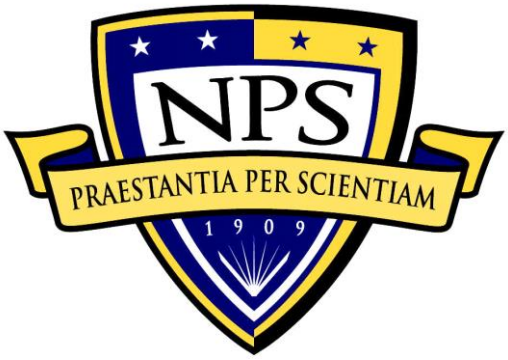

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IS NATO READY FOR A CYBERWAR?

by

Mustafa Canbolat
Emrah Sezgin

December 2016

Thesis Advisor: Bryan J. Hudgens
Second Reader: Dorothy E. Denning

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE IS NATO READY FOR A CYBERWAR?			**5. FUNDING NUMBERS**
6. AUTHOR(S) Mustafa Canbolat and Emrah Sezgin			
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**

13. ABSTRACT (maximum 200 words)

This thesis analyzes the sufficiency and effectiveness of the North Atlantic Treaty Organization's (NATO) cyber policies against cyber threats, considering the recent cyber cases and incidents that could be related to NATO's cyber defense. The authors use analytical and descriptive approaches to answer the research questions by examining the categories of cyber threats facing NATO and the policies implemented to fight against cyber operations and attacks. Finally, the authors make policy recommendations in order to respond to cyber threats more effectively in regard to eight specific areas: cooperation with the European Union; relations with business enterprises; information sharing among members; education, training, and exercises; capabilities of NATO Communications and Information Agency (NCIA); critical infrastructure protection; cyber law and legislature; and collective cyber defense.

The cyber domain is a challenging arena in which to carry out operations and develop policies. NATO can be considered successful in cyberspace; however, the alliance should be aware that there is no limit to the development of capabilities, especially in cyber defense issues.

14. SUBJECT TERMS NATO, cyberwar, cyber policy, cyber threats, cyber cases, cyber law			**15. NUMBER OF PAGES** 117
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

IS NATO READY FOR A CYBERWAR?

Mustafa Canbolat
1st Lieutenant, Turkish Army
B.S., Turkish Military Academy, 2008

Emrah Sezgin
1st Lieutenant, Turkish Air Force
B.S., Turkish Air Force Academy, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
December 2016

Approved by: Bryan J. Hudgens
Thesis Advisor

Dorothy E. Denning
Second Reader

Glenn R. Cook
Academic Associate
Graduate School of Operational and Information Sciences

James Hitt
Academic Associate
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzes the sufficiency and effectiveness of the North Atlantic Treaty Organization's (NATO) cyber policies against cyber threats, considering the recent cyber cases and incidents that could be related to NATO's cyber defense. The authors use analytical and descriptive approaches to answer the research questions by examining the categories of cyber threats facing NATO and the policies implemented to fight against cyber operations and attacks. Finally, the authors make policy recommendations in order to respond to cyber threats more effectively in regard to eight specific areas: cooperation with the European Union; relations with business enterprises; information sharing among members; education, training, and exercises; capabilities of NATO Communications and Information Agency (NCIA); critical infrastructure protection; cyber law and legislature; and collective cyber defense.

The cyber domain is a challenging arena in which to carry out operations and develop policies. NATO can be considered successful in cyberspace; however, the alliance should be aware that there is no limit to the development of capabilities, especially in cyber defense issues.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. BACKGROUND 1
B. PURPOSE AND SCOPE 3
C. RESEARCH QUESTIONS 3
D. METHODOLOGY 3
E. OVERVIEW 4

II. LITERATURE REVIEW 7
A. EARLY WARNING FOR CYBERWAR 7
B. DEFINING KEY CYBER TERMS 8
C. CYBER ISSUES BECOMING MORE SERIOUS 10
D. CYBERWAR IS REAL 12
E. LEGAL CONSIDERATIONS 12
F. TALLINN MANUAL 14
G. CYBER POWER AND NUCLEAR LESSONS 16
H. CYBERWAR AND NATO 17
I. SUMMARY 20

III. THE CYBER THREATS AGAINST NATO 21
A. CYBER THREATS 21
1. Introduction 21
2. Categories of Cyber Threats 22
B. CYBER ACTORS 25
1. State Actors 26
2. Non-state Actors 28
3. Most Active and Dangerous Cyber Actors 31
C. CYBER INCIDENTS AND CASES 31
1. Serbian-NATO Conflict (1999) 32
2. Estonia (2007) 34
3. Georgia (2008) 37
4. Stuxnet (2010) 40
5. Ukraine (2014) 41
6. Other Cyber Incidents 43
D. SUMMARY 45

IV. NATO POLICIES TO FIGHT AGAINST CYBER THREATS 47
A. EVOLUTION 47

1. Prague Summit (2002) 48
2. Riga Summit (2006) 48
3. Bucharest Summit (2008) 49
4. Strasburg-Kehl Summit (2009) 50
5. Lisbon Summit (2010) 51
6. Chicago Summit (2012) 53
7. Wales Summit (2014) 55
8. Warsaw Summit (2016) 57
B. GOVERNANCE 58
1. Cyber Defense Policy Updates 59
2. Hierarchical Responsibilities in Governance 60
C. SUMMARY 62

V. POLICY RECOMMENDATIONS TO RESPOND CYBER THREATS 65
A. CYBER DEFENSE PLEDGE 66
B. EVALUATION AND RECOMMENDATIONS FOR SPECIFIC AREAS 67
1. Cooperation with the European Union (EU) 68
2. Relations with Business Enterprises 70
3. Information Sharing Among Members 73
4. Education, Training, and Exercises 76
5. Capabilities of NCIA 79
6. Critical Infrastructure Protection 81
7. Cyber Law and Legislature 84
8. Collective Cyber Defense (Article 5) 86
C. SUMMARY 88

VI. CONCLUSION 91
A. SUMMARY OF RECOMMENDATIONS 91
B. CONSIDERATIONS 94
C. SUGGESTIONS FOR FUTURE RESEARCH 95

LIST OF REFERENCES 97

INITIAL DISTRIBUTION LIST 103

LIST OF ACRONYMS AND ABBREVIATIONS

AFCEA	Armed Forces Communication and Electronics Association
APT	Advanced Persistent Threat
C3	Consultation, Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCDCOE	Cooperative Cyber Defense Center of Excellence
CDMA	Cyber Defense Management Authority
CDMB	Cyber Defense Management Board
CERT-EU	Computer Emergency Response Team of the European Union
CIP	Critical Infrastructure Protection
CIS	Communications and Information Systems
DDoS	Distributed Denial of Service (Attack)
DNS	Domain Name Service
DoS	Denial of Service
EU	European Union
FOC	Full Operational Capability
MISP	Malware Information Sharing Platform
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NICP	NATO Industry Cyber Partnership
OSCE	Organization for Security and Cooperation in Europe
UN	United Nations
UNSC	United Nations Security Council

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express our great appreciation and gratitude to our country and the Turkish Armed Forces for providing us the opportunity to study at the Naval Postgraduate School. We would like to address our special thanks to our advisors, Professor Bryan J. Hudgens and Dr. Dorothy E. Denning, for their contributions, patience, support, and guidance. We also would like to express our appreciation to our instructors, fellow students, and school personnel during this pleasant journey. To our families, please know that without your love and support, nothing could be possible. We thank you very much.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Information supremacy has been one of the most significant advantages on the battlefield. As Sun Tzu stated in his book *The Art of War,*

> if you know the enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. (Thamm, 2010, p. 3)

John Arquilla and David Ronfeldt (1993) portray the triumphs of Mongols from the perspective of information dominance. Although Mongols were almost always disadvantaged in their numbers compared to their adversaries, they conquered and ruled one of the biggest empires in the world for more than a century. The key reason why Mongols were successful in the 13th century was their information dominance in the battlefield. Mongolian arrow riders prevented the opponent's commanders from communicating effectively with their warriors in the field. Also, Mongolian messengers used to take three to four more horses with them during travel so as to not be bound by the horses' physical limits and so that they could deliver information quickly. Much like the real-time intelligence obtained from satellites today, the information gathered about the enemy's tactics, intentions, and situation provided the Mongolian forces an enormous advantage.

The Mongol example teaches us the importance of information dominance for an effective defense. When we look at the world today, we see the cyber realm as one of the most conflicted arenas for information dominance. The Mongol example teaches another lesson when it is examined from the perspective of cyber warfare. Cyberwar depends on strategic interaction, that is, by how one sees and manipulates the conflict rather than on merely having high technological capabilities (Arquilla & Ronfeldt, 1993).

New technologies and inventions change people's lives and the world we live in. Among the most transformative inventions of the last century were the Internet and information technologies. These developments have had far-reaching effects not only on the social lives of individuals, but also on the defense concerns of nation states. While the Internet has made the world a smaller place by providing unprecedented opportunities and capabilities to connect with other people, it also has made the world more dangerous because of the attendant security issues. Information technology can be used by individuals with malicious intentions to commit cybercrimes, cyber espionage, cyberterrorism, or cyber warfare. Even a small number of people can execute these wide-ranging and devastating activities, which creates asymmetry in the force equations. Therefore, the introduction of the cyber domain has changed how states defend themselves forever.

Like nation states, the North Atlantic Treaty Organization (NATO) needs to build a strong cyber defense to deter and fight against cyber threats. However, implementing successful policies and having effective cyber defense forces is not an easy task. Keeping up with every new development in the cyber realm, renewing policies, and improving forces take serious efforts. This gets more complicated when addressing the varying opinions and concerns from member countries; however, it does not change the fact that the alliance still needs to provide collective defense in the cyber domain.

NATO's cyber policy has a significant role in its collective defense. The cyber domain has created unprecedented threats and vulnerabilities to NATO. To sustain its collective defense objectives, NATO needs to be ready and capable of coping with potential cyber-attacks. The policies and strategies that define NATO's cyber response plan will determine how well prepared NATO is to address cyber threats.

B. PURPOSE AND SCOPE

The purpose of this thesis is to analyze the sufficiency and effectiveness of NATO's cyber policies against cyber threats, considering the cyber incidents that NATO encountered in past years. This thesis focuses on the cyber policies NATO has developed so far and determines whether these policies are sufficient to overcome cyber threats. It presents the advantages and disadvantages of NATO's cyber policies and strategy toward cyber-attacks.

The scope of this thesis includes a detailed literature review, categorization of cyber threats from the perspective of NATO, examination of cyber-attacks and incidents from which NATO could take lessons for its cyber defense strategy, and an overview of NATO's cyber policy evolution. It also provides recommendations for and evaluation of these policies.

C. RESEARCH QUESTIONS

This thesis answers the following questions:

1. How sufficient are the current NATO policies to respond to cyber threats against NATO?
2. What are the cyber threats facing NATO?
3. What policies has NATO implemented to fight against cyber operations and cyber-attacks so far?
4. What policy recommendations can be made to respond to cyber threats more effectively?

D. METHODOLOGY

Analytical and descriptive approaches are used in this thesis to answer the aforementioned research questions. This thesis starts with a review of the prevalent literature about key issues relating to cyberwar and NATO. Several primary and secondary resources are examined in order to get a comprehensive picture of the cyberwar and what NATO has done to bolster its cyber defenses. This thesis also explores different typologies of cyber threats and actors, and it offers case analyses that would concern NATO and its member countries. For

NATO's cyber policy development, this thesis primarily relies on the unclassified information from official NATO publications, statements, and declarations, and on experts' research and opinions about these policies. This thesis aims to evaluate the effectiveness and sufficiency of NATO's cyber policies by considering cyber threats in the context of NATO's cyber capacity and its organizational structure.

E. OVERVIEW

The remainder of this thesis is organized into five chapters. Chapter II is a detailed literature review that describes a variety of topics to familiarize the reader with the important concepts and issues. The literature review includes the assessment of key cyber terms, early warning for cyberwar; traces how cyber issues have grown more serious over time and examines related legal considerations; reviews the *Tallinn Manual*, cyber power, and nuclear lessons; and discusses NATO's position on cyber issues.

Chapter III explores the categories of cyber threats, cyber actors as state actors, non-state actors, and the most active and dangerous cyber actors. After setting this foundation, the chapter includes a discussion of major cyber incidents, such as the Serbian-NATO conflict (1999), and cases involving Estonia (2007), Georgia (2008), Stuxnet (2010), and Ukraine (2014), to portray what future cyber-attacks against NATO could look like.

By looking at the alliance's evolution and governance in this field, Chapter IV describes NATO policies to fight against cyber threats. Policy evolution in the cyber realm covers decisions and declarations from the Prague Summit (2002), the Riga Summit (2006), the Bucharest Summit (2008), the Strasburg-Kehl Summit (2009), the Lisbon Summit (2010), the Chicago Summit (2012), the Wales Summit (2014), and the Warsaw Summit (2016) related to NATO's cyber defense. The governance section deals with cyber defense policy updates and hierarchical responsibilities in governance.

Chapter V discusses policy recommendations to respond to cyber threats effectively. It provides details of the Cyber Defense Pledge made at the Warsaw

Summit in 2016. Then, considering this pledge, it presents recommendations in eight specific areas: cooperation with the European Union; relations with business enterprises; information sharing among members; education, training, exercises; capabilities of NCIA; critical infrastructure protection; cyber law and legislature; and collective cyber defense.

Chapter VI concludes with a summary of recommendations, presenting considerations and making suggestions for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. EARLY WARNING FOR CYBERWAR

When John Arquilla and David Ronfeldt wrote, “Cyberwar Is Coming!” in 1993, they noted then that innovations in information technology challenged and changed the structural design of many institutions. Since then, hierarchies have eroded further, and some smaller and weaker actors have become more powerful. Success in war does not just depend on capital, human resources, and technology, but also on superior information about the battlefield (Arquilla & Ronfeldt, 1993). The authors also predicted correctly in 1993 that cyberwar might enable victory without the requirement of destroying an enemy force and without a chain of bloody combats. Under cyberwar doctrine, due to organizational and operational concerns, they expected a reduction in the force size in the U.S. military. Arquilla and Ronfeldt (1993) argued that one of the earliest examples of cyberwar in history comes from Mongol doctrine. According to this doctrine, Mongols “relied for success almost entirely on learning exactly where their enemies were, while keeping their own whereabouts a secret until they attacked” (p. 148). Even though the Mongols were fewer in number, thanks to superior battlefield information, they were successful against China, Islam, and Christendom (p. 148).

Arquilla and Ronfeldt (1993) predicted, “As an innovation in warfare, we anticipate that cyberwar may be to the twenty-first century what blitzkrieg was to the twentieth century. Yet, for now, we also believe that the concept is too speculative for precise definition” (p. 147). Almost 20 years later, Thomas Rid (2012) argues that “cyberwar has never happened in the past, [that] cyberwar does not take place in the present, and [that] it is unlikely that cyberwar will occur in the future” (p. 5). However, John Arquilla (2012) defends his position, stating that “nearly 20 years since David Ronfeldt and I introduced our concept of cyberwar, this new mode of conflict has become a reality. Cyberwar is here, and it is here to stay, despite what Thomas Rid and other skeptics think.”

Furthermore, John Stone (2013) also disagrees with Rid's opinion and states that "cyberwar is possible in the sense that cyber-attacks could constitute acts of war" (p. 107).

B. DEFINING KEY CYBER TERMS

In addition to arguments over whether cyberwar will take place or not, another issue is the definition of various concepts related to cyberwar. Arquilla and Ronfeldt (1993) define cyberwar as "disrupting, if not destroying, information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth" (p. 146). In the book *Cybersecurity and Cyberwar, What Everyone Needs to Know,* Peter W. Singer and Allan Friedman inform and educate an average reader about cyber related terms and concepts. The authors organize the book under subchapters of questions that a reader might have about cyber security and cyberwar. They also include several accounts of historical incidents, descriptive anecdotes that illustrate the topic. The book can be a foundational resource in the cyber area and provides an annotated bibliography. Singer and Friedman (2014) define cyberspace as "the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online" (p. 13).

Chapter eight of the book, *Networks and Netwars: The Future of Terror, Crime, and Militancy,* is written by Dorothy E. Denning, and the title of this chapter is "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." Denning (2001) focuses on three main types of activity: "activism, hacktivism, and cyberterrorism." The first activity, activism, means "normal, non-disruptive use of the Internet in support of an agenda or cause" (p. 241). The second, hacktivism, means "the marriage of hacking and activism" (p. 241). It includes operations in which hacking techniques are used against an Internet site to disrupt normal functions without causing serious harm. Examples of hacktivism are "web sit-ins and virtual blockades, automated email

bombs, web hacks, computer break-ins, and computer viruses and worms" (p. 241). The last activity, cyberterrorism, refers to "the convergence of cyberspace and terrorism" (p. 241). Hacking operations motivated by political goals and planned to cause "grave harm such as loss of life or severe economic damage" (p. 241) are considered cyberterrorism. To illustrate, cyber terrorists may penetrate "an air traffic control system" and cause two aircraft to collide (p. 241). These three activities, "activism, hacktivism, and cyberterrorism," may affect foreign policy in different ways. As Denning (2001) notes,

> the Internet can be an effective tool for activism, especially when it is combined with other communications media. It can benefit individuals and small groups with few resources as well as organizations and coalitions that are large or well-funded. It allows activists in politically repressive states to evade government censors and monitors. With respect to hacktivism and cyberterrorism, those who engage in such activity are less likely to accomplish their foreign policy objectives than those who do not employ disruptive and destructive techniques. (p. 242)

Instead of accepting the demands of hacktivists and cyber terrorists, a target's primary response is possibly enhancing cyber defense policies, both at the national and international level (p. 242). Denning (2001) also provides various examples related to "activists, hacktivists, and cyber terrorists" and their effects on policymakers. Especially, during the Kosovo War, cyber activities of state and non-state actors against NATO and its members were very important because this was the first time NATO faced such serious cyber operations.

In "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," Joe Burton (2015) analyzes the theoretical and definitional problems regarding the cyber security field and explains the strategic challenges of the cyber-attacks against NATO. Burton explores the transformation of NATO's cyber policies and doctrines while reviewing some actual cyber incidents that have occurred. The article represents a good source of information about NATO's cyber policy and the challenges that it faces in this domain. Burton (2015) divides cyber security issues into four categories: cybercrime, cyber

espionage, cyberterrorism, and cyber warfare. He defines cyber security as "being secure from cyber-attacks and efforts to disrupt, delay, or destroy computer networks, and cyber exploitation efforts to covertly obtain information from computer networks" (p. 299). Cybercrime is an act "carried out by private individuals or groups, directed against private individuals and businesses, and take the form of identity theft and financial fraud" (p. 299). The main incentive behind cybercrime is financial gain. Cyber espionage is an activity that "involves state controlled or directed cyber attackers targeting private businesses and foreign governments in order to steal sensitive information for commercial, political and military gain" (p. 300). Cybercrime differs from cyber espionage, because in cybercrime private groups or individuals are conducting the act, while in cyber espionage states or entities acting on behalf of states are conducting these activities. Edward V. Linden (2007) references Denning's definition of cyberterrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (p. 71). Finally, cyber warfare is defined as "an armed conflict conducted in whole or part by cyber means, and military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict" (Cartwright, 2010, p. 8).

