure components and damaging client systems with widespread botnets. A large-scale attack is an attack with which NATO would be more concerned, and would be more likely to result in an Article 5 response.

When does a cyber-attack deserve an Article 5 response? As with other conflicts of the past, NATO has proven that it can adapt to meet the challenging needs of its alliance members; cyber conflict is no different. After being the victim of several major cyber-attacks in 1999 during Operation Allied Force, NATO formulated its mission for cyber space. Its purpose was to "protect its own networks, enhance the capabilities of the member states, and to cooperate with partner nations, the European Union (EU), and industry."[134] During the 2002 Summit in Prague, NATO adopted the Cyber Defense Program and established the NATO Computer Incident Response Capability (NCIRC) to detect and respond to cyber incidents.[135] Even though NATO adopted the Cyber Defense Program in 2002, the alliance enjoyed a somewhat peaceful cyber world that did not

[132] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, ed. *Cyberpower and National Security* (Washington, DC: Center for Technology and National Security Policy, 2009), 172.

[133] Ibid.

[134] Jason Healey and Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Atlantic Council, August 29, 2014, http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities.

[135] Ibid.

require much action until the 2007 cyber-attacks on Estonia. These DDoS attacks on Estonia were an eye-opener for NATO because they showed how serious cyber-attacks could be technically and politically.

Determining when a cyber-attack is worthy of an Article 5 response is difficult, particularly since there has yet to be an instance when a cyber-attack was severe enough to result in a response. The 2007 cyber-attacks on Estonia targeted critical telecommunications infrastructure and, while there was no loss of life, did cause substantial harm.[136] While it is generally believed that the attacks were due to the removal of a Soviet-era Red Army statue, no party from within Russia claimed responsibility.[137] Even though this attack was not publicized to the same extent that the 9/11 attacks were, there are suspects that could be considered the perpetrator, and harm was done.[138] This cyber-attack occurred before the creation of the *Tallinn Manual*, and in fact, was the event that helped lead to the creation of the manual. There were serious questions raised by NATO's newest, smallest, and most vulnerable member state to the trust and reliability of the security guarantee of the alliance and the willingness of NATO to support the most vulnerable member states in situations, such as cyber-attacks.[139]

Although the attacks were brought under control after several days, NATO officials knew they needed to become more strategic in terms of cyber defense. There was no policy in place to handle such an attack, and it was evident that the time had come to develop a cyber-attack policy as an alliance to prepare for such an event. During the 2008 Bucharest Summit, the NATO Cyber Defense Policy was adopted. The point of the policy was for alliance members to be able to share best practices with one another in terms of cyber defense and come to an alliance member's aid in the event of a cyber-attack. The hope was that another country, if in the same situation as Estonia, would not feel left behind or forgotten by NATO. At the 2008 Summit, two institutions were created with the goal of implementing and supporting the objectives of the Cyber Defense Policy.

[136] Fedyszyn, "Saving NATO: Renunciation of the Article 5 Guarantee," 377.

[137] Ibid.

[138] Ibid.

[139] Ibid., 379.

These new units are known as the Cyber Defense Management Authority (CDMA) and the Cooperative Cyber Defense Center of Excellence (CCDCOE).[140] These new institutions were put under the purview of the Cyber Defense Management Board (CDMB) and became operational in April 2008.[141] Their overarching mission is to initiate and coordinate cyber defenses, review capabilities, and conduct appropriate security risk management that aligns with the need to understand, stop, and prevent cyber-attacks.[142] The CDMA is meant to help each member nation beef up its own cyber defense abilities, but has since been replaced by the CDMB to coordinate cyber defense in both the civilian and military units.[143]

[140] Healey and Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow."

[141] Ibid.

[142] Ibid.

[143] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

V. NATO AND CYBER-ATTACKS

A. IS NATO PREPARED TO RESPOND TO A CYBER-ATTACK?

The response by NATO to address cyber-attacks largely stems from the 2007 Estonia attacks, and while the policy took several years to formulate, it represents significant progress in addressing the challenges highlighted in Estonia.[144] In 2010, the Strategic Concept published by NATO highlighted the importance of developing the ability to prevent, defend against, and detect cyber-attacks.[145] While this failed to include specific and concrete strategies, this was the first major step that NATO took towards recognizing the severity of cyber-attacks and formulating a response in the event of one.[146] In June 2011, NATO adopted its most significant cyber policy to date with the introduction of the Cyber Defense Policy and the Action Plan. The Cyber Defense Policy highlights the new and ever-changing threats to security arising from our dependence on critical, but complex, communications and information systems powered by networks and computers.[147]

A report issued by the Atlantic Council[148] lists the main points of the 2011 Cyber Defense Policy as the following.

- Realization that cyber defense is required to perform NATO’s core tasks of collective defense and crisis management
- Recognition that prevention, resilience, and defense of cyber assets is critical to NATO and its constituent allies
- Implementation of robust cyber defense capabilities and centralized protection of NATO’s own networks
- Definition of minimum requirements for cyber defense of national networks critical to NATO’s core tasks

[144] “Defending Against Cyber-Attacks,” accessed March 15, 2015, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611natocyberattacks_/sede150611natocyberattacks_en.pdf.

[145] “NATO Policy on Cyber Defense, 2011,” accessed on March 15, 2015, http://www.cfr.org/cybersecurity/nato-policy-cyber-defence-2011/p27491.

[146] Ibid.

[147] Ibid.

[148] Healey and Tothova Jordan, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.”

- Assistance to the allies to achieve a minimum level of cyber defense to reduce vulnerabilities of national critical infrastructure
- Engagement with partners, other international organizations, the private sector, and academia

The policy is important in that it gives members a process to use when a cyber-attack occurs, but also keeps the threshold for what delineates an attack vague, thereby allowing NATO to respond to cyber-attacks on a case-by-case basis. To implement this new policy, NATO has to receive the proper authority of all 28-member states by having each state sign a Memorandum of Understanding. This memorandum requires members to report regularly to the North Atlantic Council (NAC) about their progress in regards to cyber threats and cyber security. Alliance members would also be able to have discussions with NATO about the invocation of Articles 4 and 5 of the Washington Treaty if a cyber-attack was significant enough and caused substantial harm.

Considering how NATO has responded to cyber-attacks over the last few years, including the attack on Sony Pictures by North Korea, it is difficult to ascertain if NATO is prepared for a cyber-attack outside of the policies the organization has to rely on for direction in how to respond. While it is understood that a cyber-attack can qualify as an event that could require a NATO response, there has not yet been an event worthy of a response. The damage done in Estonia could have been substantial had Russia, or non-state Russian actors, targeted the transportation infrastructure. Would NATO have responded had there been any harm caused to people or property? While it is nearly impossible to say for certain one way or another, speculation could be made that if people were harmed to the same extent, or similar extent, as those injured in the United States during 9/11, there could have been an Article 5 response.

As for having the appropriate policy in place to respond to a cyber-attack against an enemy, NATO cemented such policy at the Wales Summit in 2014 when all member states agreed to stand with, and come to the aid of, any member state suffering from a major cyber-attack.[149] There are many elements of this acknowledgment of mutual

[149] Robert Lemos, “In Case of Cyber Attack: NATO Members Ready to Pledge Mutual Defense,” Arstechnica, Risk Assessment, accessed March 14, 2015, http://arstechnica.com/security/2014/09/in-case-of-cyberattack-nato-members-ready-to-pledge-mutual-defense/.

defense in the case of a cyber-attack, but the most important is recognition of the importance of cyber defense for the NATO alliance and application of international law to cyberspace.[150] NATO agreed to "intensify" its cooperation with the cyber industry and work to ensure their own systems are secure from cyber-attacks.[151] Furthermore, NATO made clear that they will treat a serious cyber-attack in the same manner in which they would treat a serious kinetic attack, with an attack against one member state treated as if there had been an attack on all member states.[152]

B. UNDER WHAT CONDITIONS WOULD A CYBER-ATTACK TRIGGER AN ARTICLE 5 RESPONSE?

Determining at what point a cyber-attack would trigger an Article 5 response is very complex, and until there is an actual attack worthy of such a reaction, the issue will remain murky.[153] On September 11, 2001, one would have been hard pressed to find individuals who believed that commercial airliners would be used as weapons against the American people, and in a single day be exploited in the murder of nearly 3,000 American civilians. Similarly, while it might be hard to imagine computers being used as weapons against the United States or any other state, NATO member or not, terrorists are actively using electronics to further their cause, making the issue of cyber-attacks as important as any other national security threat, such as terrorism.

To be able to answer this question appropriately, the conditions under which a cyber-attack could invoke an Article 5 response needs to be explored, as well as what NATO currently believes about such attacks. At the previously discussed summit in Wales in the fall of 2014, the alliance acknowledged that if a cyber-attack was sufficiently severe, it could trigger a NATO Article 5 response. However, as with most political and military statements, the alliance was unsurprisingly vague about what the magnitude of a cyber-attack would have to be to do so, adding that such attacks would be reviewed on a case-by-case basis. It is important to note that neither NATO, nor anyone

[150] Lemos, "In Case of Cyber Attack."

[151] Ibid.

[152] Ibid.

[153] Ibid.

else, has yet experienced a truly massive cyber-attack causing the level of damage seen in 9/11. Although the Estonia attacks caused NATO to open its eyes and ramp up its cyber security capabilities, they were not severe enough to invoke an Article 5 response from NATO.

Along with needing to meet the requirements of an Article 5 response, such as serious bodily harm or damage to property, there is the question of attribution. The United Nation addresses the issue of attribution of conduct to a specific state. The international body writes that the conduct of anyone, individual, corporation, or collective, who is linked to the state, whether by nationality, incorporation, or habitual residence, can be attributed to that state, regardless of their connection to the government.[154] Yet, in terms of international law, there is need to show at least some connection, either through direction, instigation, or control, of the conduct in order for the state to be attributed to the action.[155] International law also requires that attribution be based on more than just the recognition of a factual causality, and that it not be decided through implications and assumptions alone.[156] Article 4 of the United Nations charter states "the conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other … organ includes any person or entity, which has that status in accordance with the internal law of the State,"[157]. While this does not proscribe what attribution is within NATO, the United Nations clearly defines attribution, and with member states of NATO also signatories to the United Nations, it is expected that similar values would be held.