C. CYBER ISSUES BECOMING MORE SERIOUS

Richard A. Clarke and Robert Knake (2010) walk the reader through the fundamentals and mechanics of cyberwar in their book, *Cyber War*. The authors also talk about some of the actors and countries who could engage in cyberwar such as Russia and China and give some technical information about their capabilities. The book, which lacks references and footnotes, gives the impression that it offers unsupported opinions. However, the authors try to support their claims with their arguments depending on their experiences. Clarke and Knake (2010) state some of the significant features of cyberwar. They consider cyberwar to be real, because there have been several incidents that

targeted some nation's critical elements. Second, cyberwar's speed is as fast as the speed of light; for this reason, the time between the effect of a cyber-attack and its launch is very hard to measure. Third, cyberwar is global: attackers' capabilities are beyond regional limitations, because information technologies make cyberspace global. Fourth, cyberwar skips traditional battlefields, because there is no need to eliminate an adversary's traditional defense systems before executing a cyber-attack. Finally, cyberwar has begun, because many nations are already preparing for cyberwar to defend their cyberspace and deter their enemies (Clarke & Knake, 2010).

Salih Bicakci (2014) deals with various cyber issues such as the first self-replicating software in ARPANET, *creeper,* and the solution to this worm, *reaper*. The first worm was a sign for future cyber-attacks, and in 2010, the Stuxnet attack showed that worms can stay dormant and may not cause any harm until they achieve their goals (p.124). However, each cyber-attack teaches target countries to defend their systems better. After Stuxnet, Iran started to build its own intranet to limit Internet connections among critical facilities (p. 108). On the other hand, Bicakci provides an example from Egypt during the Arab Spring to show the power of the Internet. Hosni **Mubarak**, the former president, temporarily blocked access to Twitter, Facebook, and Blackberry to prevent activists from exploiting Internet connectivity to support their social movement in the country (Bicakci, 2014). The author also mentions the emergence of the World Wide Web (www), as well as of *hackers* (Bicakci, 2014, p. 115).

According to Singer and Friedman (2014), the number of governments preparing to fight cyberwar in the world is more than 100. In the business sector, 97 percent of the companies on the Fortune 500 list have been hacked. National Security Agency monitoring, the WikiLeaks scandals, and unprecedented cyber weapons like Stuxnet suggest the significance of cyber security. President Barack Obama has stated that "cyber security risks pose some of the most serious economic and national security challenges of the 21st century" (Deibert, 2011, p. 2).

D. CYBERWAR IS REAL

In 2013, John Arquilla published “Twenty Years of Cyber War,” in which he not only asserts that cyberwar is real, but also focuses on the ethical side of the issue. Arquilla (2013) notes that his and Ronfeldt’s 1993 prediction about communication systems, sensors, and weapon systems has become true, and they are crucial for armed forces. However, the negative side of this development is, if systems are disrupted, heavy reliance upon them would imperil the forces in operations. Arquilla (2013) states, “the dominant response to our notion that cyberwar was coming soon was ‘No, it’s not.’ Twenty years on, the tide has clearly turned, with only a few hold-outs taking the view that there is less than meets the eye to cyberwar” (p. 81). Cyber-attacks against Estonia in 2007 and in the Russian-Georgian war, which was supported by skillful hacker attacks in 2008, have made it difficult to deny the existence of cyberwar. Furthermore, in 2010, the Stuxnet malicious worm caused physical damage to Iran’s nuclear centrifuges. This event showed that binary codes could cause destruction in the real world. Despite speculation, no official proof connects these attacks to Russia, Israel, and the United States; however, it is apparent that cyberwar is real (Arquilla, 2013).

Arquilla (2013) raises several ethical questions such as “Can one retaliate justly without knowing the identity of the guilty party?”; “Does the principle of proportionality require an in-kind cyber-response to a cyber- attack?”; or “Can a more physical response be allowed, even a declaration of war followed by military operations?” (pp. 81–82). Answers to these questions are not very clear. Ethically, the attacker’s intent is very important, and if the aim is to cause severe disruption, then a type of military reaction could be legitimate. Yet, the execution of cyber techniques may limit long, bloody, *unethical* conflicts (Arquilla, 2013).

E. LEGAL CONSIDERATIONS

Oona Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel (2012) offer a comprehensive

discussion about the legal issues related to cyber-attacks in their article “The Law of Cyber Attack.” The authors initially define and analyze the terminology of cyber-attack and identify the different types of cyber-attacks. They then explain the legal principles of war, namely *jus ad bellum* and *jus in bello*,[1] and tie these principles to cyber warfare. They also explore the international legal regimes such as the United Nations, NATO, and Council of Europe that regulate cyber-attacks directly, and other international legal regimes like telecommunications law, aviation law, and law of space that indirectly regulate cyber-attacks. The article answers several questions that a reader might have in the area of law of cyber-attacks.

Hathaway et al. (2012) state that cyber-attacks are capable of threatening national security by damaging air defense systems, nuclear power plants and centrifuges, and power grids. Since some consequences of cyber-attacks could be as disruptive as armed attacks, the question of how existing law could be applied to respond to possible cyber threats is very significant. Due to the uniqueness of cyber threats, Hathaway et al. (2012) propose that there must be legal reform on both international and domestic levels besides filling the gaps in the existing law. The legal framework needs to be sufficient for responding to new and growing cyber threats. However, because cyber-attacks are often perpetrated by actors who have transnational roots, domestic law alone is insufficient. Therefore, international cooperation is essential in preparing the international legal framework for fighting against cyber threats (Hathaway et al., 2012).

In the article “In Perspectives for Cyber Strategists on Law for Cyberwar,” Charles Dunlap (2011) focuses on the legal issues that a cyber strategist needs to consider when dealing with cyber-attacks. Dunlap draws a comparison between a cyber-attack and a conventional attack from the Law of Armed

[1] *Jus ad bellum* means the right to go to war, and *jus in bello* means right conduct within war.

Conflict's perspective. The article makes an appreciable contribution to the reader's knowledge about the legal issues in the cyber domain.

Dunlap (2011) states that there is an urgent requirement for a new legal regime covering cyberwar issues. Traditional arms control agreements are not sufficient in deterring attackers in the cyber domain due to the complexity of the attribution problem (Dunlap, 2011). In addition, if there were an international cyber treaty, every nation would have different expectations for it, and each nation would perceive its objectives in its own way. The United States declared that "existing international law could theoretically be applied to cyber conflict and that the United States would support the establishment of 'norms of behavior' that like-minded states could agree to follow in cyberspace" (Dunlap, 2011, p. 83). Response to a cyber-attack depends on the severity of the attack. Cyber-attacks can be legally equivalent to armed attacks only when their consequences are as violent as an armed attack (Dunlap, 2011). However, evaluating the damage of a cyber-attack and assessing its disruption is not a simple task. There can be controversial issues associated with this assessment when it comes to tracking the perpetrator. Nevertheless, even when a cyber incident is equivalent to an armed attack, which justifies the use of force against the adversary for self-defense, it does not automatically create an armed conflict or a state of war (Dunlap, 2011).

F. TALLINN MANUAL

According to the *Tallinn Manual* (2013), cyber operations started to draw attention in the late 1990s. Notably, in 1999, the United States Naval War College assembled the first large-scale legal conference on this topic. Later, "the massive cyber operations by 'hacktivists' against Estonia in 2007 and against Georgia during its war with the Russian Federation in 2008, as well as cyber incidents like the targeting of the Iranian nuclear facilities with the Stuxnet worm in 2010" diverted more attention to cyber operations (Schmitt, 2013, p. 16). Ken

Jones (2015) analyzes the *Tallinn Manual* and NATO in his thesis, *"*Cyber War: The Next Frontier for NATO.*"* Jones notes that

> 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. The Cyber Defense Center is an International Military Organization accredited 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. (pp. 19, 20)

The *Tallinn Manual'*s Part A (International Cyber Security Law), Chapter II (The Use of Force), Section 2 includes rules specifically related to self-defense, namely rules 13 through 17 (Schmitt, 2013). Jones (2015) summarizes these rules: Rule 13, "Self-Defense Against Armed Attack," deals with the right that all countries have to guard themselves when a cyber-attack occurs. Rule 13 also includes "the scale and effect of the attack." In Rules 14 and 15, the *Tallinn Manual* shows that the "right to use force in self-defense" relies on "necessity, proportionality, imminence, and immediacy." Rule 16 in the manual focuses on collective self-defense, restating the need for "necessity, proportionality, imminence, and immediacy." Rule 17 invokes the United Nations (UN) Charter Article 51. If a cyber-attack is ongoing or has already taken place, the United Nations Security Council should be informed immediately about "the violation of Article 51" (pp. 20–25).

Following the *Tallinn Manual* guidance, if the cyber-attack just collected intelligence information, or enabled cyber theft, defining such an attack as an armed attack would not be appropriate. Concepts and rules in the *Tallinn Manual* are generally stated in the abstract terms, because it tries to build an ethical and comprehensive approach for cyber conflict. According to Jones (2015), "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" (p. 25).

G. CYBER POWER AND NUCLEAR LESSONS

In his paper "Cyber Power," Joseph Nye (2010) discusses how the concept of power can be applied to cyberspace. Nye (2010) argues that the diffusion of power differs in cyberspace from other domains of warfare. He walks the reader through the concepts of power, the cyber power reality, actors in cyberspace, and the roles of government in this new domain. The article is very informative about the relationship between the power concept and cyberspace.

Nye (2010) stated that the effects of cyber power vary from commerce to war, with a very wide range of effects. Competition among individuals, corporations, and governments is not a new phenomenon, but the factors of anonymity, entry with a low price, and ability to create asymmetric threats let smaller actors achieve significant objectives in cyberspace by exercising soft and hard power that is very hard to do in the other domains of warfare with such limited resources (Nye, 2010). Therefore, the differentials of power among actors are reduced due to the characteristics of cyberspace, and this represents an example of the diffusion of power in world politics. The biggest powers are not able to dominate the cyber domain completely as much as they do in the other domains of warfare like sea, air, or space. Nye (2010) claims that although cyberspace enables some power shifts among the strong and weak states with the opportunity stated previously, the likelihood of these power transitions being a game changer in international politics is very small.

In another article, "Nuclear Lessons for Cyber Security," Nye (2011) raises an important question, "Can the nuclear revolution in military affairs seven decades ago teach us anything about the current cyber transformation?" (p. 22). He makes a useful comparison between cyber and nuclear technology. This article is very helpful for making an analogy between these two very different technologies. It also provides significant lessons from the nuclear strategies in the past.

Nye (2011) states that there are significant technological differences between nuclear and cyber capabilities. For instance, while nuclear explosions are unambiguous, cyber intrusions can be unnoticeable for a long time. The destruction level of nuclear technology is enormous, while cyber-attacks do not pose such a catastrophic threat. Nye (2011) argues that the results of a nuclear war could take the world back to the Stone Age, while a big cyberwar at most could take a country to the economic level of 1990s.

Despite these differences, Nye (2011) argues that several nuclear lessons can be learned and applied to the cyber domain. The general lessons he explains in his article are that "continuing technological change [will] complicate early efforts at strategy" (p. 23); "strategy for a new technology will lack adequate empirical content" (p. 25); "new technologies raise new issues in civil-military relations" (p. 26); "civilian uses will complicate effective national security strategies" (p. 27); "learning can lead to concurrence in beliefs without cooperation" (p. 29); "learning is often lumpy and discontinuous" (p. 30); "learning occurs at different rates in different issues of a new domain" (p. 31); "military in international contacts [should be involved]" (p. 32); "deterrence is complex and involves more than just retaliation" (p. 33); and "arms control with positive-sum games related to third parties [should be started]" (p. 34). To sum up, these lessons represent a useful guideline when making an analogy between nuclear and cyber technologies.

H. CYBERWAR AND NATO

In the article, "NATO's Emerging Threat Perception: Cyber Security in the 21st Century," Bicakci (2014) argues that the "Westphalian state system has been deeply affected from the civilianization of the cyber space." The legacy of nuclear war competition is apparent in the post-Cold War period. Nowadays, threats in cyberspace and their ambiguous boundaries can be observed in recent cyber cases. The latest cyber-attacks against NATO and its member states show that cyber will be a crucial issue in the future. The author also discusses the

kinds of defensive measures and strategies that NATO has implemented to meet these new cyber threats. NATO's first step for a cyber defense strategy is to increase the level the cyber capabilities of allied countries (p. 101).

Jason Andress and Steve Winterfeld have written *Cyber Warfare,* a comprehensive book that provides substantial information on cyber issues. This book covers not only strategic, but also operational and tactical approaches to current conflicts in cyberspace. The design of the book helps anyone understand the necessary parts of recent developments, besides providing strong background information. The book uniquely presents the information in a way that can be utilized "to establish a strategic cyber security vision for an organization" (Andress & Winterfeld, 2014, p. xiii). On the other hand, it also contributes to the national debate on the future of cyber. A variety of individuals or groups, including policy makers and security professionals, can benefit from this resource, because the concepts are helpful to determine the allocation of resources and implementation of security projects and policies (p. xiii).

Andress and Winterfeld (2014) have designed the book in a way that readers can read chapters separately. The first chapter deals with what cyber warfare is and its different aspects compared to conventional warfare. Chapter 2 is related to cyber threats, especially attackers' methods, tools, and techniques. The authors mention cyber as the fifth domain of war in Chapter 3, and current cyber warfare doctrine for militaries, states, and organizations in Chapter 4. The fifth chapter focuses on present and future cyber warriors in terms of their education, training, certifications, and so forth. Logical, physical, and psychological weapons are covered in Chapters 6 through 9, and computer network attacks and defense are the main focus of Chapters 10 and 11. In addition to state actors, non-state actors are also active in the cyber domain. Chapter 12 discusses corporations engaged in cyberwar, cyber terrorists, cyber-criminal groups, and autonomous cyber actors. Finally, Chapter 16 covers the future of cyberwar, "the most likely and most dangerous course of action for conflicts in the cyber domain," and what should be done through international relations (p. xvii).

Andress and Winterfeld (2014) argue that “organizations like NATO have very active cyber communities” (p. 10). The Cooperative Cyber Defense Center of Excellence (CCDCOE) located in Tallinn, Estonia, was officially founded on the May 14, 2008, to develop NATO’s cyber defense capacities (p. 68). The appendix of the book provides a “Cyber Timeline,” which includes the major cyber events until 2013. The events directly related to NATO are the 1999 Serbian hackers’ attack on NATO systems during NATO’s military operations in Kosovo; the 2007 Estonian attacks, in which hackers were linked to the Russian government; and the 2008 cyber-attacks against Georgia, which applied for membership to NATO previously, during the military engagement with Russia (pp. 293, 294).

In “International Cyber Incidents: Legal Considerations,” Eneken Tikk, Kaska Kadri, and Vihul Liis (2010) analyze four cases in the years between 2007 and 2008. The Estonia Case in 2007, the Radio Free Europe/Radio Liberty Case in 2008, the Lithuania Case in 2008, and the Georgia Case in 2008. The authors give details for each case, including background of the incident, facts of the case, and legal considerations about the case. The authors also make an evaluation of these cases at the end and provide their observations and recommendations for the readers.

Tikk et al. (2010) state that reliance on information technologies makes organizations vulnerable to cyber threats. These incidents have shown that most of the countries lack adequate legal frameworks to cope with this kind of threat. They also demonstrated how easy it is to launch cyber-attacks, and how complex the challenge is to defend the networks and infrastructures of an organization due to the rapid developments in this field. These incidents have also exposed the need for change in cyber strategy. Adequately addressing real cyber incidents is beyond most states’ preparation level (Tikk et al., 2010). In addition to providing important takeaways from these incidents in the conclusion, the authors present a detailed timeline at the end of the report showing key events in each case.

I. SUMMARY

Overall, the presence of cyberwar is undeniable, and every country has to take action to address threats in the cyber realm. This problem is not simple enough to be addressed entirely within national boundaries; the reality of the cyber domain stands as a transnational phenomenon. NATO plays a significant role in this transnational environment with its collective defense strategy. The cyber incidents against NATO and its member countries have opened up a new frontier for NATO. The organization has been trying to adapt to these changes by taking some measures, such as implementing new strategies and policies against cyber threats, and establishing new institutions like NATO CCDCOE. However, more research must address the sufficiency of NATO's cyber policies to defend itself and its member countries against cyber threats.

III. THE CYBER THREATS AGAINST NATO

Threats in the cyber domain and the abilities of cyber actors are evolving rapidly because of unprecedented technological advances. Like every individual state, NATO as a collective defense alliance must also be vigilant about the threats and actors in the cyber realm. In this chapter, the cyber threats against NATO are discussed by analyzing cyber threat categories, cyber actors, and cyber incidents related to NATO's security in the cyber domain.

A. CYBER THREATS

Defining and categorizing cyber threats is a challenge due to their complexity and variety. In this section, cyber threats are classified and discussed under the four categories of cybercrime, cyber espionage, cyberterrorism, and cyber warfare.

1. Introduction

In 2010, President Barack Obama stated that "it is now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation, and we are not as prepared as we should be, as a government or as a country." As governments and economies have become too dependent on Internet and digital infrastructures, they have become a valuable target for adversaries (Andress & Winterfeld, 2014). Denning (2007) also observe that an increasing number of criminals, spies, hackers and others who have found benefit in damaging and exploiting computer networks have been targeting them. Several critical infrastructures are vulnerable to cyber-attacks, such as nuclear power plants, transportation infrastructures, healthcare, emergency services, dams, banking and finance, communications, agriculture, chemical, and defense infrastructures (Andress & Winterfeld, 2014).

2. Categories of Cyber Threats

Conceptual and definitional challenges are associated with the cyber realm that scholars have been trying to overcome since the beginning of the cyber era. The fundamental terminology about cyber and categories of cyber threats are the subject of debate. The UN defines *cyber* as “the global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net” (Andress & Winterfeld, 2014, p. 4). The United States Department of Defense defines *cyberspace* as the “notional environment in which digitized information is communicated over computer networks” (Andress & Winterfeld, 2014, p. 3). To analyze cyber threats from the perspective of NATO requires a classification framework for these threats. As Burton (2015) put it, cyber threats can be classified into four main categories. These categories are cybercrime, cyber espionage, cyberterrorism, and cyber warfare.

(1) Cybercrime

Cybercrime can be defined as a “crime enabled by or that targets computers” (Alexander, 2014, p. 2). These criminal activities can be carried out by individuals or groups who have diverse goals such as financial gain, identity theft, and damaging property. Most cybercrime is financially motivated and incurs economic costs. According to Steve Morgan (2016), the global cost of cybercrimes to business increased to $500 billion per year, and this number quadrupled from 2013 to 2015. Morgan (2016) also predicts that the cost of cybercrimes and data breaches could reach $2.1 trillion a year globally by 2019. Although cybercrime is not regarded as a military threat, the increase in organized cybercrime represents an important threat to the security of NATO member countries (Burton, 2015).

(2) Cyber Espionage

Cyber espionage can be defined as “the use of computer systems or information technology to illegally obtain confidential/secret information from the

government, private sector, or some other entity" (Alexander, 2014, p. 2). Cyber espionage activities are conducted by cyber attackers directed or controlled by states for the purpose of providing required knowledge to the states to obtain political, commercial, and military gain (Burton, 2015). Since cybercrimes are conducted by groups or private individuals, cyber espionage differs from cybercrime in terms of its perpetrators (Burton, 2015). Espionage activities have existed in the international system for ages, but new information technologies have introduced an unprecedented capability and ease to this field. Alexander Klimburg (2011) points out that the Pentagon lost 25 to 27 terabytes of data in 2007, which is equivalent to 5,000 DVDs of digital information. Cyber espionage can be conducted by any motivated state actor with sufficient cyber-attack capabilities. Therefore, states have never been this vulnerable to espionage at any time in history.

(3) Cyberterrorism

In 2001, Denning defined *cyberterrorism* as "the convergence of cyberspace and terrorism" (p. 241) that "covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" (p. 241). There is also a continuing debate on defining cyberterrorism just like the arguments on definitions of terrorism itself. Dean C. Alexander (2014) defines cyberterrorism as "unlawful attacks and threats of attack against computers, networks, and information stored therein—carried out through the computers, Internet, or the use of flash drive storage devices—when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Alexander, 2014, p. 3).

Burton (2015) describes two conditions that need to be fulfilled to count a cyber-attack as cyberterrorism: first, "its effects should be comparable to terrorist attacks" (p. 300); second, "the intent should be coercing political change" (p. 300). The main difference between cyber-attacks and cyberterrorism is the motives behind these activities. Cyber-attacks are carried out because of

financial and other (political) aims, but the motives for cyberterrorism are mostly political, religious, or social (Alexander, 2014). Cyber-attacks can be utilized by terrorist groups owing to their convenience, flexibility, and low cost. The attribution problem also can serve as an advantage for the terrorist groups. The consequences of cyber terrorist activities can be very damaging to a state's assets. Therefore, this field represents a critical area for the national security of the states.

(4) Cyber Warfare

Cyberspace is regarded as the fifth domain of warfare after land, sea, air, and space by many states. NATO Secretary General Jens Stoltenberg announced in June 2016 that "the 28-member alliance has agreed to declare cyber an operational domain, much as the sea, air and land are" (Clark, 2016). Andreas Hagen (2013) stated this breakthrough as follows: "warfare has reached a new frontier. Over the past several years and even decades, it has been accumulating to this point where war is not only fought with bombs and guns anymore but also with bits and bytes" (p. 1).

Introducing a new battlefield to the defense organizations brings up several issues related to cyber warfare. Like other fundamental terminology in this field, cyber warfare is also defined in various ways by scholars. One definition of cyber warfare can be "utilizing computers and other instruments to target an enemy's information systems rather than attacking an enemy's armies or factories" (Alexander, 2014, p. 4). The use of cyber power in military operations would definitely serve as a huge force multiplier in contemporary military doctrines. Since the armed forces are highly dependent on information technologies and computer networks, disruption of these systems would provide great advantages to the adversary. Therefore, defending national defense systems from cyber-attacks in terms of cyber warfare is very critical for states. One of the most prominent examples of cyber warfare was observed during the Russo-Georgia War in 2008 (Hagen, 2013). Experts claimed that the Georgian

government got cyber-locked after Russian cyber-attacks gave Russia a strategic advantage for its continuing military operations (Korns & Kastenberg, 2008).

NATO's involvement in each of these cyber threat categories is debatable. Although NATO's mission might not be to define and classify everything in cyberspace, "it is the alliance's role to prevent crises, manage conflicts, and defend one another against attacks, including against new threats – none of which can be conducted with vague directions and abstruse concepts" (Laasme, 2011, p. 61). Burton (2015) identifies the core and peripheral role of NATO in four categories of cyber threats. First of all, he argues that since NATO is not a police organization or a justice institute to fight crimes, civil and legal responses would be a better solution to fight cybercrimes, and the role of NATO in this area may be inappropriate. Second, he states that NATO's role in cyber espionage might be both necessary and appropriate due to the critical and confidential information that it keeps in its own networks. If this information were exfiltrated from its systems, this breach would damage the security of all of the alliance, and this information could be used against member countries. Third, after 9/11 NATO invoked Article 5 for the first time; this showed its determination to fight against terrorist organizations and activities. Since, cyberterrorism is just a variant of terrorism in general, NATO has a natural stake in fighting cyberterrorism. Finally, Burton (2015) points out that cyber warfare is an evolving domain that NATO cannot disregard. To meet its collective defense goals, NATO must defend its alliance in this frontier.

B. CYBER ACTORS

The Internet provides great power to its users through global interconnected networks. Since national and international laws for the Internet are very limited, some non-state actors have freely acquired cyber power, and they can even threaten states' activities in cyberspace (Czosseck, 2013). In cyberspace, borders and sovereignty of states are controversial. Electrons do not have passports or visas, and malicious packets can be blocked only when they

are detected. Potentially severe cyber-attacks are not detectable because these attacks do not require planners to prepare great logistic support. Denning (2001) observes, “They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker” (p. 285). The nature of cyberspace forces us to face an undesirable fact that experienced and wary cyber actors such as individuals, groups, or states, can operate malicious attacks from anywhere in the world, with a low possibility of being detected (Czosseck, 2013). In this section, cyber actors are discussed under two categories, state actors and non-state actors.

1. State Actors

According to Scott Jasper (2015), the most remarkable and publicly known actors are “groups of attackers categorized as an advanced persistent threat” (APT) (p. 62). “APT hacking is designed to covertly penetrate networks and systems to steal or alter information, manipulate data, or cause damage” (p. 62). These groups can be military units or some other related groups who get support from national governments (Andress & Winterfeld, 2014, p. 46).

Cyber power is crucial at the deterrence level of countries; however, it is difficult to determine which countries are stronger in cyberspace than others. Furthermore, classifying state actors as threats against NATO is also challenging because of the attribution problem. In order to differentiate the cyber power level of countries, cyber offense and defense capabilities can be compared. The level of a state’s dependence on cyberspace is also important because it directly relates to the vulnerability of that state. However, without adequate information about countries, it is almost impossible to compare them. Clark and Knake compare the “cyberwar strength of the U.S., Russia, China, Iran, and North Korea” (Clarke & Knake, 2010, p. 148). In order to rank all countries or at least to compare some of them, they should provide all cyber related information;

nevertheless, the information-sharing level will never reach that point for apparent reasons.

Aside from cyber power considerations, focusing on the activities of states in cyberspace, these activities can be divided into three main categories, which are law enforcement, intelligence services, and armed forces (Czosseck, 2013). However, law enforcement bodies conceptually cannot be considered a threat to NATO, because their fundamental goal is to ensure domestic security by enforcing laws or keeping citizens away from crime in cyberspace. This leaves intelligence services and armed forces as potential cyber threats from states.

(1) Intelligence Services

Espionage among nations is an internationally accepted and common practice. Even though this act is generally outlawed by the legal systems of countries, it has become a traditional activity. With the international development in information and communication technology, intelligence agencies benefit from new ways to reach their targets. Relatively safe and globally accessed espionage activities via the Internet have led many nations to develop capabilities to conduct operations in cyberspace. States can broadly spy on the Internet by focusing on activities of interest via cyber tools (Czosseck, 2013).

(2) Armed Forces

Although some countries officially recognize cyberspace as the fifth warfare domain, others prefer not to do so. However, without hesitation, almost all countries are under pressure to enhance cyber military capabilities to fight against cyber actors. Many scholars compare and find similarities between current developments in cyberspace and past cases of traditional arms races. These are strong signs of another race starting among countries (Jellenc, 2012; Czosseck, 2013).

2. Non-state Actors

Almost 25 years ago, scholars were saying that non-state actors in cyberspace should also be treated as opponents. Activities of these actors do not recognize national boundaries (Arquilla & Ronfeldt, 1993). “Non-state actors, logically, are those that take actions of a cyber nature, but are not directly part of a nation-state” (Andress & Winterfeld, 2014, p. 207). In the literature, scholars define and classify non-state actors divergently. According to Christian Czosseck (2013),

> hackers, (organised) cyber criminals, hacktivists and, to a disputed extent, cyber terrorists, have emerged over time. To make a clear-cut distinction between them is, in many cases, futile, as globally different definitions, legal frameworks and, more often than not, political agendas lead to different assessments of the same action. (p. 3)

One of the most famous words related to cyber actors is “hacker,” which has become a universal word in cyber terms. However, due to this popularity, people tend to mistakenly call all cyber actors hackers. Czosseck (2013) provides distinct definitions as follows: “hackers without a malicious intent are referred to as white hats or ethical hackers” (p. 5); “grey hats … often want to support the wider community, making cyberspace more secure by using their skills against wrong-doers” (p. 5); and “others use such knowledge to blackmail their victims, which leads into the last subculture of hackers introduced here, often referred to as black hats” (p. 6).

Andress and Winterfeld (2014) provide a more comprehensive classification in their book, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, for non-state actors in cyberspace. The terms used to describe individuals or groups who are considered as non-state actors are “rather arbitrary and tend to vary wildly from one source to another” (Andress & Winterfeld, 2014, p. 208).

Six different terms related to non-state actors and their alternatives are presented by the authors. The terms are “script kiddies, malware authors,

scammers, blackhats, hacktivists, and patriot hackers" (Andress & Winterfeld, 2014, p. 209). Script kiddies have the lowest level of skills, but they are the most common ones. "Script kiddies generally use scripts and tools that have been written by others in order to conduct their attacks, but have no great skill or ability beyond the use of such tools" (p. 209).

Malware authors, who may be employed by states and organized crime groups, can compile "original items of malware, [but] some certain amount of skill at programming and knowledge of the target operating systems is required" (p. 209). Scammers are often treated as the lowest of the low among attackers (p. 209), and blackhats are "the bad guys of the hacker world. Such hackers often have no particular care for the rule of law, the systems that they disrupt, or what ill effects they cause" (p. 210).

Hacktivists act primarily for political reasons, and they "tend to select targets with high visibility which they see as appropriate to deliver the intended political message" (Czosseck, 2013, p. 7). Hacktivists' tools are "website defacement, mass emailing, Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, Domain Name Service (DNS) hijacking, or any of a number of other methods" (Andress & Winterfeld, 2014, p. 211). Patriotic hackers can also be considered as hacktivists; however, they generally deal with national conflicts and "can even join into cyberwars as independent players" (p. 211).

Having identified the six different terms related to non-state actors, we consider the four categories of non-state actors who can threaten NATO.

(1) Individual Actors

Individual attackers "range greatly in skill level, from the lowliest script kiddie who can only run automated tools," to the most skilled hackers, "who can penetrate a system with disturbing ease and leave no trace for the owners of the system to detect" (Andress & Winterfeld, 2014, p. 208).

(2) Corporations

Giant corporations can be “possessors of great power and resources, often rivaling those of small countries” (Andress & Winterfeld, 2014, p. 211). Corporations, especially, “in the technical industry are often well organized, staffed with highly trained employees, and have access to the latest technologies and equipment, including those with which cyber warfare can be carried out” (p. 211). Refraining from criminal activities, business people and politicians are the practitioners of traditional organized commercial and industrial espionage, which dates back to the 14th century (p. 211).

(3) Cyber Terrorists

Cyber terrorists are an emotionally motivated category of attackers, and they are related to “both hacktivists and patriotic hackers, differing largely in both the scale and the intensity of their actions” (Andress & Winterfeld, 2014, p. 212). A cyber terrorist may disrupt “banks, international financial transactions, and stock exchanges” (Denning, 2001, p. 282). Following such disruptions, economic systems may stop, the public may lose confidence, and destabilization can be achieved (p. 282).

(4) Organized Cybercrime Actors

The attribution problem, lack of cyber related laws, and the cross-border feature of cybercrime have encouraged the formation of organized cybercrime groups that operate globally (Czosseck, 2013). One of the most famous international cybercrime organizations was the Russian Business Network, which was the only cybercrime organization recognized as a primary threat by NATO in 2009 (*Daily Beast*, 2009; Czosseck, 2013). Recently, “organized cyber criminals have begun to target the organizations where large amounts of such data [personal and exploitable information] are warehoused, often credit card processing centers and other financial institutions” (Andress & Winterfeld, 2014, p. 215).

3. Most Active and Dangerous Cyber Actors

Analysis of war requires a deep "understanding of the enemy forces and their composition, disposition, strength, centers of gravity, and terrain…. [T]his was true under Sun Tzu, Napoleon Bonaparte, Alexander the Great, and still [is] today" (Andress & Winterfeld, 2014, p. 45). In the cyber battlefield, various actors operate, and they cause different levels of damage to their targets. Script kiddies are the most active threat in terms of amount of activity (p. 45). In addition to the activity level of cyber actors, it is crucial to determine the level of impact or damage that threat actors can cause. The threat that results in the greatest impact and damage is the APT, which generally originates from nation states (p. 46).

After evaluating cyber threats and actors that operate in cyberspace, we are left with one question: Have we have seen a cyberwar or not? So far, no state actor has officially declared a war in cyberspace, but a series of serious cyber-attacks were conducted against Estonia in 2007. In 2008, Georgia suffered from coordinated cyber and kinetic attacks. These kinds of cyber incidents directly involve nation states and may require military action (Andress & Winterfeld, 2014, p. 10). Estonia is a NATO member country, and Georgia is a candidate state for NATO alliance. Many other cyber incidents have had a direct or indirect effect on NATO, and to better understand cyber threats and actors, we should study and scrutinize these cyber cases.

C. CYBER INCIDENTS AND CASES

Cyber threats against NATO can be understood by analyzing recent major cyber incidents. These incidents give an idea about how future cyber-attacks might be executed against NATO and its member countries. Would any of these incidents call for a NATO response if conducted against a NATO member? This question needs to be kept in mind when examining the following cases. In this section, the 1999 Serbian-NATO conflict, 2007 Estonia case, 2008 Georgia case, 2010 Stuxnet case, 2014 Ukraine case, and other cyber incidents are discussed.

1. Serbian-NATO Conflict (1999)

As an international actor, in 1999, NATO warned its members about attacks to their communication systems and wanted members to be ready for such attacks (Bicakci, 2014). However, the first cyber-attacks occurred earlier than expected. When NATO forces began bombing Serbian targets, unexpected cyber-attacks started. Hackers mostly preferred DDoS attacks to disable the military communication systems of NATO and its member states (Bicakci, 2014).

Denning (2001) notes in the book chapter, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” that the Kosovo conflict has been interpreted as the first Internet war. She concludes that “government and nongovernment actors alike used the Net to disseminate information, spread propaganda, demonize opponents, and solicit support for their positions” (Denning, 2001, p. 239).

Denning (2001) provides examples of activism and hacktivism during the Serbian-NATO Conflict. She emphasizes actions by non-state actors, yet state activities “are discussed where they reflect foreign policy decisions triggered by the Internet” (Denning, 2001, p. 241). Publication, coordination of action, and lobbying decision makers are examples of activist operations; however, focusing on hacktivist activities against NATO will be a better approach to understand cyber threats to the alliance. As mentioned previously in brief, there are four types of hacktivist activities: “virtual sit-ins and blockades [DDoS attacks], automated email bombs, web hacks and computer break-ins, and computer viruses and worms” (Denning, 2001, p. 263). These activities are detailed here.

(1) DDoS Attacks

DDoS attacks in cyberspace are similar to the physical version of sit-ins or blockades (Denning, 2001). The aim of these attacks is to draw “attention to the protestors and their cause by disrupting normal operations and blocking access to facilities” (p. 264). For example, “Belgrade hackers bombarded NATO’s web server with ‘ping’ commands, which test whether a server is running and

connected to the Internet," and the effect of these attacks was to generate "line saturation" of the target servers (p. 268).

(2) Email Bombs

Denning (2001) asserts that bombarding government policy makers with thousands of messages via automated tools can cause a complete jam in their inboxes and make it impossible for required email to be received. During the Kosovo crisis, both sides of the conflict email bombed official sites. Denning (2001) notes:

> According to PA News, NATO spokesman Jamie Shea said the NATO server had been saturated at the end of March by one individual who was sending 2,000 messages a day. Fox News reported that when California resident Richard Clark heard of attacks against NATO's website by Belgrade hackers, he retaliated by sending an email bomb to the Yugoslav government's site. Clark said that a few days and 500,000 emails into the siege, the site went down. (pp. 269–270)

(3) Web Hacks and Computer Break-ins

Hacktivists can change what Internet users see when they visit a web page by hijacking the site, which involves "tampering with the Domain Name Service so that the site's domain name resolves to the Internet protocol address of some other site" (Denning, 2001, pp. 272–273). Hacktivists can also deface a website by hacking into the site and changing its home page. During the Kosovo conflict, many websites were defaced. According to Fox News, the *Boston Globe* reported that a U.S. hacking group named Team Spl0it accessed government sites and posted statements like "Tell your governments to stop the war." The Kosovo Hackers Group, which consisted of European and Albanian members, changed more than five sites with "Free Kosovo" banners. Furthermore, the "Serb Black Hand hackers group had deleted data on a U.S. Navy computer." They also participated in operations to "block and disrupt military computers operated by NATO countries." On the other hand, after NATO accidentally

bombed China's Belgrade embassy, furious Chinese hackers supposedly attacked U.S. government sites (Denning, 2001, pp. 273–274).

(4) Computer Viruses and Worms

Denning (2001) notes that hacktivists have disseminated protest messages and impaired opponents' computer systems by using computer viruses and worms. These malicious codes infect computers and proliferate over computer networks. She says that "during the Kosovo conflict, businesses, public organizations, and academic institutes received virus-laden emails from a range of Eastern European countries, according to mi2g, a London-based Internet software company" (p. 280). The damage to the receiver generally originated from many viruses attached to email, which included plain text or an anti-NATO cartoon. According to the mi2g's claims, Serbian hackers threatened the economic infrastructure of NATO members more than "their better prepared" command and control systems (p. 280).

2. Estonia (2007)

In April and May of 2007, Estonia suffered a major cyber assault, and the world learned how severe a cyber-attack could be on a nation state (Miller & Kuehl, 2009). Some argue that this incident was a clear representation of cyberwar toward a country; however, some think that it was just a cyber riot taking place due to a political decision that created unrest in the society (Heickerö, 2010). Regardless of how these attacks are classified, this was a wake-up call to states to realize the seriousness of cyber threats.

The riots started when the Estonian government decided to remove the Bronze Soldier monument made in the Soviet-era as a memorial of the Soviet victory against Nazi Germany in the World War II. However, people in Estonia ascribed different meanings to that monument. For the Estonians, the monument represented the occupation of Estonia by the Soviets; for the Russian minority in Estonia, the monument was a means to commemorate the heroism and sacrifice in World War II. Thousands of people made protests and demonstrations at the

memorial site after the Estonian government's removal decision. These protests escalated into street riots, and many people were arrested or injured in these street riots. The riot in the streets then moved into cyberspace. In addition to the domestic riots between the people and government, Estonia also experienced political tension with Russia especially after joining NATO in 2004.

The reason why these cyber-attacks spread over all of the country in a very short time and in a serious way is related to the Estonia's highly computerized infrastructure. Despite its small size and population, Roland Heickerö (2010) notes that Estonia is "one of the most highly connected countries in the world" (p. 42), and the country is often referred to as *eStonia* by its citizens. The dependence of private and public sectors on cyberspace was very heavy at the time. Therefore, Estonia was a very attractive target because of its widespread public e-services and common use of Internet access by its population. This dependency made the Estonian government and its agencies, the economic entities in the country, and the population very vulnerable and open to large-scale disruptions (Tikk et al., 2010).