Unfortunately, determining attribution does not create a definite understanding of the threshold of attribution needed to invoke Article 5 in the event of a cyber-attack. In the case of Estonia, the cyber-attack was understood to be of Russian origin, although as is typical in cases of cyber-attacks, it is difficult to definitely identify the specific

[154] "Attribution of Conduct to a State," 27, accessed March 15, 2015 http://legal.un.org/legislative series/documents/Book25/Book25_part1_ch2.pdf.

[155] Ibid., 27.

[156] Ibid., 27–28.

[157] Ibid., 31.

aggressor(s). In contrast, the cyber attacks against Sony Pictures were attributed to North Korea. Nevertheless, like the Estonian attacks, they likely did not cause enough damage to actual property or people to qualify for an Article 5 response. However, had the attack not been against Sony, but against a financial institution, such as the New York Stock Exchange or the Federal Reserve, the response might have been stronger. Although the United States publicly charged North Korea with conducting the attack, a broader distribution of the U.S. evidence basis for this conclusion would probably have been required for a collective NATO response. In any event, the hack likely did not meet the other elements necessary for an Article 5 response.

C. HOW WOULD NATO RESPOND TO A CYBER-ATTACK UNDER ARTICLE 5?

To answer this question, it is important to look at the first (and only) time NATO invoked an Article 5 response; namely, following the 9/11 attacks on the United States. When the partners of the alliance first wrote the Washington Treaty, it was initially to deter the Russians from expanding and to deter nuclear warfare at the onset of the Cold War. Article 5 is purposefully vague to give NATO considerable room to maneuver. Before the 9/11 attacks led by Al Qaida, it would have been nearly impossible for anyone, anywhere, including the framers of the Washington Treaty, to imagine such an attack. Likewise, at the 2014 summit in Wales, NATO announced that it would and could invoke an Article 5 response to a cyber-attack, and that the ambiguity would stand.[158] NATO's Ambassador Sorin Ducaru, NATO's assistant secretary general for "emerging security challenges," made the following remarks:

> [T]here's no predetermined threshold…there was a conscious decision by the allies in this policy that there is benefit in keeping flexibility and ambiguity…article 5 was by design something that should be invoked politically by [member] nations in a specific context, on a case by case basis…article 5 was never designed to be triggered by a certain threshold.

[158] Sydney J. Freedberg, "NATO Hews to Strategic Ambiguity on Cyber Deterrence," Breaking Defense, November 7, 2014, http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/.

> The only time it was invoked was after 9/11, which was a scenario that had never been contemplated by the founding partners.[159]

In this same vein, Christopher Painter, the U.S.' State Department cyber coordinator said:

> The NATO leaders' declaration that international law including the UN Charter, the Law of Armed Conflict, international humanitarian law, etc. applies in cyberspace just like it does in the physical world…[t]his is a clear statement that this is not a lawless space. There was some doubt before. There was some thought you had different rules entirely for the cyber world than the physical world, which made no sense and in fact would be very destabilizing.[160]

In light of the recent developments of NATO, it would seem to be in NATO's best interest to remain ambiguous and allow the organization to approach its response to a cyber-attack on a case-by-case basis. For instance, the attacks on Estonia might require intervention on behalf of the Estonian people due to the fact they are a smaller, lesser defensible state. Estonia would not be successful standing up against Russia, and as Russia becomes more aggressive in the former-Soviet bloc region, small states like Estonia are at risk. If another attack were to occur against Estonia, the attacks would have to be more severe to invoke an Article 5 response. Such a response would enable NATO states to act as if they too have been attacked as per the mutual defense announcement against cyber-attacks at the Wales Summit. Yet, if the United States is attacked in a similar manner, there likely does not need to be the same scale of defense taken, because the United States has more resources and capabilities to respond on its own. Remaining ambiguous allows NATO to choose the best opportunities for supporting and defending member states.

Before it could decide on a response, NATO would first need to consider the severity of the attack to determine the appropriate level of response, whether it be sanctions, cutting off financial aid to the offending country, or a boots on the ground campaign. However, even while retaining flexibility in its response to a cyber-attack,

[159] Freedberg, "NATO Hews to Strategic Ambiguity on Cyber Deterrence."

[160] Ibid.

NATO understands the importance of cyber defense. It aims to deter cyber-attacks against its networks and member country's networks through strong cyber defenses, although NATO has yet to fully seek what Cold War theorists have called "deterrence by denial," and which could be an effective mechanism.[161] With such a posture, the enemy need not be convinced that a cyber-attack will be followed by retaliation or punishment; instead, it is only necessary to convince the enemy that the initial attack will have no effect.[162]

D. HOW SHOULD NATO RESPOND TO A CYBER-ATTACK AGAINST A MEMBER COUNTRY?

To attempt to answer this question, this author looks to the recommendations of Jason Healy and Klara Tothova Jordan presented in the brief to the Atlantic Council titled, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow." Healy and Tothova Jordan state that the recommendations they give are generic and can be used by any organization or government in trying to prevent or combat a cyber-attack. Speaking in the abstract, it is possible that, if a cyber-attack were to occur, that NATO could use the following list in helping to either prevent of combat a cyber-attack. The following lists their recommendations.

- Stick to the basics
- Pursue a relevant standard
- Fight through cyber-attacks
- Develop an agenda for private sector collaboration
- Push multinational sharing of baseline capabilities
- Reinforce coordination with the EU
- Consider offensive coordination, not capability
- Focus on Articles 4 and 5
- Be prepared for attribution
- Support beyond RRTs
- Pool and share IT

NATO could utilize each recommendation in the event of a cyber-attack against a member state. The first recommendation, stick to the basics, essentially means focus on

[161] Freedberg, "NATO Hews to Strategic Ambiguity on Cyber Deterrence."

[162] Ibid.

defense.[163] Focusing on defense, which was the original NATO mission against the spread of communism against Europe, includes focusing on coordination and training, two important segments of defense.[164] Focusing on defense also requires a focus on policy, and ensuring that the policy of the organization is in alignment with the goals and purpose. The second recommendation, pursuing a relevant (security) standard, such as ISO/IEC 27001:2013, will help ensure resilience and performance when the state, or NATO, is facing a crisis.[165]

The third recommendation, fighting through cyber-attacks, is an interesting strategy that could be surprisingly useful. It utilizes resiliency plans, specialized incident response teams, and redundant hosting for critical infrastructure sites in an attempt to keep cyber-attacks from becoming NAC issues.[166] By fighting through an attack and not surrendering the network, Healy and Tothova Jordan suggest that militaries should just react and operate, much like they do when there is a fighter jet flying through hostile territory; neither the pilot nor military seeks out NAC permission before flying.[167] The fourth recommendation, developing an agenda for private sector collaboration, is perhaps the easiest and most efficient recommendation made because many organizations already have the capability to fight, and win, against a cyber-attack. Private organizations might work with governments and firms from other states, providing that organization a substantial amount of information and knowledge that could be utilized in a positive and purposeful manner by NATO.[168]

In a similar vein, the fifth recommendation, pushing multinational sharing of baseline capabilities, is another strategy that NATO could embrace for bettering preparing and preventing cyber-attacks, both against the organization and member states. Instead of NATO seeking out an entirely different and separate IT unit for each member

[163] Healey and Tohova Jordan, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.”

[164] Ibid.

[165] Ibid.

[166] Ibid.

[167] Ibid.

[168] Ibid.

state, NATO members can collaborate, as they likely use identical systems and switches.[169] Sharing access, and thus information, could result in better performance and better outcomes in times of crisis, which is the purpose of the organization.[170] The sixth recommendation, reinforcing coordination with the EU, would help to overcome issues, particularly regarding infrastructure, and the EU and NATO should collaborate and work together during crises, as well as during peacetime.[171]

The seventh recommendation, consider offensive coordination, not capability, allows units from different countries to work together, but without necessarily sharing information, which might be top secret or proprietary.[172] This would allow for better communication of objectives, without risking national secrets. Having the ability to coordinate is important during a crises and having the skill-sets that such coordination would provide would be invaluable. Focusing on Articles 4 and 5, the eighth recommendation recognizes that cyber conflict is likely to take place during an existing geopolitical crisis with a known national adversary, making it possible to prepare in advance for such situations[173]

The ninth recommendation, be prepared for attribution, similarly recognizes the geopolitical context surrounding cyber-attacks. In such clearly defined situations, it would not require substantial investigation to determine the aggressor nation, making the invocation of Articles 4 and 5 much easier and clearer.[174] The tenth recommendation, providing support beyond Rapid Reaction Teams, could allow for a much wider range of actions that could be utilized after invoking Article 5.[175] This could be something as simple as providing satellite telephones and access to satellite data or more complicated like intelligence sharing and coordinating civilian telecommunication organizations

[169] Healey and Tohova Jordan, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.”

[170] Ibid.

[171] Ibid.

[172] Ibid.

[173] Ibid.

[174] Ibid.

[175] Ibid.

during a cyber-attack.[176] Finally, the eleventh recommendation, pooling and sharing of IT resources, could cut costs and provide collaboration and coordination, which would better provide defenses. Healey and Tothova Jordan use the example of Belgium and the Netherlands, and the benefits both would have if they shared procurements of cloud computing, server storage, and military structures if they operated together as a single entity instead of two separate and distinct entities.[177]

Healy and Tothova Jordan discuss the importance of defense as being one of the most effective ways NATO should respond to cyber-attacks. They also noted the benefits of deterrence and that deterrence by punishment might be achieved in several ways.

- Any nation choosing another major attack even on a small ally, such as Estonia, now knows a very well understood path for NATO's political leadership is available to escalate the situation to an Article 4 consultation or Article 5 invocation of collective defense.
- Both the White House and Pentagon have been extremely clear that Alliance commitments extend to major cyber-attacks.
- Although NATO does not have an offensive cyber capability, several member nations do have those capabilities that could be used in response.[178]

[176] Healey and Tohova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow."

[177] Ibid.

[178] Ibid.