Tikk et al. (2010) divided the cyber-attacks into two phases. The first phase occurred between April 27 and 29, and the attacks, which were mostly carried out by emotionally motivated actors, were less complex and showed poor coordination. However, during the second phase, which took place from April 30 to May 18, the attacks were sophisticated and coordinated more professionally. There was also a clear correlation between the political tension and the intensity of the cyber-attacks. The attackers used denial of service (DoS) and distributed denial of service (DDoS) attacks, mass unsolicited emails against government servers, website defacements, and disrupted DNS servers (Tikk et al., 2010). Tikk et al. (2010) assigns the targets of cyber-attacks to four categories. These are Internet infrastructure providers; governmental and political website targets, such as the websites of the prime minister, president, and Parliament State Audit Office, state departments, and state agencies like the Police Board, and the Reform Party; commercial services like e-banking; and random personal targets.

Heickerö (2010) states that the individuals, groups or organizations behind the operation had not been fully established yet al.though common perception and belief attribute these cyber-attacks to the Russian government, no digital forensics have ever proved the involvement of the Russian government (Miller & Kuehl, 2009). After the attacks, the State Informatics Center announced that 178 countries' computers were involved in these attacks, so it seemed like they were sourced worldwide (Tikk et al., 2010). However, Jason Healey and Leendert van Bochoven (2012) argue that many attacks came from Russia, the code of the malware was written in Russian, or the coordination was done through Russian websites, but it still is not adequate to attribute these cyber-attacks to Russia. Estonian Foreign Minister Urmas Paet also accused the Russian government of being directly involved in the cyber-attacks (Bright, 2007). Despite the lack of evidence that would establish a direct link between the attacks and the Russian government, the allegation of Russia's guilt was encouraged or at least ignored by the Kremlin (Healey & Bochoven, 2012).

The cyber-attacks affected Estonia in economic, societal, and political ways. After seeing the consequences of these attacks, Estonia adopted its Cyber Security Strategy (Tikk et al., 2010). This strategy aims to develop a sophisticated and comprehensive cyber security culture to fight the risks associated with the vulnerabilities of cyberspace. Tikk et al. (2010) specify five main policy fronts to reach the objectives discussed in the Estonian Cyber Security Strategy. These are developing and implementing "system of security measures" (p. 30), "increasing expert awareness and competence in cyber security" (p. 30), improving "the legal framework for supporting cyber security" (p. 30), "bolstering international cooperation" (p. 30), and "raising public awareness on cyber security" (p. 30). Stephen Herzog (2011) described the Estonia case as follows.

> The severity of the Estonian cyber-attacks served as a wake-up call to the world, as it became clear that potentially autonomous transnational networks—like unhappy pro-Kremlin hacktivists—could avenge their grievances by digitally targeting and nearly

> crippling the critical infrastructure of technically sophisticated nation-states. (p. 56)

Therefore, this incident represented a cautionary example for states and international organizations about the cyber domain, and prompted them to take more serious measures in this area. For instance, NATO established the CCDCOE in 2008 in Tallinn, Estonia as a headquarters for the alliance's cyber security concerns, because the Estonia case demonstrated to NATO that, as an alliance, it did not have the sufficient capability and presence in this domain to ensure the protection of its member countries' sovereignty in cyberspace (Herzog, 2011).

3. Georgia (2008)

In 2008, the conflict between Georgia and Russia brought cyber security issues and considerations to the states' attention once again, and as Robert Miller and Daniel Kuehl (2009) note, the "wake-up call in Estonia was repeated even more loudly" (p. 3). South Ossetia sits between Georgia and Russia, and historically, has been a region with many unresolved problems. After the Georgia-Ossetia conflict in 1991, the region became independent from Georgia in a *de facto* way (Tikk et al., 2010). Even though South Ossetia was recognized as integrated with Georgia by the international community, separatist movements continued.

In a surprise and radical decision, the Georgian government started an attack against the separatist forces on August 7, 2008. The tension between Georgia and Russia rose quickly, and after Georgian Armed Forces responded to the provocation of the separation groups, the tension transformed into a hot conflict between two states. The following day, Russia responded with a military operation into the Georgian territories. This military operation was also backed by serious cyber-attacks that started on the evening of August 7 (Bicakci, 2014).

There were three main methods used in the cyber-attacks against Georgia: website defacements, Structured Query Language (SQL) injections,

and DDoS attacks (Heickerö, 2010). In addition to these attacks, malicious software and attack instructions were distributed, and a list of email addresses of Georgian politicians was released for spamming purposes. On August 8, the cyber-attacks by hacktivists started against the websites of the president, defense and foreign affairs ministries, parliament, and the national bank when the Russian forces started their military operations across the border (Heickerö, 2010). For more than a day, the website of the president was down due to a DDoS attack (Tikk et al., 2010). Many other websites of news and media institutions, hacker platforms, and financial institutions were also subjected to DoS and DDoS attacks.

One of the Russian forums that played a critical role in the hacktivist attacks was *stopgeorgia.ru*. This website was set up within a couple of hours after the Russian forces started their military operations in South Ossetia (Heickerö, 2010). Although the hosting firm for this website was registered in New York, its operations were conducted in St. Petersburg. More interestingly, Heickerö (2010) states that the office of this hosting firm was in the same building in St. Petersburg as a "Ministry of Defence Institute, the Russian Centre for Research of Military Strength of Foreign Countries" (p. 46). Moreover, the headquarters of the firm was located on the same street as well (Heickerö, 2010).

There is also a consensus about the existence of coordination of the cyber-attacks (Tikk et al., 2010). The support and coordination activities were made in the Russian language and on the Pro-Russia forums, which demonstrate the Russian hacker community's involvement. Although the consequences and the goals of the cyber-attacks strongly align with the Russian Federation's interests in the Georgia conflict, it is very difficult to prove that Russia was directly involved in these attacks. The Russian government rejected the accusations of involvement in the cyber campaign. However, as Sergei A. Medvedev (2015) has observes in a Naval Postgraduate School thesis, "the historical record shows clear support of the Russian government and implied consent in its refusal to intervene or stop the hacker attacks" (p. 24). Even if the

Russian government was directly involved in the cyber-attacks or supported them, it participated in a very clandestine way (Medvedev, 2015).

International assistance played a significant role in mitigating the effects of the cyber-attacks against Georgia. For example, the location of the website of the Ministry of Defense was moved to Atlanta, Georgia; the website of the Ministry of Foreign Affairs was transferred to the servers of Estonia; Poland helped analyzing Internet protocol data, and France assisted with collecting log files while the attacks were taking place (Tikk et al., 2010). Therefore, the severity of the attacks was relatively reduced by the international assistance.

The cyber-attacks did not cause very serious impacts on Georgia's information capabilities because of the country's relatively limited adoption of information technologies. In 2008, only 7 percent of the people in Georgia had Internet access, but the percentage was growing in a rapid way (Tikk et al., 2010). Nevertheless, the attacks affected the country's situation while the war was going on. Georgia lacked the ability to distribute information about the conflict both to its people and to the international community during the first few days of the conflict. Also, conventional and cyber warfare damaged the country's communication and information network structure physically and technically (Tikk et al., 2010).

The Georgia case was the first time that an offensive military operation was combined with a cyber operation (Heickerö, 2010). Heickerö states that "it could be seen as new *modus operandi* that could set the standard for the future cyber conflicts" (p. 47). Even though the war lasted for only a short time, Russia gained strategic advantages from this war by showing its military and cyber readiness (Hagen, 2013). Although the cyber warfare that took place in the Georgian conflict did not have a high level of sophistication, even at this low level of sophistication it succeeded in impairing strategic information and communication capabilities. Therefore, the role of cyber capabilities in the modern war concept arose once again in this case.

4. Stuxnet (2010)

Although Iran suffered the most from the infamous Stuxnet attack, Indonesia, India, Azerbaijan, the United States, and Pakistan were also affected. Compared to these other countries, though, Iran seemed to be the prime target of this malicious computer warm (Bicakci, 2014). Neither NATO nor any of its member states faced severe harm from this attack, but similar methods could be used against the alliance. Ralph Langner, who is a German control system security consultant, delivered a TED talk, “Cracking Stuxnet, A 21st-century Cyber Weapon,” in 2011 about his analysis of the Stuxnet attack. Worldwide-recognized consultant Langner (2011) described the concept behind the attack.

> The idea behind the Stuxnet computer worm is actually quite simple. We do not want Iran to get the bomb. Their major asset for developing nuclear weapons is the Natanz uranium enrichment facility. … Now if we manage to compromise these systems [real-time control systems] that control drive speeds and valves, we can actually cause a lot of problems with the centrifuge. The gray boxes don’t run Windows software; they are a completely different technology. But if we manage to place a good Windows virus on a notebook that is used by a maintenance engineer to configure this gray box, then we are in business. And this is the plot behind Stuxnet.

Thanks to the Stuxnet cyber weapon, Iran had to delay its nuclear program, and developers of Stuxnet accomplished their mission (Langner, 2011). Before his six months of research on Stuxnet, the only thing that Langner and his team knew was that the Windows part of Stuxnet was very complex, and “the dropper part, used multiple zero-day vulnerabilities.” After some research, they realized that this was a directed attack. Depending on the configuration of the system, Stuxnet either infects seriously and harms the system, or stays passive and does nothing at all. On the other hand, Langner and his team also figured out that professionals who had complete insider information designed the Stuxnet. “They [Stuxnet creators] knew all the bits and bytes that they had to attack.” Obviously, the designers knew every detail about the operators (Langner, 2011).

Jeffrey S. Caso (2014) notes that similar to how a virus physically penetrates the human body, Stuxnet infiltrates a digital system through a flash drive. This “malware, rumored to have been created by the U.S. and Israeli governments, infects all computers” that operate on Windows. Siemens, as a software firm, structured control systems used in Iran to control centrifuges of nuclear plants. Stuxnet is configured to gain “control of the Siemens system’s logic controllers, and force the centrifuges to spin at high speeds until they self-annihilate—all while manipulating the feedback mechanisms into reporting that all is normal” (p. 255).

The experts who wrote the *Tallinn Manual* could not reach consensus on whether the Stuxnet case was an armed attack or not; however, they agreed that the attacks created an illegal use of force (Caso, 2014). Langner (2011) asserts that if an agent could use traditional worm technology to spread the Stuxnet worm as wide as possible, that agent could construct “a cyber weapon of mass destruction.” Stuxnet significantly affected Iran, more specifically, the Natanz uranium enrichment facility. However, most of targets, which are prone to future attacks that may follow Stuxnet’s method, are in the United States, Europe, and Japan (Langner, 2011). Considering members of NATO, the alliance should be ready for this kind of attack, and NATO and its individual members should begin to prepare immediately.

5. Ukraine (2014)

For centuries, Crimea has been an arena for political and military struggles. Due to Crimea’s strategic and geopolitical significance, the conflicts have been very severe and bloody, like the Crimean War between 1853 and 1856, where the biggest empires of the time fought one of the most critical wars in the modern history. The most recent crisis started in March 2014, with Russia’s annexation of Crimea, which was a Ukrainian territory. This happened when Ukraine was going through civil unrest caused by pro-Russian demonstrations. The conflict soon migrated to the cyber realm, and pro-Russian

hackers started disrupting Ukrainian communication and media networks early in the conflict.

Tony Vegue (2015) outlines some major incidents regarding the timeline of the attacks against Ukraine. In February 2014, telecommunication facilites and fiber optic cables were damaged by armed men who infiltrated into the complex. In the same month, hackers started a campaign against NATO and Ukrainian media agencies by launching DDoS attacks. To create confusion and mistrust in the public during the Ukrainian elections held in October 2014, election committee websites were targets of DDoS attacks by pro-Russian hackers (Vegue, 2015).

The Kremlin has made substantial investments in information operations as part of its strategy in Ukraine (Geers, 2015). As Kenneth Geers (2015) notes, cyber-attacks against Ukraine have included “cyber espionage, prepping the battlefield, selective telegraphing of capabilities, and some hints at destructive activities” (p. 67). According to Medvedev (2015), a pro-Russian hacker group called CyberBerkut stated that they had interfered in the Ukrainian elections, defaced several German websites, prevented many military cooperation documents to be communicated between the United States and Ukraine, blocked government websites and media outlets of NATO and Ukraine, and did black propaganda on various platforms. There were also other cyber-attacks committed by other pro-Russian groups, such as leaking private calls of government officials, releasing critical documents and information about political and military decisions, and blocking phone service (Medvedev, 2015). The sophistication level of the attacks varied from low level to high level; therefore, the measures to defend against these attacks changed due to the different features of the attacks being faced (Geers, 2015).

Like in the cases of Estonia and Georgia, the Ukrainian case has no clear evidence identifying the state actor behind the cyber-attacks. However, it was again very obvious that all of the cyber campaigns and attacks served Moscow’s strategic and operational goals. Therefore, Ukraine’s head of counterintelligence,

Vitaly Naida stated, “We consider that there is only one country in the world that would benefit from these attacks, and this is Russia” (Coker & Sonne, 2015, para. 10). However, Dmitry Peskov, who is the Kremlin’s spokesperson, denied all of the accusations and noted that many hacker groups also attack Russian computer systems regularly (Coker & Sonne, 2015). Even though Russian government officials reject any accusations, their denials of their role in the attacks started to lose credibility with the recent incidents.

Hybrid war concepts have been shown to be very effective and promising in recent international conflicts. Medvedev (2015) has acknowledged that “cyber operations conducted by Russian surrogates have undermined Ukrainian state legitimacy, embarrassed NATO allies, and intimidated opposition forces” (p. 26). Therefore, states, as individual actors, and collective defense mechanisms like NATO need to take more serious measures to defend themselves in the cyber domain.

6. Other Cyber Incidents

In addition to the significant cyber cases mentioned previously, many other cyber operations have been conducted by various actors to reach different goals. Andress and Winterfeld (2014) provide a cyber timeline in their book; however, when it comes to comparing this cyber timeline with *Wikipedia*’s (“Timeline of Computer Viruses and Worms,” 2016), there are some mismatches—especially in virus and worm related information. Omitting the controversial asides, a shorter list of the significant events that Andress and Winterfeld (2014) provided in their timeline appears here:

> 1999 Melissa virus unleashed.
>
> 1999 NATO accidentally bombs the Chinese embassy in Belgrade, spawning a wave of cyber-attacks from China against U.S. government websites.
>
> 2001 Code Red worm hit—designed to conduct DDoS against White House.
>
> 2003 Titan Rain attacks identified, believed to be from China; it spawns new term “Advanced Persistent Threat”

2007 Storm Worm (one of the first botnets) began infecting thousands of (mostly private) computers in Europe and the United States

2007 British Security Service, French Prime Minister's Office, and Office of the German Chancellor all complained to China about intrusion on their government networks.

2008 Databases of both the Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

2008 The networks of several congressional offices were hacked by unknown foreign intruders (some incidents involved offices with an interest in human rights or Tibet).

2009 Ghost Net report released by Canadian researchers who found espionage tools they attributed to China implanted on government networks of 103 countries.

2009 Reports in the press suggest that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran.

2009 Reports reveal that hackers downloaded data about the F-35 Joint Strike Fighter, a multibillion-dollar high-tech fighter jet.

2010 Operation Aurora in which Google publicly reveals being hacked (China blamed).

2010 WikiLeaks released U.S. embassy cables; Anonymous attacks MasterCard for no longer accepting donations for them.

2010 China redirected 15 percent of Internet traffic through its country (claimed it was an accident); this showed DNS weaknesses.

2011 Rivest-Shamir-Adleman (RSA) attack allowed its security tokens to be compromised (used by government, Department of Defense (DOD) contractors, and financial organizations to name a few); China suspected.

2011 Duqu (son of Stuxnet) discovered.

2011 Global Energy Cyber-attacks "Night Dragon" report released showing systematic economic espionage against energy sector companies; China suspected.

2012 Anonymous attacks Sony multiple times causing impact on gamers.

2012 Flame and Gauss state-sponsored cyber exploit discovered—tied to Stuxnet.

> 2012 Shamoon attack against Saudi Aramco, one of the world's largest oil conglomerates, resulted in more than 30,000 computer systems being wiped of all data.
>
> 2013 South Korean banks and media report large number of computer network crashes causing speculation of North Korea cyber-attack. (pp. 291–295)

This cyber timeline covers cases until 2013, but many other cases have been reported by the media since then. To illustrate, three cyber-attacks are worth mentioning: cyber-attacks against a German steel mill and Sony Pictures in 2014 and the Ukrainian power grid attack in 2015.

D. SUMMARY

As an intergovernmental military alliance, NATO is under various cyber threats. In general, scholars classify cyber threats into four categories: cybercrime, cyber espionage, cyberterrorism, and cyber warfare. There are two types of cyber actors, who may pose as threats to NATO: state actors and non-state actors. Intelligence services and armed forces are considered as state actors. Non-state actors can be categorized as individual actors, corporations, cyber terrorists, and organized cybercrime actors.

Various cyber actors have been conducting numerous cyber operations, and many of these incidents have a direct or indirect relation with NATO. Among the significant cases, during the Serbian-NATO Conflict, NATO was confronted with activist and hacktivist activities in cyberspace. In the Estonia case, the actors mainly used DoS and DDoS attacks as well as website defacements. In 2008, during the conflict between Georgia and Russia, cyber actors used three main methods against Georgia: webpage defacements, SQL injections, and DDoS attacks. In 2010, the Stuxnet case showed that a computer worm can cause physical damage to critical infrastructure. In 2014, Ukraine suffered from various cyber-attacks, such as distrupting cellular phones, campaigning against media agencies by DDoS attacks, and creating mistrust of the October 2014 Ukrainian elections by sophisticated cyber-attacks against official websites.

Consequently, these significant cyber cases show that similar methods can be used in different cyber-attacks, and unique tactics can be implemented for the first time to conduct a successful cyber operation. Other cyber cases and recent developments reveal that cyber actors may continue to use conventional methods, and these attackers may also transform the previous tactics into unprecedented ones. The next question is what policies has NATO implemented to fight against cyber threats?

IV. NATO POLICIES TO FIGHT AGAINST CYBER THREATS

As discussed in the previous chapter, NATO's new focus on cyber defense stems from the 1999 Kosovo conflict when the pro-Serbian cyber attackers tried to impair the communication infrastructure of the alliance (Burton, 2015). According to the official webpage of NATO (2016f), cyber threats and aggressions "are becoming more common, sophisticated and damaging." NATO faces a very complex and evolving threat environment. A part of military operations, both state and non-state actors can effectively conduct cyber operations. Recent developments have shown that cyber operations are part of hybrid warfare (NATO, 2016f).

According to Jeffrey L. Caton (2016), the improvement of cyber defense capabilities for NATO "has been making steady progress since its formal introduction at the North Atlantic Council Prague Summit in 2002" (p. 1). Between this summit and the 2016 Warsaw Summit, NATO members agreed on important decisions in terms of cyber defense. Bolstered by various and numerous cyber-attacks "such as those in Estonia in 2007," NATO's priorities were "formalized in subsequent NATO cyber policies that were adopted in 2008, 2011, and 2014" (Caton, 2016, p. 1). NATO and its members aim to depend on sound and resilient cyber security to accomplish "the Alliance's core tasks of collective defence, crisis management and cooperative security" (NATO, 2016f).