VI. CONCLUSION

A. RECOMMENDATIONS

This thesis recommends that NATO take the following actions:

- Establish. As part of its cyber defense program, NATO should establish an early warning system that lets the alliance and its members know when an attack is happening within enough time to stop it.
- Focus. NATO's deterrence strategy should focus more on denial.
- Encourage. NATO and its allies should encourage information sharing among its member nations and within the alliance itself.
- Share. NATO and its allies should encourage information sharing within and among its member nations.
- Maintain ambiguity. NATO should on what justifies an Article 5 response in order to ensure that NATO can act when justified.

Looking at the first recommendation, as part of its cyber defense program, NATO needs to have an early warning system that lets the alliance and its members know when an attack is happening within enough time to stop it. Establishing such a system is crucial for NATO and its allies. Above all else, it is truly the most important recommendation. By defending its own networks and alliance countries doing the same, the need for an Article 5 response would be unnecessary. An article 5 response, of course, is a last resort when all else has failed.

In their essay to NATO in the *Atlantic Council*: *Issue Brief*, Jason Healey and Leendert van Bochoven explain why an early warning system is so important. They explain that NATO needs "intelligence-based indications and warning, to give advance notice of geopolitical situations that might lead to serious cyber conflict."[179] To achieve this, NATO needs to phase in a system as opposed to looking for a perfect solution to cyber security. Healey and von Bochoven suggest a phased adaptive approach for cyber defense and believe that NATO is on the right track with its monitoring system, which is

[179] Jason Healey and Leendert van Bochoven, "Strategic Cyber Early Warning: Phased Adapting Approach for NATO," Atlantic Council, Smarter Alliance Initiative, November 6, 2012, http://www.atlanticcouncil.org/publications/issue-briefs/strategic-cyber-early-warning-a-phased-adaptive-approach-for-nato.

a decent first step.[180] As part of the phased adaptive approach, "later phases could consider a more sophisticated sensor grid integrated with militaries and national grids, once there is sufficient budget and trust in the Alliance."[181] It would make it possible for political leaders to act in the case of a cyber-attack serious enough to invoke an Article 4 or 5 responses. Likewise, it would allow leaders to determine if a cyber-attack is simply a nuisance that does not require any action.

The second recommendation is that NATO's deterrence strategy should focus more on denial. Deterrence by denial essentially means that it would be pointless for one country to launch a cyber-attack against another country because the attack would be futile. Essentially, deterrence by denial frustrates the attacker, leading to an abandonment of the attack.[182] Typically, deterrence is established through punishment, with the threat of retaliation by the victim, or the victim's allies, being sufficient to prevent such an attack.[183] But the threat of punishment is often not enough, especially in situations where attribution is difficult to establish, making deterrence by denial an attractive alternative.[184] Whereas Article 5 gives NATO some means of deterrence by punishment, strengthening its cyber defense capabilities would enable NATO to also draw upon deterrence by denial.[185] In addition to deterrence by denial and punishment, deterrence theory covers such measures as making declarations, establishing credibility and assurance, creating fear, and making cost-benefit calculations.[186] Employing multiple measures together can help to prevent engagement.

The third recommendation, that NATO and its allies encourage information sharing among its member nations and within, suggests it would be beneficial to NATO

[180] Healey and van Bochoven, "Strategic Cyber Early Warning."

[181] Ibid., 1.

[182] Martin Libicki, "Cyberdeterrence and Cyberwar," Rand Corporation, 2009, 7–8, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[183] Ibid.

[184] Ibid.

[185] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* Fall 2010, 105, accessed March 15, 2015, http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf.

[186] Ibid.

and the members of the alliance to share information between agencies. Hannes Krause addresses this topic in his article, “NATO on Its Way towards a Comfort Zone in Cyber Defence,” which is one part in a series of papers known collectively as *The Tallinn Papers*. Krause emphasizes that for NATO truly to be successful in cyber defense, transparency is key.[187] Information sharing would be a great starting point for further political discussions surrounding cyber defense, and the discussions should include “information related to situational awareness, national developments and existing capabilities.”[188] This would be a vast improvement over the current system where information is shared on a need to know basis, and is one of the key recommendations made by Heeley and Tothova Jordan.[189]

The fourth recommendation states that NATO needs to hire or train a team of experts in hacking, computer forensics, and cyber defense to aid its own organization and come to the aid of member countries that have experienced a breach in their security networks. Following the Wales Summit and the declaration that a cyber-attack could be treated like a kinetic one, it might become easier for policy to be drafted that will encourage the sharing of information. Heeley and Tothova Jordan stress this as an important recommendation that NATO could embrace because they could bring in experts from each nation to share information and collaborate to create a better, more efficient, and superior system. This expertise would be needed if NATO’s or a member country’s defense systems have been seriously breached. They can be on call in the meantime until NATO and its member countries adopt a more sophisticated defense system as suggested by Healey and von Bochoven.[190]

Finally, NATO needs to maintain ambiguity on what justifies an Article 5 response. As mentioned previously, ambiguity has served NATO well. A set threshold for when NATO will invoke an Article 5 response to a cyber-attack on a member country

[187] Hannes Krause, “NATO on Its Way towards a Comfort Zone in Cyber Defence,” *The Tallinn Papers*, 11, no. 3 (2014), https://ccdcoe.org/publications/TP_Vol1No3_Krause.pdf.

[188] Ibid.

[189] Healey and Tothova Jordan, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.”

[190] Healey and van Bochoven, “Strategic Cyber Early Warning: Phased Adapting Approach for NATO.”

is not necessary. This ambiguity has historically served the alliance well, as demonstrated by the 9/11 attacks. If the alliance had said weapons were *only* include guns, bullets, tanks, and bombs, it would have set a threshold precluding a NATO response to attacks that turned four planes into improvised missiles. The larger issue of ambiguity is that there is no set definition of what constitutes an armed attack and what circumstances dictate a collective response, as per Article 5. Remaining ambiguous on the severity threshold of a cyber-attack allows the alliance to act in cases of future cyber-attacks that cause severe damage, but also allow NATO to refrain from over-reacting, even if an event is a cyber, or kinetic, attack as per a definition. It would be a mistake to set a threshold for attacks that cannot currently be anticipated.

When NATO was originally formed, it was with the purpose to be unambiguous, with the promise of "massive retaliation" by Eisenhower. This was meant to constantly act as a reminder to the Soviet Union and the Red Army that if they were to surge into Western Europe, in no uncertain terms NATO would respond with nuclear weapons. Ambiguity is useful in times, and at other times, it is not. Had NATO been ambiguous in dealing with the Soviet Union, there could have been opportunity for the Red Army to advance further across Europe, to test and see what NATO, and the United States, would allow them to get away with, without an attack. Ambiguity can also cause problems, particularly in the event of a cyber-attack with some members feeling an attack might warrant retaliation through Article 5, with others feeling that the necessary thresholds have not been met. It is important for NATO to have a clear understanding, or general belief, of what would constitute a serious enough cyber-attack in order to respond, but not through official policy or rules to ensure proper consideration.

B. CONCLUSION

This thesis has reviewed the history of NATO and its role in the world, and has found that since its creation post-WWII, the NATO alliance has been able to adapt to changing times. It remains an organization that promotes peace but will use force if necessary. NATO has taken on the new challenge of cyber-attacks that the current world faces today. It has also taken steps to prevent cyber-attacks on itself and member countries, as well as to make it clear to any person, nation, or organization that an Article 5 response will be invoked in the case of a serious cyber-attack that can be deemed an armed attack according to scale, effects, and attacker motivation.

Article 5 is the most important article in the Washington Treaty, on which the entire alliance is hinged. As in the 9/11 attacks on the United States by a foreign enemy, NATO showed it was a force to be reckoned with when it invoked Article 5 for the first time in its history. It came to the aid of the United States and sent a loud resounding message to the world that terrorism would not be tolerated.

Since the cyber world is still so new and continues to advance each day with new technologies, NATO is still trying to find the best policies and best course of action to take in response to the new threats to peace and democracy that cyber-attacks pose on the alliance and this new world. NATO welcomes and many experts on cyberspace give it recommendations on how to deal with this new threat. The cyber world is too new for NATO to bind its hands, so to speak, with rigid rules and laws regarding when, how, and why it would invoke Article 5 in the case of a cyber-attack on a member country. In response, at the 2014 summit in Wales, the alliance made it clear that a cyber-attack can and will invoke an Article 5 response. It also made it clear that ambiguity has served the alliance well, and it refused to define the kind of attack that would invoke an Article 5 response.

However, that is not to say that NATO has been irresponsible or lackadaisical in trying to give some understanding on when a cyber-attack becomes an armed attack. With the help of experts in the field of cyberspace, international law, and policymakers, the *Tallinn Manual* was written and published to provide guidance to NATO and any other international or national alliance or government seeking it. Although the Manual offers guidance on what scale, effects, and attacker motivation would be severe enough to fall into the category of an armed attack, it does not give specific details, only a conceptual idea of what an armed attack might look like in the cyber realm. Then, with the guidance of the Manual, and international law, there could be a better understanding of what would then invoke an Article 5 response. Nevertheless, it is not, and was not intended to be, a complete go-to-guide for how each member country should conduct itself in the cyber world.

As this thesis was written, many more cyber-attacks have targeted government agencies, unsuspecting consumers, and companies that have cost victims billions of dollars worldwide. That situation, in itself, is a serious issue. As briefly mentioned earlier in the thesis, the hacking of Sony by North Korea is a perfect example of the varying degrees of cyber-attack and the varying level of harm it can cause. The American government claims North Korea is responsible for the hacking in response to the previously discussed film released by Sony Pictures. While a mysterious group called "Guardians of Peace" claimed responsibility for the attacks, the United States government is confident that the true perpetrator is the North Korean government. This situation has parallels to the 2007 cyber-attacks on Estonia. We do know that many persons of Russian ethnicity participated, not only in cyber-attacks, but also in street protests. But attribution to the Russian government was harder, and Russia was able to evade responsibility by simply denying even indirect involvement.