A. EVOLUTION

Organizations and institutions evolve throughout time as they face new and different challenges. In terms of cyber threats, NATO has experienced significant evolution and transformation in its structure, policies, and doctrines. The decisions made and actions taken in the summits of the North Atlantic Council (NAC) are good representations and reflections of tracking the evolving progress of NATO's cyber policy. The following subsections examine the 2002 Prague Summit, the 2006 Riga Summit, the 2008 Bucharest Summit, the 2009

Strasburg-Kehl Summit, the 2010 Lisbon Summit, the 2012 Chicago Summit, the 2014 Wales Summit, and the 2016 Warsaw Summit from the perspective of cyber defense.

1. Prague Summit (2002)

The 2002 Prague Summit was the first place where cyber defense appeared in the political agenda of NATO, even though the organization had taken several measures to defend its information and communication capabilities before this summit (NATO, 2016f). In the NATO press releases of the Prague Summit Declaration, the cyber defense issues were expressed as follows:

> Effective military forces, an essential part of our overall political strategy, are vital to safeguard the freedom and security of our populations and to contribute to peace and security in the Euro-Atlantic region. We have therefore decided to: … strengthen our capabilities to defend against cyber-attacks. (para. 4)

In this summit, numerous measures were taken to fight against terrorism and strengthen NATO's capabilities because of the 9/11 attacks. This included measures in the cyber domain as well. Member countries collectively decided to form the NATO Computer Incident Response Capability (NCIRC), and they established the NATO Cyber Defense Program as an institutional development for responding to threats in the cyber domain (Caton, 2016). The NATO Communications and Information Agency (NCIA) and NCIRC serve to provide an integrated and constant cyber defense for the alliance's information and communication infrastructure in accordance with the Cyber Defense Program. Over time, the capabilities and the capacity of the NCIRC have evolved to meet the requirements of current technological advances and the complexity of cyber threats.

2. Riga Summit (2006)

Although there were attempts and initiatives for making progress in cyber defense after the Prague Summit, the issue did not come up again in the formal meetings of the NAC until the Riga Summit in 2006. In the NATO (2006) press

releases of the Riga Summit Declaration, the cyber defense issues were expressed as follows:

> The adaptation of our forces must continue. We have endorsed a set of initiatives to increase the capacity of our forces to address contemporary threats and challenges. These include: work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber-attack. (para. 24–29)

The leaders of the member countries had agreed in this summit to provide further protection for the information systems of NATO (NATO, 2016f). It was emphasized that efforts for advancing NATO's cyber security should be continued and increased (Burton, 2015). It was also stated that the NATO Network Enabled Capability could serve as a means to share information in the operations of NATO and improve cyber defense of the organization (Caton, 2016).

3. Bucharest Summit (2008)

The cyber-attacks against the private and public institutions of Estonia in 2007 were a wake-up call for NATO. After this incident, defense ministers of the member countries agreed to work on the issue of cyber defense urgently. In response to this case, the first policy on cyber defense was approved by NATO in early 2008. The conflict between Georgia and Russia had also proven to the alliance that cyber capabilities could be used in combination with conventional warfare (NATO, 2016f). In the 2008 Bucharest Summit, the member states agreed that the relationship between NATO and the national authorities on cyber defense should be enhanced, the experiences of the member states regarding cyber issues should be shared, and the states should assist each other when required. In the NATO press releases of the Bucharest Summit Declaration, the cyber defense issues were expressed as follows:

> NATO remains committed to strengthening key Alliance information systems against cyber-attacks. We have recently adopted a Policy

> on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasizes the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber-attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities. (para. 47)

In summary, the key tenets of NATO's cyber policy after the Bucharest Summit were to "emphasize protection of key information systems"; "share best practices for cyber defence"; "develop capability to assist Allied nations, upon request, to counter cyber-attack"; "develop NATO's cyber defence capabilities"; and "strengthen linkage between NATO and national authorities" (Caton, 2016, p. 7).

4. Strasburg-Kehl Summit (2009)

There were two significant developments after the Bucharest Summit. The first was the establishment of the NATO Cyber Defense Management Authority for the purpose of centralizing cyber defense capacity under one authority in order to increase the operational capability. Second was the activation of the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Estonia (Bicakci, 2014). In the 2009 Strasburg-Kehl Summit, leaders decided to improve their Computer Incident Response Capability as well. In the NATO press releases of the Strasburg-Kehl Summit Declaration, the cyber defense issues were expressed as follows:

> We remain committed to strengthening communication and information systems that are of critical importance to the Alliance against cyber-attacks, as state and non-state actors may try to exploit the Alliance's and Allies' growing reliance on these systems. To prevent and respond to such attacks, in line with our agreed Policy on Cyber Defence, we have established a NATO Cyber Defence Management Authority, improved the existing Computer Incident Response Capability, and activated the Cooperative Cyber Defence Centre of Excellence in Estonia. We will accelerate our cyber defence capabilities in order to achieve full readiness. Cyber defence is being made an integral part of NATO exercises. We are

> further strengthening the linkages between NATO and Partner countries on protection against cyber-attacks. In this vein, we have developed a framework for cooperation on cyber defence between NATO and Partner countries, and acknowledge the need to cooperate with international organizations, as appropriate. (para. 49)

In 2009, the NATO Parliamentary Assembly issued a detailed report called *NATO and Cyber Defense,* which discusses critical issues in the cyber domain relating to NATO (Caton, 2016). NATO had made significant policy implementations and institutional developments in order to protect itself against cyber threats within a couple of years after experiencing serious incidents in the cyber domain. The organization also pursued a strategy to enhance its members' cyber security through both coordinating measures and deterrence.

5. Lisbon Summit (2010)

At the 2010 Lisbon Summit, NATO introduced a new strategic concept, and announced that NAC had been tasked to develop a detailed cyber defense policy and come up with an action and implementation plan for this policy (NATO, 2016f). This new concept and policy aimed to strengthen protection of NATO's communication and information systems against advanced cyber threats (Alexander, 2014). In the NATO press releases of the Lisbon Summit Declaration, the cyber defense issues were expressed as follows:

> Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber-attack against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralized cyber protection. We will use NATO's defence planning processes in order to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimize information sharing, collaboration and interoperability. To address the security risks

> emanating from cyberspace, we will work closely with other actors, such as the United Nations (UN) and the European Union (EU), as agreed. We have tasked the Council to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyber defence policy by June 2011 and to prepare an action plan for its implementation. (para. 40)

The new strategic concept, called *Active Engagement, Modern Defense,* delineates the purpose of NATO, critical security missions of the alliance, and the future security environment (Caton, 2016). It also addresses how military forces need to adapt themselves in accordance with the new strategic concept. In the history of NATO, there had only been six strategic concepts before this one. They were all related to the Cold War and post-Cold War security considerations. The new concept focuses on three fundamental tasks: "collective defense, crisis management, and cooperative security" (Caton, 2016, p. 5). The new strategy recognizes that the future security environment will include more complex, frequent, organized, and costly cyber-attacks. The attacks will not necessarily come from states, but could also come from criminal or terrorist groups that threaten the alliance. Therefore, NATO continuously needs to update its defense and deterrence posture. The strategic concept of *Active Engagement, Modern Defense* (2010) states,

> We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. Therefore, we will…develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations. (para. 19)

After the Lisbon Summit, NATO defense ministers endorsed a new policy on cyber defense that includes an associated implementation and action plan for the new threat environment in the cyber domain in order to achieve a well-coordinated effort throughout the alliance (NATO, 2016f). The key tenets stated in "Defending the Networks: The NATO Policy on Cyber Defense" (2011) are

“integrate cyber considerations into NATO structures and planning processes in order to perform NATO’s core tasks of collective defence and crisis management”; “focus on prevention, resilience, and defence of critical cyber assets to NATO and Allies”; “develop robust cyber defence capabilities and centralize protection of NATO’s own networks”; “develop minimum requirements for cyber defence of national networks critical to NATO’s core tasks”; “provide assistance to the Allies to achieve a minimum level of cyber defence and reduce vulnerabilities of national critical infrastructures”; and “engage with partners, international organizations, the private sector and academia” (p. 1).

One of the most important issues raised in the Lisbon Summit was the call for NATO to work and cooperate more closely with the European Union (EU) on cyber defense issues (Caton, 2016). International organizations like NATO and the EU are likely targets for cyber-attacks. Therefore, cyber security is a significant aspect of the organizations’ and their member countries’ defense. The cooperation between NATO and the EU in the cyber domain could provide significant advantages for both organizations (Caton, 2016).

Although there was a clear call at the Lisbon Summit for the integration of the cyber dimension into the structure of NATO, the actual process has not been as consistent and rapid as desired (Caton, 2016). For instance, FOC could only be achieved in 2014 at a cost of $74.5 million even though it was pushed after the Lisbon and Chicago Summits in 2010 and 2012, respectively. One of the leading managers of the project has said that “full operational capability is perhaps a misnomer—cyber threats are constantly evolving, and we [NATO] will never have a final or full capability” (Caton, 2016, p. 34). Currently, the FOC provides an enhanced cyber security to the 55 NATO sites all around the world.

6. Chicago Summit (2012)

At the Chicago Summit, leaders of the member states reiterated their commitment to enhance the cyber security of NATO’s information and communication systems under a centralized defense structure with some

upgrades to NCIRC (NATO, 2016f). In the NATO press releases of the Chicago Summit Declaration, the cyber defense issues were expressed as follows:

> Cyber-attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyber defence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which [is] now being implemented. Building on NATO's existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, will be in place by the end of 2012. We have committed to provide the resources and complete the necessary reforms to bring all NATO bodies under centralized cyber protection, to ensure that enhanced cyber defence capabilities protect our collective investment in NATO. We will further integrate cyber defence measures into Alliance structures and procedures and, as individual nations, we remain committed to identifying and delivering national cyber defence capabilities that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from cyber-attacks. To address the cyber security threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organizations, inter alia the EU, as agreed, the Council of Europe, the UN and the Organization for Security and Cooperation in Europe (OSCE), in order to increase concrete cooperation. We will also take full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia. (para. 49)

At the Chicago Summit, NATO decided to adopt a new Cyber Defense Policy, concept, and action plan (Caton, 2016). The improvement of cyber defense capabilities of NATO was reemphasized by the implementation of more developed procedures and structures for interoperability and collaborative purposes. Collaboration among the member states in the alliance is vital for the success of the new cyber defense policies and concepts. It helps states' cyber systems reach certain standards that reinforce the alliance's overall cyber security. The collaboration could be accomplished by building situational awareness, optimized information sharing, and reliable interoperability under agreed upon and shared standards among member countries. The cooperation

with other international organizations like the EU, the UN, and OSCE was highlighted again in the Chicago Summit.

There were some other developments between the Chicago and Wales Summits. In 2014, allied defense ministers were charged with developing a new Cyber Defense Policy, NAC changed the name of the Defense Policy and Planning Committee/Cyber Defense to Cyber Defense Committee, and NCIRC FOC was achieved with an improved protection of NATO's information systems and networks (NATO, 2016f).

7. Wales Summit (2014)

Allied countries approved a new Cyber Defense Policy and action plan at the 2014 Wales Summit. The policy and action plan are being reviewed by the member countries to determine if they meet the technical and political requirements for the current cyber threat environment (NATO, 2016f). In the NATO (2014b) press releases of the Wales Summit Declaration, the cyber defense issues were addressed:

> As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis. (para. 72)

The press release describing the declaration of NATO's stance on cyber defense continues:

> We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. We will improve the level of NATO's cyber defence education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO Communications and Information Systems (CIS) School and other NATO training and education bodies. (para. 73)

At the Wales Summit, NATO emphasized the significance of close relationships with industry and restated the importance of cooperation with the other international organizations like the EU. The role of training, education, and exercise for the cyber defense of the alliance was noted and the efforts for development in this field were approved. The NATO Industry Cyber Partnership (NICP) was endorsed at the Wales Summit as an initiative to increase cooperation between the private sector and NATO on cyber challenges and threats. A two-day conference about cyber collaboration took place in Belgium that hosted more than a thousand industry leaders and policy makers. NICP understands that a successful cyber defense of the alliance depends on strong communication and collaboration between private industry and NATO (NATO, 2016f). For the purpose of preventing and responding to cyber-attacks, the EU

and NATO made a technical arrangement on cyber security. This arrangement between the Computer Emergency Response Team of the European Union (CERT-EU) and NCIRC enables them to share information, experiences, practices, and knowledge about cyber-related issues.

8. Warsaw Summit (2016)

Cyberspace was recognized as the fifth domain of operations at the 2016 Warsaw Summit, adding to the existing domains of land, sea, air, and space (NATO, 2016f). However, recognition of this new domain does not alter the defensive mission of NATO. The alliance is still constrained to act by international law in every domain. Since most of the current crises and conflicts involve cyber elements, treating cyberspace as a new domain offers advantages and flexibility for NATO's operations and missions. In the NATO (2016c) press releases of Warsaw Summit Declaration, the cyber defense issues were expressed as follows:

> Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success. Furthermore, it will ensure more effective organization of NATO's cyber defence and better management of resources, skills, and capabilities. This forms part of NATO's long term adaptation. We continue to implement NATO's Enhanced Policy on Cyber Defence and strengthen NATO's cyber defence capabilities, benefiting from the latest cutting edge technologies. We reaffirm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable. We will continue to follow the principle of restraint and support maintaining international peace, security, and stability in

> cyberspace. We welcome the work on voluntary international norms of responsible state behaviour and confidence-building measures regarding cyberspace. (para. 70)

The press release describing the declaration of NATO's stance on cyber defense continues:

> We will ensure that Allies are equipped for, and meet requirements tailored to, the 21st century. Today, through our Cyber Defence Pledge, we have committed to enhance the cyber defences of our national networks and infrastructures, as a matter of priority. Each Ally will honor its responsibility to improve its resilience and ability to respond quickly and effectively to cyber-attacks, including in hybrid contexts. Together with the continuous adaptation of NATO's cyber defence capabilities, this will reinforce the Alliance's cyber defence. We are expanding the capabilities and scope of the NATO Cyber Range, where Allies can build skills, enhance expertise, and exchange best practices. We remain committed to close bilateral and multilateral cyber defence cooperation, including on information sharing and situational awareness, education, training, and exercises. Strong partnerships play a key role in effectively addressing cyber challenges. We will continue to deepen cooperation with the EU, as agreed, including through the on-going implementation of the Technical Arrangement that contributes to better prevention and response to cyber-attacks. We will further enhance our partnerships with other international organizations and partner nations, as well as with industry and academia through the NATO Industry Cyber Partnership. (para. 71)

The partnership with the EU was reemphasized at the Warsaw Summit, together with cooperation with private industry through NICP. By introducing the Cyber Defense Pledge, NATO aimed to strengthen the nation states' networks and infrastructure for reinforcing the overall resilience and cyber defense of the organization (NATO, 2016f).

B. GOVERNANCE

In the previous section, several summits were discussed and analyzed in terms of cyber defense. This section focuses on cyber defense policy updates in 2008, 2011, and 2014. Moreover, hierarchical responsibilities of various bodies in NATO are reviewed to better understand the governance of cyber defense.

1. Cyber Defense Policy Updates

Caton (2016) notes that "[a]n initial NATO Cyber Defence Policy was adopted at the 2008 NATO NAC Summit in Bucharest" (p. 6). Later, this policy was updated after the 2010 Lisbon and 2014 Wales summits. Focusing on "key tenets of NATO Cyber Policy," in 2008, the policy highlighted protection of critical information systems, development of capability to support allies, and strong ties between NATO and national officials (Caton, 2016, p. 7).

In 2011, the cyber defense policy aimed to "integrate cyber defence considerations into NATO structures and planning processes" to implement NATO's main tasks of "collective defence and crisis management." Another goal was to develop strong cyber defense capabilities especially for critical cyber assets and to centralize security of NATO's own networks. Furthermore, assisting members to reach a minimum level of cyber defense and engaging with allies, international organizations, the private sector and academic world were other objectives of the policy (Caton, 2016, p. 7).

In 2014, in addition to the 2011 updates, the policy focused on fundamental cyber defense responsibility, which was to protect its own networks, but at the same time assumed responsibility to help allies to develop their national networks. Besides, NATO acknowledged that international law applies to cyber operations and confirmed that "cyber defense is part of NATO's collective defense under Article 5" (Caton, 2016, p. 8).

The initial version of the policy provided some of the basic elements for future policies and started the process of centralizing NATO efforts in cyberspace through institutions such as the Cyber Defense Management Authority (CDMA). The mission of The CDMA was "to initiate and coordinate cyber defenses, review capabilities, and conduct appropriate risk management" (Caton, 2016, p. 6). Although publicly available information is limited, the CDMA is believed to have "real-time electronic monitoring capabilities for pinpointing threats and sharing

critical cyber intelligence in real-time," with the aim of ultimately "becoming an operational war" institution for cyber security (Hathaway et al., 2012, p. 862).

2. Hierarchical Responsibilities in Governance

The NATO Policy on Cyber Defense is carried out by "political, military and technical authorities" of NATO, as well as by alliance members (NATO, 2016f). As Caton (2016) notes, "The 2011 NATO Cyber Defence Policy followed the adoption of the new NATO Strategic Concept" and thus concentrated on methods to enhance NATO's collective capacity to block, detect, "defend against and recover from cyber-attacks" (p. 7). On the other hand, the 2011 policy also built "a cyber defense governance with a hierarchy that flowed from the NAC to the Defence Policy and Planning Committee in Reinforced Format, then to the NATO Cyber Defence Management Board (CDMB), and finally to the NCIRC" (Caton, 2016, p. 7).

According to Caton (2016), the 2014 NATO Enhanced Cyber Defense Policy clarifies cyber governance mechanisms and formally connects cyber to the conventional and core collective defense task of NATO. However, alliance members are expected to guard their national networks, because the updated policy formulates that NATO is primarily responsible for guarding its own network systems (Caton, 2016, p. 8). "The NAC is apprised of major cyber incidents and attacks" (NATO, 2016f), as it is the responsible body that provides "strategic-level oversight and exercises principal authority in cyber defence-related crisis management" (Caton, 2016, p. 8).

Another key element of NATO cyber governance is the Cyber Defense Committee, previously named the Defense Policy and Planning Committee/Cyber Defense, and "subordinate to the NAC." It serves as "the lead committee for political governance and cyber defence policy in general, providing oversight and advice to Allied countries on NATO's cyber defence efforts at the expert level" (Caton, 2016, p. 8). When it comes to the working level, the NATO CDMB is mainly responsible for cyber security coordination among both "NATO

civilian and military bodies." The CDMB charges "the leaders of the policy, military, operational and technical bodies in NATO" with responsibilities for cyber defense (Caton, 2016, p. 9).

The NATO Consultation, Control and Command Board establishes the primary "committee for consultation on technical" and application aspects of cyber defense (NATO, 2016f). The NATO Military Authorities and NATO Communications and Information Agency (NCIA) carry the distinct responsibilities for detecting "the statement of operational requirements, acquisition, implementation and operating of NATO's cyber defence capabilities." Allied Command Transformation deals with the planning and implementation of the yearly Cyber Coalition Exercise (NATO, 2016f).

In a general overview, Caton (2016) summarizes the NCIRC development progress as follows:

> The effort will be implemented in several increments and will include an upgraded capability to identify, trap and analyze malware and cyber-attacks launched against alliance systems; advanced sensors to provide improved early detection of threats against NATO networks; a consolidated information assurance picture that will give operators an overview of the situation across NATO networks, including a dynamic risk assessment; and an upgraded and advanced threat assessment capability. (p. 49)

Finally, the NCIRC Technical and Coordination Centers are two critical bodies in terms of cyber defense efforts in NATO. According to the official webpage of NATO, NCIA, "through its NCIRC Technical Centre in Mons, Belgium," is in charge of "the provision of technical" services of cyber defense throughout the alliance. The NCIRC Technical Center has a crucial role in reacting to all cyber-attacks against NATO. This center also deals with and reports incidents, and distributes critical information from incident to system/security managers and users (NATO, 2016f). As a staff element, the NCIRC Coordination Center's responsibility is the organization of cyber defense actions in NATO and with the organization members, and for personnel "support to the CDMB" (NATO, 2016f).

C. SUMMARY

Focusing on policy development and governance, NATO has acknowledged that cyber security is part of collective defense and confirmed that international law should be applied in cyberspace. In 2016, Alliance members reaffirmed that they recognize cyberspace as a new domain of operations in addition to air, land, sea, and space. Allies are responsible for the security of their own networks, but at the same time, their systems are required to be compatible with those of other members and NATO. NATO develops its capacity for cyber-related "education, training and exercises." Allies are responsible for information sharing and cooperation in blocking, alleviating, and restoring from cyber-attacks. In February 2016, to develop better cyber defense cooperation, NATO signed a Technical Arrangement with the EU. Lastly, NATO intensifies "its cooperation with industry," by means of the NATO Industry Cyber Partnership (NATO, 2016f).

Nevertheless, Caton (2016) raises the question "how would this governance process be applied to determine the appropriate response to any perceived aggression in cyberspace against NATO" or its members (p. 9)? The steps for engagement start at the technical level, and if an event has political significance, "NATO's cyber defense efforts get elevated from the NCIRC to the CDMB and Cyber Defence Committee through to the NAC" (p. 9). The NAC would "determine the appropriate level of response," to that point of "invoking collective defense through Article 5 of the NATO Charter, although this is considered unlikely unless there is significant physical damage or deaths involved" (Caton, 2016, p. 9). Professor Michael Schmitt, "the best-known proponent of the effects-based approach for determining when a cyber-attack should be considered an armed attack," notes that effects of a cyber-attack should be evaluated by reference to six factors[2] (Hathaway et al., 2012, p. 848).

[2] These are severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.

However, these factors are not binding for NATO and other states, nor are they easy to measure. Therefore, arriving at a consensus on whether a cyber-attack should be considered as an armed attack is difficult at best.

In conclusion, under rules of international law, “the NATO charter and the United Nations charter there remains general ambiguity as to exactly how an incident in cyberspace may be considered an act of war” (Caton, 2016, p. 9). Cyber defense policies show that NATO does not prefer to define what kind of attacks against the alliance require collective defense and maintains ambiguity policy by evaluating cyber incidents case by case. Under these circumstances, NATO has developed cyber defense policies and implements them in coordination with all members. The question is whether these policy enhancements and applications are enough to meet cyber threats against the NATO alliance, or whether further measures are needed.

THIS PAGE INTENTIONALLY LEFT BLANK

V. POLICY RECOMMENDATIONS TO RESPOND CYBER THREATS

Even though NATO faced serious attacks during the Kosovo Conflict, it is obvious that NATO and member states did not take their lessons and prepare for more serious cyber threats. The fact that NATO declarations after the 2004 Istanbul and 2005 Brussels Summits did not even mention any cyber issues (Caton, 2016, p. 85) suggests that NATO ignored cyber defense in those years. Estonia was a NATO member when it was targeted in the 2007 cyber-attacks; yet, the alliance was not in a position to defend Estonia collectively even if it had been asked. A wake-up call from the Estonia case, however, urged NATO to establish the CCDCOE (Cooperative Cyber Defense Center of Excellence) in 2008 in Tallinn, Estonia. NATO CCDCOE serves as the headquarters for the alliance's cyber security concerns. The Estonia case demonstrated to NATO that as an alliance it did not have sufficient capability and presence in this domain to ensure the protection of its member countries in cyberspace (Herzog, 2011).

The cyber threat landscape rapidly changes, and NATO needs to maintain a strong cyber defense. Especially after the Wales Summit in September 2014, the organization has made decisive steps to show that robust defense in cyberspace is an important part of the "NATO's core task of collective defense" (NATO, 2016f). In coordination with this mindset, NATO has developed cyber defense policies and executes them with assistance of all members.

The main focus of this chapter is answering whether the policy enhancements and applications are sufficient to meet cyber threats against the NATO alliance, or whether further measures are required. After providing details about the Cyber Defense Pledge, which was signed at the Warsaw Summit in 2016, the chapter describes and evaluates NATO's cyber policies and operations in eight areas. For each area, it offers recommendations for continuing or strengthening the current approach.

A. CYBER DEFENSE PLEDGE

NATO members pledged at the Warsaw Summit in 2016 to bolster and develop the cyber defenses of their networks and infrastructures. Each member will deem “its responsibility to enhance its resilience and capability” to react swiftly and “effectively to cyber-attacks, including in hybrid” forms (NATO, 2016f). NATO’s official cyber defense pledge text is shown here:

> Cyber Defense Pledge (2016)
>
> 1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.
>
> 2. We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.
>
> 3. We welcome the work of Allies and the EU on enhancing cyber security, which contributes to reinforcing resilience in the Euro-Atlantic region, and we support further NATO – EU cyber defence co-operation, as agreed. We reaffirm the applicability of international law in cyberspace and acknowledge the work done in relevant international organisations, including on voluntary norms of responsible state behaviour and confidence-building measures in cyberspace. We recognise the value of NATO’s partnerships with partner nations, industry and academia, including through the NATO Industry Cyber Partnership.
>
> 4. We emphasise NATO’s role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.
>
> 5. We, Allied Heads of State and Government, pledge to strengthen and enhance the cyber defences of national networks and

infrastructures, as a matter of priority. Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long-term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance. We will:

I. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks;

II. Allocate adequate resources nationally to strengthen our cyber defence capabilities;

III. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices;

IV. Improve our understanding of cyber threats, including the sharing of information and assessments;

V. Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;

VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;

VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.

6. To track progress on the delivery of our Pledge, we task an annual assessment based on agreed metrics, and we will review progress at our next summit. (NATO, 2016e)

B. EVALUATION AND RECOMMENDATIONS FOR SPECIFIC AREAS

Considering the cyber defense pledge, an evaluation of and recommendations for NATO's cyber defense policies are discussed under eight specific areas: cooperation with the European Union; relations with business enterprises; information sharing among members; education, training, and exercises; capabilities of NCIA; critical infrastructure protection; cyber law and legislature; and collective cyber defense (Article 5).

1. Cooperation with the European Union (EU)

This section comprises evaluation of and recommendations for NATO's cooperation with the European Union.

a. Evaluation

Besides NATO, the EU has also identified cyber issues as one of the crucial threats and challenges it faces (Homan, 2014). The majority of member states of the EU have some sort of national intentions to defend critical networks and to react to cyber threats (Homan, 2014). The European Cyber Security Strategy has three goals: "to strengthen the security and resilience of networks and information security systems, to prevent and fight cybercrime, and to establish a more coherent cyber security policy across Europe" (Homan, 2014).

The cross-border nature of cyber threats necessitates focus on powerful international cooperation (Homan, 2014). NATO cooperates with pertinent countries and organizations to develop international cyber security (NATO, 2016f). NATO states that "requests for cooperation with the Alliance are handled on a case-by-case basis founded on mutual interest" (NATO, 2016f). NATO cooperates with "the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE)" (NATO, 2016f).

The 2010 Lisbon Summit Declaration urges NATO to work more jointly with the EU in the field of cyber defense. Of the 28 NATO members, "all but Albania, Canada, Iceland, Norway, Turkey, and the United States" are members of the EU (Caton, 2016, p. 30), and "these countries share common interests in security programs conducted by both organizations as well as the desire not to have unnecessary duplication of resource contributions" (p. 31). Considering cyber defense, both groups have analogous aims, but divergent approaches. Caton (2016) summarizes the analysis by Piret Pernik, researcher at the International Center for Defense Studies in Estonia:

> For both NATO and the EU, cyber security is a strategic issue that impacts the security and defence of member states and of the

> organisations themselves. They both prioritize the resilience and defence of their own networks, organisations and missions, leaving cyber security of individual members states a national responsibility. The missions of the two organisations are complementary, with NATO focusing on security and defence aspects of cyber security, and the EU dealing with a broader, mainly non-military range of cyber issues (Internet freedom and governance, online rights and data protection), and internal security aspects. (p. 31)

In February 2016, to enhance better cyber defense cooperation, NATO signed a Technical Arrangement with the EU (NATO, 2016f). Cooperation between NATO and the EU in areas such as critical infrastructure protection is crucial; however, unlike NATO, the EU does not give direct technical support to its members. Rather, the EU "facilitates information sharing through such organizations as the European Network and Information Security Agency (ENISA) and the European Defence Agency (EDA)" (Caton, 2016, p. 31). Other noteworthy differences between the EU and NATO are that the former does not have "its command and control information systems and it lacks the central authority for common cyber security, such as that found in the NAC" (p. 31).

b. Recommendations

The "political will in the EU to cooperate further with NATO on cyber defense" is an advantage to enhance strong and "resilient cyber defense capabilities" (Caton, 2016, p. 32). This is required within the EU Cyber Defense Policy Framework, which was adopted by the Council of the EU (p. 32). To avoid redundant duplication and establish "coherence and complementarity of efforts," in terms of cyber defense, NATO and the EU should have "regular staff-to-staff consultations, cross-briefings, as well as possible meetings between the Politico-Military Group and relevant NATO committees" (p. 32).

Both NATO and the EU point out that inadequate cyber security of a member state is a national liability. The EU does not have a central authority in charge of collective cyber defense, "while in NATO the top political decision-making body NAC exercises principal decision-making authority" and inspects

the development on NATO's cyber defense position (Caton, 2016, p. 78). Compared to the EU, NATO's structure is more sufficient to deal with cyber issues, and encouraging the EU to have similar responsible authorities will also boost the alliance's cyber defense.

The 2002 Prague Summit declaration shows that NATO was aware of cyber issues at the time. However, especially after the 2006 Riga Summit, NATO made serious steps in cyber defense development. In contrast, military cyber defense in the EU is at a relatively early stage of maturity (Homan, 2014). Considering that NATO and the EU have many common member states, both organizations should search for ways to reinforce links between them for cyber security issues.

Some states among these common members are relatively well developed in their technological competence and internal structures for dealing with cyber issues, while others are less advanced. Furthermore, "in terms of technical, legal and political harmonized measures, there are still significant differences between individual member states and EU institutions" (Homan, 2014), as it is the case in NATO alliance. Considering the proverb that a chain is only as strong as its weakest link, both NATO and the EU should find ways to develop their weaker members. In this aspect, NATO members signed the aforementioned Cyber Pledge, and NATO should encourage the EU and its members to adopt similar goals and promises. In this way, both organizations will have similar goals and approaches in terms of cyber defense.

2. Relations with Business Enterprises

This section comprises evaluation of and recommendations for NATO's relations with business enterprises.

a. Evaluation

For an effective cyber defense of NATO and its member countries, relations with private sector and business enterprises are crucial for exploiting

technological expertise and innovations in cyberspace (NATO, 2016f). NATO started a formal initiative in September 2014 to increase the cooperation efforts between NATO and the private sector on cyber challenges and threats. NATO and the allied countries are trying to improve and strengthen the relationship with private industry by the help of the NICP. NICP was presented to 1,500 policy makers and business leaders in the cyber conference held in 2014 in Mons, Belgium (NATO, 2014a). The partnership between NATO and the private sector is through existing structures of NATO and includes national Computer Emergency Response Teams, NATO allied countries' private sector representatives, and other NATO entities (NATO, 2016f).

There are many areas where NATO and industry work together, including education and training, information sharing activities, exercises, and multinational Smart Defense projects (NATO, 2016f). NICP's objectives are to "improve cyber security in NATO's defence supply chain," "raise mutual understanding and awareness of cyber threats and risks, including through information sharing;" "contribute to the Alliance's efforts in cyber defence education, training and exercises;" "improve sharing of best practices and expertise on preparedness and recovery;" and "help NATO and Allies to learn from industry" (NATO, 2014a, para. 4).

Another significant event for NATO and private industry cooperation was the Global Conference on Cyberspace held in The Hague, the Netherlands, in 2015. This conference helped government representatives, civil society, and the private sector to increase cooperation in cyberspace and improve cyber capabilities against any kind of cyber threat (NATO, 2015). The themes that dominated this conference were "building the trust to work collaboratively in order to understand cyber risks, raise situational awareness, and improve cyber protection;" "facilitating actionable information sharing between NATO and Industry;" and "advancing innovation by identifying the next cutting-edge cyber security solutions, promoting small business participation, and enabling application of most innovative technologies" (NATO, 2015, para. 3). The urgency

for advances in cooperation between NATO and business enterprises was emphasized in this conference, and enhancing cyber resilience, mitigating vulnerability against cyber threats, and improving incident handling were addressed as significant issues for a better cooperation (NATO, 2015).

A good example of how NATO builds partnerships with the private sector is the information sharing agreement with Leidos (NATO, 2016b). The agreement enables both parties to collaborate better and share non-classified information in a timely manner so that they can protect their information infrastructures and networks and enhance their situational awareness about cyber threats. This sharing will improve NATO's prevention and detection processes. Officials considered the agreement with Leidos as "an important part of the effort to bolster the Alliance's cyber defence posture through the NATO Industry Cyber Partnership (NICP)" (NATO, 2016b, para. 5).

Another important event for the NATO-Industry collaboration was the 2016 NATO C4ISR Industry Conference and AFCEA TechNet International (NITEC16) (NATO, 2016d). At this conference, the significance of building closer relationships and partnerships between NATO and private industry was reemphasized in order to stay ahead of cyber threats and deliver effective methods for the alliance's cyber defense (NATO, 2016d). The conference lasted for two days, with the first day dedicated to discussing the need for partnership, and the second, to discussing ways for building stronger collaboration and partnerships (NATO, 2016d).

b. Recommendations

The realization of the importance of NATO collaborating with private industry in cyberspace is a big step towards bolstering the alliance's cyber defense. Even though some efforts for cooperation with industry started earlier, the official initiative came with the establishment of NICP in 2014. Considering the seriousness of cyber threats and cyber-attacks against NATO, as discussed in previous chapters, this initiative could have been launched earlier.

The efforts through NICP helped the alliance to build very strong relationships with some enterprises in the industry. This brought a more scientific and civilian perspective to the cyber defense issues that increased the versatility of methods and ideas for protecting NATO's existence in cyber realm. However, these efforts do not seem adequate to integrate a very large organization like NATO with numerous successful enterprises in the industry. Therefore, more efforts and developments are needed to enhance the cooperation, collaboration, and the partnership between NATO and private industry.

3. Information Sharing Among Members

This section comprises evaluation of and recommendations for NATO's information sharing among members.

a. Evaluation

After 2002, NATO and some of its members invested significant resources in the defense of their networks. However, "Allies that have invested heavily in cyber capabilities worry that others might benefit without making a similar investment themselves" (Veenendaal, Kaska, & Brangetto, 2016). Therefore, these allies remain reluctant to join any serious discussion on the role of cyber capacities in military operations within NATO (Veenendaal et al., 2016). In addition, the sensitivity of cyber issues for states hinders information sharing among members within NATO. Nevertheless, having recognized the concerns, the allies have pledged to develop information-sharing and collective assistance in blocking, alleviating, and "recovering from cyber-attacks" (NATO, 2016f).

NATO has made great efforts to increase information sharing. For example, "in April 2015, the Portuguese Ministry of Defence hosted the first Cyber Defence Smart Defence Projects' Conference," and in addition to sessions related to cooperation with businesses and academia, the conference included three project presentations (Caton, 2016, p. 15). The first project was led by Belgium and named "the Malware Information Sharing Platform (MISP), an initiative to 'facilitate information sharing of the technical characteristics of

malware within a trusted community without having to share details of an attack'" (p. 15). This platform was initially developed to assist NCIRC Technical Center work but is now available to all NATO members (p. 15). Caton (2016) describes MISP as follows:

> MISP – Malware Information Sharing Platform is a combination of a community of members, a knowledge base on malware, and a web-based platform. It is a practical and successful instantiation of the Smart Defence concept and is fully coherent with all current NATO Cyber Defence information sharing initiatives.
>
> It combines a searchable repository with a multidirectional information sharing mechanism. Where possible, MISP also provides automation mechanisms that enable the automatic import and export of data and the interfacing with other systems. The aim is to speed up the detection of incidents and the production of defence countermeasures, especially for malware that is not blocked by anti-virus protection, or that is part of sophisticated targeted intrusion attempts. (p. 52)

The second project, Multinational Cyber Defense Capability Development (MN CD2), started in March 2013 and is led by the "Netherlands teamed with Canada, Denmark, Norway, and Romania"; the goal of the project is to "cooperate on the development of improved means of sharing technical information; shared awareness of threats and attacks; and advanced cyber defence sensors" (Caton, 2016, p. 15). One of the four first work packages of MN CD2 is Technical Information Sharing, and Caton (2016) describes the relevance of this package to NATO operations:

> The objective of this work package is to deliver a capability for the efficient exchange of unclassified, but potentially sensitive, cyber defence technical information related to incidents, threats and vulnerabilities amongst national Computer Security Incident Response Teams (CSIRTs).The project enables the participating Nations to build on previous NATO work in the development of national capabilities. The development of this capability through a multinational project has reduced its overall cost per nation. (p.52)

The third project is Multinational Cyber Defense Education and Training (MN CD E&T). Although this topic may be considered as a part of information sharing, it is covered separately in the next section.

b. Recommendations

As Matthijs Veenendaal, Kadri Kaska, and Pascal Brangetto (2016) note, cyber capabilities are still regarded as strategic assets by most states. Because of the secrecy of these capabilities, states are reluctant to delegate the authority to use them, particularly in offensive operations. For instance, in the United States, “only the President can approve a cyber-attack likely to result in ‘significant consequences.’ However, this does not mean that these capabilities are irrelevant to NATO and NATO-led operations” (Veenendaal et al., 2016). NATO must plan for the “contingency of nations wanting to deploy them during a NATO-led military operation” (Veenendaal et al., 2016). However, without information sharing and knowing the level of possible contribution of an allied member, it will be very difficult to plan for possible cyber scenarios and react swiftly to cyber-attacks against NATO and its members.

Handling “the need for secrecy or political sensitivity concerning specific military operations is not new for the Alliance” (Veenendaal et al., 2016). To enhance a full-fledged cyber doctrine, it would be beneficial to check the NATO Allied Joint Doctrine for Special Operations. It states in its introduction that special operations

> may be described as military activities conducted by specially designated, organized, trained, and equipped forces using operational tactics, techniques, and modes of employment not standard to conventional forces. Politico-military considerations may require low prominence, covert or discreet techniques, and the acceptance of a degree of physical and political risk not associated with conventional operations. (Veenendaal et al., 2016)

The approach for special operations is applicable for NATO to develop information sharing among members for cyber operations. NATO has the capacity to develop a sound doctrine, which deals with unconventional small

sized units depending on secret information and conducting clandestine operations. Countries hesitate to share information because of their vulnerabilities in the cyber domain; however, if NATO becomes a more powerful cyber actor, willingness to share information among members will increase, and the bonds of NATO members will strengthen.