The Estonia attack fortunately did not result in substantial damage to the country, and the cyber infrastructure was able to be returned to its stable condition. In contrast, the film company lost some of the millions of dollars it had invested in the film because of the initial decision to cancel its scheduled release. This author believes that the Sony attack was much more serious, at least in terms of financial losses, than the Estonian attack due to the damage done to a major international organization. Sony's reputation was tarnished by the private, embarrassing, and proprietary information stolen by the attacks and then disclosed to the public. More importantly, though, the Sony hack demonstrated that cyber-attacks can effectively muzzle freedoms of speech and artistic expression if the government does not effectively respond. The United States did not seek an Article 5 declaration against North Korea, mainly because it did not have to; U.S. responses were sufficient to induce Sony to release the film after all and to result in no subsequent adverse North Korean actions of any significance. Nevertheless, the incident showed that cyber-attacks can threaten vital information flows by intimidating people, as well as compromising networks.

As part of this conclusion, and based on the research done by this author, it is important to look at areas of understanding and unresolved issues of the current research. Points made in the earlier summary are reiterated as follows.

C. AREAS OF AGREEMENT AND UNDERSTANDING

- Experts do not have consensus when it comes to defining the severity of a cyber-attack. While the *Tallinn Manual* offers a good first step in understanding if the threshold has been met, there still needs to be application of it in the real world for a consensus to be built. But, it can be agreed upon that a cyber-riot, as in the Estonian case, should not be confused with a cyber-attack that could kill or injure large populations of people or cause extreme damage to property or financial markets.
- Ambiguity has served NATO well. Although setting a precise threshold for when a cyber-attack rises to the level of an armed kinetic attack might make it easier for NATO to invoke Article 5, choosing to remain ambiguous gives the alliance more flexibility in responding to cyber-attacks. Moreover, it would be difficult for NATO to set a threshold for an attack it has never seen before, which was the case on September 11, 2001.
- Experts on the topic of cyber-attacks agree that the rules that apply in the kinetic world should apply to the cyber realm. Therefore, invoking an Article 5 response in the case of a cyber-attack on a member country is an acceptable outcome.

D. UNRESOLVED ISSUES

Very little research has been done to address what is to be done when it is not known with perfect certainty who committed a cyber-attack. In the Estonian case, Russia was suspected of being involved, but it was difficult to prove. While Russia was also suspected of committing cyber-attacks on Georgia in 2008, once again, attribution was difficult to prove and Russia did not suffer any consequences.

NATO, and the rest of the world, has not yet seen the true extent of damage that could be done if there were to be a violent and deadly cyber war. Now, experts on the topic of cyber-attacks can only speculate about what a severe cyber-attack would look like. Stuxnet might be the closest example of a real world cyber-attack. As individuals and nations disrupt the cyber world with cyber-attacks, causing damage to the real world, NATO needs to continue to adapt to meet the needs of its alliance members in the cyber world, while sending a resounding message to the world that cyber-attacks on member nations will not be tolerated.

LIST OF REFERENCES

Arend, Anthony Clark. “International Law and the Preemptive Use of Military Force.” *The Washington Quarterly* 26, no. 2 (2003): 89–103.

Buckley, Edgar. “Invoking Article 5.” *NATO Review*. Summer 2006. Accessed March 20, 2015. http://www.nato.int/docu/review/2006/issue2/english/art2.html.

Caton, Jeffrey L. *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications*. Carlisle Barracks, PA: The United States Army War College, Strategic Studies Institute, 2014.

Clarke, Richard A., and Knake, Robert K. *Cyber War the Next Threat to National Security and What to Do about It*. New York: Ecco, 2012.

Cody, Edward. “After 43 Year, France to Rejoin NATO as Full Member.” *Washington Post*. March 12, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/03/11/AR2009031100547.html.

Council on Foreign Relations. “NATO Policy on Cyber Defense, 2011.” Accessed March 15, 2015. http://www.cfr.org/cybersecurity/nato-policy-cyber-defence-2011/p27491.

Department of State. “Milestones: 1945–1952; North Atlantic Treaty Organization (NATO), 1949.” United States Department of State Office of the Historian. March 12, 2015. https://history.state.gov/milestones/1945-1952/nato.

———. “Milestones: 1993–2000; North Atlantic Treaty Organization (NATO), 1949.” United States Department of State Office of the Historian. March 12, 2015. https://history.state.gov/milestones/1993-2000/evolution-of-nato

Dunlap, Charles J. Jr. “Perspectives for Cyber Strategists on Law for Cyberwar.” *Strategic Studies Quarterly Spring 2011* (2011). http://www.au.af.mil/au/ssq/2011/spring/dunlap.pdf.

Economist, The. “War in the Fifth Domain.” July 3, 2010. http://www.economist.com/node/16478792.

Europa. “Defending Against Cyber-Attacks.” European Parliament. Accessed March 15, 2015. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611natocyberattacks_/sede150611natocyberattacks_en.pdf.

Fedyszyn, Thomas. “Saving NATO: Renunciation of the Article 5 Guarantee.” *Orbis* 54, no. 3 (2010): 374–386.

Freedberg, Sydney J. “NATO Hews to Strategic Ambiguity on Cyber Deterrence.” *Breaking Defense*. November 7, 2014. http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/.

Garthoff, Raymond L. *Détente and Confrontation: American-Soviet Relations from Nixon to Reagan*. Washington, DC: Brookings Institute Press. 1994.

Goodman, Will. “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly,* Fall 2010. http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf.

Hallams, Ellen. “The Transatlantic Alliance Renewed: The United States and NATO since 9/11.” *Journal of Transatlantic Studies (Routledge)*, 7, no. 1 (Spring 2009): 38–60.

Hardy, Keiran. “WWWMDs: Cyber-attacks Against Infrastructure in Domestic Anti-Terror Laws.” *Computer Law & Security Review* 27, no. 2 (April 2011): 152–161. http://dx.doi.org/10.1016/j.clsr.2011.01.008.

Hathaway, Oona, A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. “The Law of Cyber-Attack.” *Yale Law Review 100* (2012). http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers.

Healey, Jason, and Klara Tothova Jordan. “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow.” Atlantic Council. August 29, 2014. http://www.atlanticcouncil.org/publications/issue-briefs/natos-cyber-capabilities.

Healey, Jason, and Leendert van Bochoven. “Strategic Cyber Early Warning: Phased Adapting Approach for NATO.” Atlantic Council, Smarter Alliance Initiative. November 6, 2012. http://www.atlanticcouncil.org/publications/issue-briefs/strategic-cyber-early-warning-a-phased-adaptive-approach-for-nato.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2 (2011): 49–60. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.

International Court of Justice. “Legality of the Threat or Use of Nuclear Weapons.” July 8, 1996. http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95.

———. “Military and Paramilitary Activities In and Against Nicaragua.” June 1986. http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5.

Isby, David, C., and Charles Kamps, Jr. *Armies of NATO’s Central Front*. New York City, NY: Jane’s Information Group, 1985.

Kenyon, Henry S. “Cyber Attacks Reveal Lessons.” *Signal* 63, no. 11 (2009). http://www.afcea.org/content/?q=cyber-attacks-reveal-lessons.

Kilian, Crawford. “Mark Twain, Father of the Internet.” The Tyee. January 8, 2007. http://thetyee.ca/Books/2007/01/08/MarkTwain/.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. ed. *Cyberpower and National Security*. Washington, DC: Center for Technology and National Security Policy, 2009.

Krause, Hannes. “Invocation in Context.” *NATO Review*. 2006. http://www.nato.intdocu/review/2006/issue2/english/summaries.html.

———. “NATO on Its Way towards a Comfort Zone in Cyber Defence.” *The Tallinn Papers*, 2014. https://ccdcoe.org/publications/TP_Vol1No3_Krause.pdf.

Laughland, Oliver. “FBI Director Stands by Claim that North Korea Was Source of Sony Cyber-Attack.” *The Guardian*. January 7, 2015. http://www.theguardian.com/world/2015/jan/07/fbi-director-north-korea-source-sony-cyber-attack-james-comey.

Lemos, Robert. “In Case of Cyber Attack: NATO Members Ready to Pledge Mutual Defense.” Arstechnica, Risk Assessment. Accessed March 14, 2015. http://arstechnica.com/security/2014/09/in-case-of-cyberattack-nato-members-ready-to-pledge-mutual-defense/.

Libicki, Martin. “Cyberdeterrence and Cyberwar.” Rand Corporation. 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Morbin, Tony. “NATO: Defending Against the Known Unknowns.” *SCMagazine UK*, 2015. http://www.scmagazineuk.com/nato-defending-agains-the-known-unknowns/article/400190/.

Nakashima, Ellen, and Joby Warrick. “Stuxnet Was Work of U.S. and Israel, Officials Say.” *The Washington Post*.” June 1, 2012. http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

National Defense University. *Allied Command Structures in the New NATO*. Collingdale, PA: Diane Publishing, 1997.

NATO. “Bucharest Summit Declaration.” Last modified May 8, 2014. http://www.nato.int/cps/en/natolive/official_texts_8443.htm.

———. “Collective Defense.” Accessed March 14, 2015. http://www.nato.int/cps/en/natohq/topics_110496.htm.

———. “North Atlantic Treaty.” Accessed March 13, 2014. http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

———. “The History of Cyber Attacks—Timeline.” *NATO Review*. Accessed March 20, 2015. http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.

NATO Cooperative Cyber Defense Centre of Excellence. “International Cyber Developments Review (INCYDER).” January 1, 2014. https://www.ccdcoe.org/sites/default/files/publications/articles/INCYDER 2014Q2.pdf.

Reynolds, David. *The Origins of the Cold War in Europe: International Perspectives.* New Haven, CT: Yale University Press, 1994.

Robertson, George. “Being NATO’s Secretary General on 9/11.” *NATO Review Magazine*. Accessed March 14, 2015. http://www.nato.int/docu/Review/2011/11-september/Lord_Robertson/EN/index.htm.

Schmitt, Michael N. “International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.” *Harvard International Law Journal Online* 54 (December 2012).

———. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013.

United Nations. “Attribution of Conduct to a State.” United Nations Legislative Series. Accessed March 15, 2015. http://legal.un.org/legislativeseries/documents/Book 25/Book25_part1_ch2.pdf.

———. “Charter of the United Nations.” Chapter VII. 1945. http://www.un.org/en/documents/charter/chapter7.shtml.

Wolff, Josephine. “NATO’s Empty Cybersecurity Gesture.” *Slate Magazine*, September 10, 2014. http://www.slate.com/articles/technology/future_tense/2014/09/nato_s_statement_on_cyberattacks_misses_some_fundamental_points.html.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California