4. Education, Training, and Exercises

This section comprises evaluation of and recommendations for NATO's education, training, and exercises.

a. Evaluation

Education, training, and exercises make a very important contribution to the alliance's cyber defense capabilities. The significance of cyber education, training, and exercises was addressed in the NATO Cyber Defense Pledge 2016.

> We emphasize NATO's role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance. (NATO, 2016e, para. 4)

The CCDCOE is one of NATO's primary components for cyber education, training, and exercises. It is located in Tallinn, Estonia, and was established in 2008 by the memorandum of understanding signed by Spain, Italy, Germany, Lithuania, Estonia, Latvia, and Slovak Republic. The vision of CCDCOE is "to enhance cooperative cyber defence capabilities of NATO and NATO nations, thus improving the cyber defence" (Caton, 2016, p. 17). In addition to the various missions of CCDCOE, the focus is on NATO's education, training, exercises, and research projects and programs on cyber defense.

Education and training on cyber defense related issues in NATO occurs at multiple levels (Caton, 2016). Strategic level cyber defense issues that have a

broader focus are discussed at the NATO Defense College in Rome, Italy. This college hosts some forums about cyber security, and publishes research papers on cyber defense and works on doctrine developments. The NATO School, which is located in Oberammergau, Germany, provides operational level courses and support to the network security personnel and staff officers in NATO. The NATO Joint Warfare Center is responsible for operational and joint cyber training among the headquarters of the alliance. The NATO Communications and Information Systems School gives several courses to staff personnel and communication and information systems operators. To test the level of knowledge and skills acquired from these educational training efforts, the Cyber Range run by the Estonian Defense Forces serves as a great establishment for cyber defense exercises.

The cyber defense exercises fall into two categories. The first category of exercises is specific to cyber operations, while the second is integrated into existing NATO exercises (Caton, 2016). The biggest cyber defense exercise in NATO is the *Cyber Coalition* series, which started in 2008 and is conducted annually. Cyber Coalition 2014 hosted “over 600 technical, government, and cyber experts operating from dozens of locations from across the Alliance and partner nations as well as observers from academia and industry” (Caton, 2016, p. 23). Cyber Coalition 2014 also “provided a stage for exercising strategic and operational level information sharing, senior level decision making, and multi-disciplined coordination in the cyber realm amongst 26 Allied and five partner nations participating” (Caton, 2016, p. 23).

CCDCOE also sponsors other exercises like Locked Shields, an annual cyber defense exercise that began in 2010 (Caton, 2016). In Locked Shields 2015, 16 countries and more than 400 players participated. Scenarios similar to cases like the Estonia attacks in 2007 have been conducted in the exercises so that NATO can develop action plans and learn from its experiences in order to fight any possible cyber threat in the future.

NATO also integrates cyber defenses in its other large exercises. For instance, in the Steadfast Juncture 2011 exercise, the NATO Joint Warfare Center integrated cyber defense activities into the exercise, so that battle staffs could reach a better understanding of the effects of cyber-attacks in an operation (Caton, 2016). The cyber-attack injections were made in three target categories by the designers of the exercise: “NATO command and control (e.g., computer networks); NATO operations (e.g., airports, seaports, petroleum, electricity); and NATO mission stability (e.g., energy, medical, financial, transportation, communication)” (Caton, 2016, p. 24). Cyber defense activities have been a part of other exercises as well, including Steadfast Jazz 2013; Coalition Warrior Interoperability Exploration, Experimentation, Examination Exercise; and Trident Juncture 2015, the largest exercise NATO conducted since 2002.

A project called Multinational Cyber Defense Education and Training (MN CD E&T) aims to improve professional development and cyber defense personnel’s certification, develop cyber education courses, and provide cyber range support (Caton, 2016).The Connected Forces Initiative was established to enhance the interoperability and interconnectivity of the allied forces (Caton, 2016). These programs help NATO Forces reach their 2020 goal: “a coherent set of deployable, interoperable and sustainable forces equipped, trained, exercised and commanded to operate together and with partners in any environment” (Caton, 2016, p. 16).

b. Recommendations

According to Caton (2016), “NATO has established robust education, training and exercise programs that include dedicated cyber exercises as well as ones integrated into large-scale exercises addressing both the political and military aspects of crisis management” (p. 37). It is apparent that NATO has been investing remarkable time, effort, and funds for the alliance’s education, training, and exercise programs to develop a stronger cyber defense against any threats.

The momentum in this field has significantly increased after the establishment of CCDCOE with a more focused attention.

Cyber operations are strongly tied to highly educated and skilled human resources. Therefore, competing with adversaries in this domain depends on the quality of the personnel working in the cyber defense force. There needs to be an education and training policy that could keep itself up-to-date with every development happening in current technology in information and computer systems. NATO seems to be achieving this renewal feature through CCDCOE and by conducting cyber defense exercises.

5. Capabilities of NCIA

This section comprises evaluation of and recommendations for capabilities of NCIA.

a. Evaluation

The NATO Communications and Information Agency (NCIA) was established in 2012 by merging NATO Headquarters Information and Communication Technology Service, NATO Communication and Information Systems Service Agency, NATO C3 Organization, NATO Air Command and Control System Management Agency, and NATO Consultation (NATO, 2016a). NCIA serves as “NATO’s principal Consultation, Command, and Control (C3) deliverer and Communications and Information Systems (CIS) provider” (NATO, 2016a, para. 1). NCIA also provides technical support to NATO Command Structure, Headquarters, and Agencies. NCIA is “the executive arm of the NATO Communication and Information Organisation, which aims to achieve maximum effectiveness in delivering C3 capabilities to stakeholders, while ensuring their coherence and interoperability, and ensuring the provision of secure CIS services at minimum cost to Allies—individually and collectively” (NATO, 2016a, para. 5).

NCIA helps identify and address new challenges and threats like cyber and missile defense; provides Command, Control, Communications, Computers,

Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to support the alliance's decision-making mechanism; and delivers communication and information services (NATO, 2016a).

NCIA promotes interoperability, includes system and architecture engineering and design, technology acquisition, technical support and testing (NATO, 2016a). Additionally, NCIA provides implementation and configuration management, system engineering, and central planning to the NATO Air Command and Control System Programme (NATO, 2016a). One of the most important things that NCIA conducts is "cooperative sharing and exchange of information between and among NATO and other Allied bodies using interoperable national and NATO support systems" (NATO, 2016a, para. 4).

NCIA offers several important advantages to the alliance. It provides benefits "from the economies of scale" in the acquisition of C4ISR systems; "cost competitive provision and maintenance" for the allied countries' purposes; "multi-year programmes of work" by bilateral frameworks between NATO systems and national requirements; "robust programme, portfolio, and project management" for complex and large scale C4ISR acquisitions; "reuse of C4ISR infrastructure and application services" within NATO cyber defense capabilities; "collective and individual education and training" with a wide range of specializations; "independent test and validation" for communication and information systems; and "subject matter expertise support" covering various fields and topics (NATO, 2016g).

b. Recommendations

NCIA has been conducting a comprehensive and visionary approach to the alliance's communication and information systems capabilities. The policies implemented, education and training initiatives, interoperability efforts and technical support within the organization have developed NATO's cyber outlook in a positive and strong way.

Even though there have been many attempts and projects related to information sharing and interoperability issues conducted by the NCIA, the progress within the alliance could still be improved. Every nation should promote cooperation and information sharing in the cyber realm in order to strengthen NATO's collective and individual cyber defense capabilities.

6. Critical Infrastructure Protection

This section comprises evaluation of and recommendations for NATO's critical infrastructure protection.

a. Evaluation

Almost all states face the risk of a nightmare scenario in which the daily life of people is crippled by the devastating effects of a cyber-attack. A plausible scenario could be as follows:

> Imagine that a coordinated cyber-attack inserts malicious software into the computer networks of private companies operating national critical infrastructure, shutting down transportation, water and other critical systems. The ensuing havoc sees trains derail, including one carrying industrial chemicals that explode into a toxic cloud. Water treatment plants shut down, contaminating drinking water and causing many to fall ill. (NATO, 2012)

This may be a nightmare scenario, but it is possible. Finding ways to avert such incidents and discussing NATO's duty in guarding members' critical infrastructures "was the theme of the annual Emerging Security Challenges Conference on 10 December 2012" (NATO, 2012).

Critical infrastructure protection (CIP) is a complex and interconnected challenge for both members of NATO and the alliance (Caton, 2016, p. 36). Even at the national level, coordinating and integrating the domestic government approaches is challenging. For example, the United States is among those nations striving to enhance and preserve a national cyberspace security "that is coordinated across federal, state, and local government" (p. 36).

At the international level, securing critical infrastructures is more painful and requires immense efforts. “To face such wide-ranging threats and challenges, no single organisation can work in isolation,” and a comprehensive approach, “involving a myriad of international and national organisations, public-private partnerships and academia, is required” (NATO, 2012). Although CIP is an individual state responsibility, the alliance represents an added value in reinforcing the “prevention, resilience and response capabilities” of NATO members. In terms of this approach, “the Rome Atlantic Forum[3] marks an important step forward towards greater awareness of a particularly topical security concern” (Caton, 2016, p. 67).

Even though conferences and forums have been held to discuss how to deal with critical infrastructure protection in cyberspace, the NATO policies and its support to members are not adequate to handle this issue.

b. Recommendations

Before anything else, NATO should evaluate the scope and terms for CIP, determine the common definition of critical infrastructure to distinguish the most valuable assets, and scrutinize individual as well as common vulnerabilities (Caton, 2016, pp. 50–51). After that, NATO should clearly assign responsibilities of CIP to the various stakeholders at the state and global level as well as in “the private business community” (Caton, 2016, p. 51).

On the other hand, to increase cyber defense capacity, states with greater capabilities should assist less capable states “with the establishment, transfer, training, and support of key cyber capabilities” (Kramer, Butler, & Lotrionte, 2016). Among these capabilities, the focus should be on “the protection of military networks, telecommunications infrastructure, and the electrical grid” and

[3] The Rome Atlantic Forum on NATO and the Future of Cyber Security was organized by the Italian Atlantic Committee at the NATO Defense College on December 2, 2013.

providing “an offensive capability to be utilized as authorized including as part of an integrated defense in a conflict” (Kramer et al., 2016).

To achieve this effectively, NATO should first establish an information-sharing mechanism and “create ‘cyber framework nations,’ each of which could help support national capabilities, including the establishment, transfer, training, and support of necessary cyber capabilities” in accordance with the “framework nation concept approved by NATO at the 2014 Wales summit” (Kramer et al., 2016). For example, the United States would be one of the cyber framework nations, which “could help a less cyber-capable ally establish an effective intrusion protection system, provide forensic support, and develop resilience capabilities” to be used in the event of cyber-attack to a critical infrastructure (Kramer et al., 2016).

Moreover, NATO should build operational partnerships with crucial private actors, such as Internet service providers and power grid operators. For instance, the military, telecommunication companies, and “electrical grid operators could create, in advance, capabilities that would mitigate a Tier V or VI attack[4]“ (Kramer et al., 2016).

Finally, the alliance should develop doctrine and skills to support “the effective use of cyberspace in a conflict as part of NATO’s warfighting capabilities.” For example, cyber tools have a potential to disrupt an enemy’s “communications, logistics, and sensors or be utilized as part of a defense of critical infrastructures” (Kramer et al., 2016). Even though it is not officially accepted, Russia has benefited from the use of hybrid techniques in various cases, such as Georgia and Ukraine. NATO should also be able to carry out similar operations.

[4] “A Tier V-VI capability is of such magnitude and sophistication that it could not be defended against. As such, a defense-only strategy against this threat is insufficient” to defend national interests and is “impossible to execute” (Wellen, 2013, para. 5).

7. Cyber Law and Legislature

This section comprises evaluation of and recommendations for cyber law and legislature.

a. Evaluation

Dunlap (2011) argues that “in any event, ‘act of war’ is a political phrase, not a legal term. It might be said that the United Nations Charter was designed, in essence, to ban ‘war’ from the lexicon of nations” (p. 85). Especially, Article 2 of the Charter prohibits all threats and employment of “force,” while Article 51 enables the use of force only in responding to a certain type of attack, particularly, an “armed attack.” The self-defense arrangement of Article 51 often puzzles cyber strategists and their attorneys (p. 85). According to Michael N. Schmitt, “all armed attacks are ‘uses of force [within the meaning of Article 2], but not all uses of force qualify as armed attacks’ that are a prerequisite to an *armed* response” (p. 85).

As Arquilla (2013) states, cyberspace is complex and difficult to control, and “it seems that Hobbes’s view of wars of ‘all against all’ is more likely to obtain than Rousseau’s notions about the possibility of harmony, even nobility prevailing on the electronic frontier. With conflict inevitable, the need for a deeper, fresher understanding of war ethics only grows” (p. 85).

How to apply existing international law to cyber activities is a continuing issue within NATO and the global community. To clarify this issue, Caton (2016) mentions two CCDCOE sponsored publications:

> From a security perspective, significant progress was made with the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare in 2013, the culmination of a 3-year collaborative effort sponsored by the CCDCOE. The Tallinn Manual was preceded by the publication of International Cyber Incidents: Legal Considerations, an earlier study by the CCDCOE that includes case studies on four high-visibility cyber-attacks: Estonia 2007; Radio Free Europe/Radio Liberty 2008; Lithuania 2008; and Georgia 2008. (p. 29)

The *Tallinn Manual,* which is based widely on Michael Schmitt's work, represents a model for assessing "the severity level of cyber conflict" (Caton, 2016, p. 30). It is not a surprise that some non-NATO states, especially Russia and China, do not fully acknowledge the principles advocated within the *Tallinn Manual* (p. 30). Margarita Levin Jaitner (2015) states that Russian officials and scholars treat information as a form and source of immense power. While the West considers cyber security and information security as two different realms, for Russia "cyber is subordinate to information security" (p. 88). This kind of fundamental difference negatively affects the possibility of agreement. Since Russia and China are two permanent members of the United Nations Security Council (UNSC), expecting the UNSC to accept the principles of the *Tallinn Manual* is a significant challenge (Caton, 2016, p. 30).

The *Tallinn Manual* deals with "cyber warfare amongst state actors at levels that comprise armed attacks." As a follow-on, a CCDCOE team is currently working on "how international law applies to less severe malevolent activity in cyberspace" (Caton, 2016, p. 30). The project, known as "Tallinn 2.0," focuses on aggression below the threshold of an armed attack. The results are expected to be published in 2016 (p. 30). Tallinn 2.0 also scrutinizes "how the general principles of international law, such as sovereignty, jurisdiction, due diligence and the prohibition of intervention, apply in the cyber context" (p. 76).

In addition to publications, the CCDCOE also sponsors courses and workshops that promote understanding the details of legal issues in terms of cyber conflict (Caton, 2016, p. 30). Overall, NATO is performing successfully and contributing great efforts in the realm of cyber law and legislature.

b. Recommendations

Globally, NATO is in the leading position in building standards for legal assessment of activities in cyberspace (Caton, 2016, p. 40). NATO should strive to find ways to have consensus on international cyber law standards with

especially two strong state actors, Russia and China, because they have veto power in the UNSC.

On the other hand, NATO has strong ties with the private sector, and significant legal issues emerge related to “the status of the private contractors’ civilian employees who support NATO operations” (Caton, 2016, p. 30). NATO should consider and evaluate the liability and vulnerability of these civilians during cyber operations against the alliance or conducted by NATO.

8. Collective Cyber Defense (Article 5)

This section comprises evaluation of and recommendations for NATO’s collective cyber defense.

a. Evaluation

One of the most discussed issues in the international arena after the 9/11 attacks was the *Digital Disaster* scenario that could be experienced in a member country (Bicakci, 2014). Many countries have incorporated cyber security strategies in their national security strategies in order to address cyber-attacks that could threaten the state. The role of NATO in the case of a serious cyber-attack against a member country has been a conundrum.

Due to the difficulty of attributing a cyber-attack, NATO appears to have a pragmatic cyber security posture that handles each attack on a case-by-case basis (Burton, 2015). However, NATO officially stated that “NATO will consider (and potentially implement) a collective Article 5 response to cyber-attacks against NATO members, just as it did in response to the terrorist attacks on 9/11” (Burton, 2015, p. 308). Nevertheless, the threshold for the cyber-attacks that could invoke Article 5 is not certain. The head of NATO’s Emerging Security Challenges division, Jamie Shea stated that “[w]e are keeping that ambiguous so a potential aggressor does not get the idea they can carry out cyber-attacks up to a certain level with impunity” (Ashford, 2014, para. 8). Even though setting a specific and certain threshold would make it easier for NATO to determine when

to invoke Article 5 against a cyber-attack, keeping it ambiguous gives an advantageous flexibility to the alliance regardless of the attack or adversary (Jones, 2015).

Article 5 was purposely left vague to give NATO more flexibility to assess a threat and determine a response. Therefore, it is also uncertain what kind of a response NATO would give against a cyber-attack. Would it be a cyber or a kinetic operation against the adversary if Article 5 were triggered? The answer to this question is deliberately left ambiguous, reinforcing NATO's position that it will evaluate cyber-attacks on case-by-case basis.

b. Recommendations

NATO's collective defense role against cyber threats is a difficult topic due to its complexity. However, NATO needs to defend itself and its members in every domain including the cyber. Therefore, letting adversaries know that Article 5 could be invoked in case of a serious cyber-attack is a significant policy and resolution in the alliance's cyber defense. Jones (2015) summarizes the actions that NATO should take to build a better collective defense against cyber threats and have effective and reliable Article 5 execution in order to deter the adversaries very well. First, he states that "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" (p. 45). This would give the alliance a further notice before a cyber-attack leads to a cyber conflict. Second, "NATO's deterrence strategy should focus more on denial" (p. 45), because deterrence by denial will result in adversary's abandonment of the action, and threat of punishment is not effective due to the attribution problems. Third, "NATO and its allies should encourage information sharing among its member nations and within the alliance itself" (p. 45) because transparency is one of the most significant aspects of a successful cyber defense for the Alliance. Fourth, "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" (p. 47). Therefore, cooperation and information sharing is one of the most significant and essential assets in fighting against the cyber threats to defend the alliance in the cyber realm. Finally, "NATO should maintain ambiguity for justifying an Article 5 response in order to ensure that NATO can act when justified" (p. 45). This could give NATO flexibility and windows of opportunity when evaluating a cyber-attack and attributing it to an adversary.

C. SUMMARY

NATO's cyber defense readiness could be evaluated by comparing cyber threats with the alliance's capabilities in cyberspace, including its policies and applications. NATO has gone through a significant evolution in its cyber defense policies within the last decade. NATO members signed a Cyber Defense Pledge at the Warsaw Summit in 2016 that clearly demonstrated the organization's resolution and unity against any adversary that could threaten NATO or any of its members, and its willingness to cooperate fully in the cyber realm.

After examining the cyber threats against NATO and its policies in the previous chapters, this chapter analyzed policy recommendations for NATO regarding cyber threats. Here we conclude with a few observations. First, NATO has made considerable effort to cooperate with the EU in the cyber realm. Political will for enhancing the cooperation has always been positive between the two organizations and there have been many developments to strengthen this mutual assistance. Second, NATO has tried to build strong relations with business enterprises and private industry, because NATO has realized that cooperating and integrating with private industry in cyberspace would provide significant advantages to the alliance. Third, information sharing among members has been a controversial issue due to security and confidentiality concerns. However, a chain is only as strong as its weakest link. Therefore, NATO has encouraged nations to share their knowledge and capabilities in the cyber realm in order to build a stronger cyber defense as an alliance. Fourth,

NATO has always emphasized developing education, training, and exercises to increase readiness of the organization in the cyber domain against any kind of cyber threat. Therefore, CCDCOE was established and has been serving to accomplish this mission.

Fifth, the NATO Communications and Information Agency provided interoperability initiatives within the alliance, education and training efforts, and technical support that have enabled NATO's cyber outlook to change in a very positive way. Sixth, critical infrastructure protection is a crucial issue for the organization's cyber security. Therefore, NATO has been investing considerable time and effort in this area as well. Seventh, no international actor can conduct an act without considering the international laws and obligations or its sanctions. Hence, NATO needs to take into consideration this fact as well when implementing cyber policies and conducting cyber operations because cyber law and legislation cannot break international law. Finally, NATO has clearly expressed that cyber-attacks could invoke Article 5 and the alliance could respond to an adversary as decided by consensus. However, execution of this policy brings some advantages and challenges to both NATO and its members.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

As a military alliance, NATO is under numerous threats in cyberspace. To promote a better understanding of these threats, several cases and incidents were discussed in Chapter III of this thesis. Cyber actors may continue to use traditional methods, or they may develop unprecedented tactics. Cyber defense policies show that NATO does not prefer to define what kind of attacks against the alliance require collective defense and instead maintains a policy of ambiguity. Under these circumstances, NATO has developed cyber defense policies and implements them in coordination with all members. In Chapter V, the sufficiency of these policy enhancements and applications was evaluated and possible recommendations were discussed. In this concluding chapter, a summary of these recommendations, considerations, and suggestions for future research are discussed.

A. SUMMARY OF RECOMMENDATIONS

In this part, the summary of recommendations is presented under eight specific areas. To promote a better understanding of the evaluation and recommendations, refer to Chapter V for more details.

NATO has put a lot of effort into cooperating with the EU on cyber issues. Considering that NATO and the EU have many common member states, both organizations should search for more ways to strengthen bonds between them in terms of cyber defense.

- NATO should have mutual consultations, briefings, and meetings with the EU.
- NATO should encourage the EU to make structural changes and determine responsible authorities for cyber defense, such as NAC and other authorities under NAC.
- Because a chain is only as strong as its weakest link, both NATO and the EU should find ways to develop their weaker members.

- NATO should encourage the EU to adopt similar goals and promises as in the NATO's Cyber Defense Pledge.

NATO wants to build strong relations with business enterprises and private industry because cooperating and integrating with the private sector provides significant advantages to the alliance.

- The alliance's efforts do not seem adequate to integrate a very large organization like NATO with many enterprises in the industry. Therefore, more efforts need to be made to enhance the cooperation, collaboration, and the partnership.

Information sharing among members is a controversial issue because of the security and confidentiality concerns. However, NATO has the capacity to develop a sound doctrine, which deals with unconventional small sized units depending on secret information and conducting clandestine operations.

- NATO should adopt the approach for special operations because this approach will enable the development of information sharing for cyber operations.

NATO focuses on developing education, training, and exercises to increase readiness of the alliance in the cyber domain. Therefore, it established the CCDCOE, which has been serving to achieve this mission.

- NATO should have an education and training policy that could keep itself up-to-date, and currently, NATO is achieving this through CCDCOE and testing its capabilities in cyber defense exercises.

NATO Communications and Information Agency has contributed interoperability initiatives, education and training efforts, and technical support that enabled changes in NATO's cyber outlook in a very positive way.

- Even though NCIA has undertaken many attempts at information sharing and at resolving interoperability issues, more progress is needed within the alliance.

- Each member should promote cooperation and information sharing in cyberspace to boost NATO's collective and individual cyber defense capabilities through NCIA.

Critical infrastructure protection is a vital issue for the alliance's cyber security. Therefore, NATO has been investing a large amount of time and effort in this area.

- NATO should evaluate the scope and terms for CIP and determine the common definition of critical infrastructure.
- NATO should explicitly designate responsibilities of CIP to the various stakeholders.
- Members with greater capabilities should assist less capable members in key cyber capabilities.
- NATO should create "cyber framework nations," such as the United States, in coordination with the "framework nation concept" adopted at the 2014 Wales Summit.
- NATO should build operational partnerships with crucial private actors, such as Internet service providers and power grid operators.
- NATO should develop doctrine and skills to support the active use of cyberspace as part of the alliance's warfighting capabilities.

All actors in cyberspace should conduct their operations under international law. Globally, NATO is in the leading position in building standards for legal assessment of activities in cyberspace.

- NATO should strive to find ways to have consensus on international cyber law standards with Russia and China.
- NATO should consider and assess the liability and vulnerability of civilians who work for private contractors during cyber operations.

NATO has clearly announced that cyber-attacks could trigger Article 5 and that the alliance could respond collectively.

- NATO should found an early warning system.
- NATO's cyber deterrence strategy should depend more on denial.
- NATO should encourage information sharing.
- NATO should employ or train a group of experts for various important cyber missions.
- NATO should maintain its ambiguous policy in regard to an Article 5 response.

B. CONSIDERATIONS

While adopting and implementing cyber defense policies, authorities should create flexible and dynamic solutions without harming Internet freedom (Bicakci, 2014). However, this is not easy because some illegal groups can also benefit from this freedom. For example, Daesh (also known as ISIS) and similar terrorist groups can conduct secret operations internationally thanks to communication enabled by applications that use end-to-end encryption, such as TextSecure, Telegram, and WhatsApp. In addition, they can recruit many people from all over the world through the Internet. These trends create new threats and challenges to Internet freedom.

There are no common definitions for many terms in international relations such as terrorism, refugee, special operations, cybercrime, and cyberwar. NATO should realize that it would be very challenging to enact cyber-related international rules because it is difficult enough to have consensus on the issue within a country, let alone in an alliance like NATO and on a global scale, without even a common terminology.

On the other hand, after 9/11 the security understanding has changed completely. The world has changed, as have the threats to the homeland and internationally. Terrorist groups have become stronger and more resilient. For example, in addition to serious cyber activities, Daesh has shown its ability to seize cities and defend those places against many strong militaries. We have not seen cyber 9/11 yet. However, certain events have foreshadowed the possibility. The Estonian, Georgian, Ukrainian, and Stuxnet incidents have shown that cyber-attacks can create immense disruption.

It is a fact that NATO does not prioritize cyberspace activities as its number one concern, and cyber defense efforts “must compete for resources with other operations and initiatives within NATO” (Caton, 2016, p. 41). This does not mean cyber issues are not important for NATO, only that the complexity of world

politics and scarcity of resources limit how much NATO can accomplish in cyber defense.

Overall, even though the cyber domain is a challenging arena in which to carry out operations and develop policies, NATO can be considered successful in cyberspace. However, the alliance should be aware that there is no limit to development, especially in terms of cyber defense issues.

C. SUGGESTIONS FOR FUTURE RESEARCH

In several parts of this thesis, NATO's cyber deterrence came into play; however, determining a successful cyber defense is a demanding task. Deterrence injects a belief that a credible threat of undesirable counteraction exists, and the cost of action exceeds the expected benefits (Jasper, 2015, p. 61). Cyber deterrence is difficult, and Jasper (2015) notes that "deterrence has to work in the mind of the attacker" (p. 60). The technical properties of cyber methods make attribution challenging, and this allows actors to carry out operations with near anonymity and impunity (Jasper, 2015, p. 62). Emilio Iasiello (2014) also accepts the difficulty of cyber deterrence, and he argues that "it is extremely difficult to determine attribution in cyberspace where savvy operators have a multitude of obfuscation techniques to thwart defenders from correctly identifying their true point of origin" (p. 58). Attribution is a fundamental component of all deterrence strategies because it is dependent "on the defending state to positively attribute" an attacker before the initiation "of any retaliatory action" (Iasiello, 2014, p. 58).

NATO has utilized a comprehensive approach for cyber deterrence to coordinate members in NATO "operations by capitalizing on shared interests, complementary opportunities, and mutual procedures" (Jasper, 2015, p. 75). However, cyber deterrence is controversial, and it is not easy to find a clear approach.

Some of the considerations for future research could include whether NATO should take an offensive posture or remain defensive in the cyber domain,

or whether the alliance is already starting to use offensive operations in the form of active cyber defense strategies. Further, future research could explore what specific policies are required for NATO to have a successful cyber defense.

When it comes to the possibility of using a nuclear deterrence strategy to set an example for cyber deterrence, Jasper (2015) argues that an enemy knows the destruction that will result from nuclear aggression; however, this is not the case for cyber because of the secrecy of cyber weapons (p. 65). Iasiello (2014) supports this idea by saying that similar strategies in nuclear deterrence are not transferrable to cyberspace. Only several “states have demonstrated the capability to” build up nuclear weapons, whereas “more than 140 nations have or are developing cyber weapons, and more than thirty countries are creating military cyber units, according to some estimates” (Iasiello, 2014, p. 54).

Building on the concept of deterrence, a set of questions for another possible future research could include the following: If nuclear deterrence strategies are not directly applicable to cyber deterrence, what should NATO’s cyber deterrence be? Can special operations tactics and strategies be applied to the cyber domain to establish a stronger cyber defense that is also more of a deterrent?

LIST OF REFERENCES

Alexander, D. C. (2014). Cyber threats against the North Atlantic Treaty Organization (NATO) and selected responses. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi (Istanbul Gelisim University Social Sciences Journal)*, *1*(2), 1–36. doi: 10.17336/igusbd.32621

Andress, J., & Winterfeld, S. (2014). *Cyber warfare: Techniques, tactics and tools for security practitioners* (2nd ed.). Waltham, MA: Elsevier.

Arquilla, J. (2012, February 27). Cyberwar is already upon us. [Blog post]. Retrieved from https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/

Arquilla, J. (2013). Twenty years of cyberwar. *Journal of Military Ethics*, *12*(1), 80–87. doi: 10.1080/15027570.2013.782632

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141–165. doi: 10.1080/01495939308402915

Ashford, W. (2014). NATO to adopt new cyber defence policy. Retrieved from http://www.computerweekly.com/news/2240228071/Nato-to-adopt-new-cyber-defence-policy

Bicakci, S. (2014). NATO's emerging threat perception: Cyber security in the 21st century. *UluslararasI Iliskiler*, *10*(40), 101–130.

Bright, A. (2007, May 17). Estonia accuses Russia of "cyber-attack." *Christian Science Monitor*. Retrieved from http://www.csmonitor.com/2007/0517/p99s01-duts.html

Burton, J. (2015). NATO's cyber defence: Strategic challenges and institutional adaptation. *Defence Studies*, *15*(4), 297.

Cartwright, J. E. (2010). Joint terminology for cyberspace operations. Department of Defense. Retrieved from http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

Caso, J. S. (2014). The rules of engagement for cyber-warfare and the Tallinn Manual: A case study (pp. 252–257). Presented at the 2014 IEEE 4th Annual International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER).

Caton, J. L. (2016). *NATO cyberspace capability: A strategic and operational evolution*. Strategic Studies Institute and U.S. Army War College Press. Retrieved from http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1321

Clark, C. (2016). NATO declares cyber a domain; NATO SecGen waves off Trump. Retrieved from http://breakingdefense.com/2016/06/nato-declares-cyber-a-domain-nato-secgen-waves-off-trump/

Clarke, R. A., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it*. New York, NY: Harper Collins.

Coker, M., & Sonne, P. (2015, November 10). Ukraine: Cyberwar's hottest front. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671

Czosseck, C. (2013). State actors and their proxies in cyberspace. In *Peacetime Regime for State Activities in Cyberspace* (pp. 1–24). Tallinn, Estonia: NATO CCDCOE Publication. Retrieved from https://ccdcoe.org/publications/books/Peacetime-Regime.pdf

Deibert, R. (2011). Tracking the emerging arms race in cyberspace. *Bulletin of the Atomic Scientists*, *67*(1), 1–8. doi: 10.1177/0096340210393703

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239–288). Santa Monica, CA: Rand Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

Denning, D. E. (2007). Assessing the computer network operations threat of foreign countries. In J. Arquilla & D.A. Borer (Eds.), *Information Strategy and Warfare: A Guide to Theory and Practice* (pp. 187–210). New York, NY: Routledge.

Dunlap, C. J. (2011). Perspectives for cyber strategists on law for cyberwar. *Strategic Studies Quarterly*, *5*(1), 81–99.

Geers, K. (2015). *Cyber war in perspective: Russian aggression against Ukraine* (1st ed.). Tallinn, Estonia: NATO CCDCOE Publications. Retrieved from https://www.ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine

Hagen, A. (2013). The Russo-Georgian war of 2008: Fairfax, VA: AFCEA. Retrieved from http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, *100*(4), 817.

Healey, J., & Bochoven, L. van. (2012). *NATO's cyber capabilities yesterday, today, and tomorrow*. Washington, DC: Atlantic Council of the United States. Retrieved from http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf

Heickerö, R. (2010). *Emerging cyber threats and Russian views on information warfare and information operations*. Stockholm: FOI, Swedish Defence Research Agency, Division of Defence Analysis.

Herzog, S. (2011). Revisiting the Estonian cyber-attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49–60. doi: 10.5038/1944-0472.4.2.3

Homan, K. (2014). Cyber threats in the EU's and NATO's new strategic context. Presented at the CCADD Conference, Paris. Retrieved from http://www.justice-paix.cef.fr/IMG/pdf/K-Homan_CEF.pdf

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security*, *7*(1), 54.

Jaitner, M. L. (2015). Russian information warfare: Lessons from Ukraine. In K. Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine* (1st ed., pp. 87–94). Tallinn, Estonia: NATO CCDCOE Publications. Retrieved from https://www.ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine

Jasper, S. (2015). Deterring malicious behavior in cyberspace. *Strategic Studies Quarterly*, *9*(1), 60–85.

Jones, K. (2015). *Cyber war: The next frontier for NATO* (Master's thesis). Naval Postgraduate School, Monterey, CA. Retrieved from http://calhoun.nps.edu/bitstream/handle/10945/45201/15Mar_Jones_Ken.pdf?sequence=1

Klimburg, A. (2011). Mobilising cyber power. *Survival*, *53*(1), 41–60. doi: 10.1080/00396338.2011.555595

Korns, S. W., & Kastenberg, J. E. (2008). Georgia's cyber left hook. *Parameters*, *38*(4), 60–76.

Kramer, F. D., Butler, R. J., & Lotrionte, C. (2016, May 26). Cyber, extended deterrence, and NATO. Retrieved from http://www.atlanticcouncil.org/blogs/natosource/cyber-extended-deterrence-and-nato

Laasme, H. (2011). Estonia: Cyber window into the future of NATO. *Joint Force Quarterly*, *63*(4), 58–63.

Langner, R. (2011). *Cracking Stuxnet, a 21st-century cyber weapon* [Video file]. Retrieved from http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon

Linden, E. V. (2007). *Focus on terrorism*. New York, NY: Nova Publishers.

Medvedev, S. A. (2015, March). *Offense-defense theory analysis of Russian cyber capability* (Master's thesis). Naval Postgraduate School, Monterey, CA. Retrieved from http://calhoun.nps.edu/handle/10945/45225

Miller, R. A., & Kuehl, D. T. (2009). Cyberspace and the "first battle" in 21st century war. *Defense Horizons*, (68), 1.

Morgan, S. (2016, January 17). Cyber crime costs projected to reach $2 trillion by 2019. Retrieved from http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#693e29ec3bb0

NATO. (2006, November 29). NATO press release - Riga Summit Declaration [Official website]. Retrieved from http://www.nato.int/docu/pr/2006/p06-150e.htm

NATO. (2010, November 19). NATO - active engagement, modern defence - strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation adopted by heads of state and government in Lisbon [Official website]. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_68580.htm

NATO. (2011). Defending the networks: The NATO policy on cyber defence [Official website]. Retrieved from http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

NATO. (2012, December 20). Protecting critical infrastructure [Official website]. Retrieved from http://www.nato.int/cps/en/natohq/news_92793.htm

NATO. (2014a, September 18). NATO launches industry cyber partnership [Official website]. Retrieved from https://www.ncia.nato.int/NewsRoom/Pages/140918-NATO-launches-Industry-Cyber-Partnership.aspx

NATO. (2014b, September 5). NATO Wales Summit Declaration issued by the heads of State and Government participating in the meeting of the North Atlantic Council in Wales [Official website]. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2015, April 28). Business leaders discuss NATO industry cyber partnership [Official website]. Retrieved from https://www.ncia.nato.int/NewsRoom/Pages/150428-GM-Industry-Dinner-discussion.aspx

NATO. (2016a, April 7). NATO Communications and Information Agency (NCI Agency) [Official website]. Retrieved from http://www.nato.int/cps/en/natohq/topics_69332.htm

NATO. (2016b, June 9). NATO expands partnership with industry through new information sharing agreement with Leidos [Official website]. Retrieved from https://www.ncia.nato.int/NewsRoom/Pages/160609_agreement_Leidos.aspx

NATO. (2016c, July 9). NATO Warsaw Summit Communiqué - issued by the heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016 [Official website]. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2016d, June 9). NITEC16 day 2 - building partnerships [Official website]. Retrieved from https://www.ncia.nato.int/NewsRoom/Pages/160609_NITEC16Day2.aspx

NATO. (2016e, July 8). Cyber defence pledge [Official website]. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2016f, July 27). Cyber defence [Official website]. Retrieved from http://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2016g, September 12). NCI Agency - demand management [Official website]. Retrieved from https://www.ncia.nato.int/Pages/Demand-Management.aspx

Nye, J. S. (2010). *Cyber power*. Cambridge, MA: Belfer Center for Science and International Affairs. Retrieved from http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Nye, J. S. (2011). *Nuclear lessons for cyber security?* St. Louis, MO: Federal Reserve Bank of St Louis. Retrieved from http://search.proquest.com.libproxy.nps.edu/docview/1698511207/BEA2D09FE5EB4397PQ/1

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32. doi: 10.1080/01402390.2011.608939

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge, UK: Cambridge University Press.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. New York, NY: Oxford University Press.

Stone, J. (2013). Cyber war will take place! *Journal of Strategic Studies*, *36*(1), 101–108. doi: 10.1080/01402390.2012.730485

Thamm, G. B. (2010). *The making of a spy: Memoir of a German boy soldier turned American army intelligence agent*. Jefferson, NC: McFarland.

Tikk, E., Kadri, K., & Liis, V. (2010). *International cyber incidents: Legal considerations* (1st ed.). Tallinn, Estonia: NATO CCDCOE Publication. Retrieved from https://ccdcoe.org/publications/books/legalconsiderations.pdf

Timeline of computer viruses and worms. (2016, August 31). In Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Timeline_of_computer_viruses_and_worms&oldid=737018409

Veenendaal, M., Kaska, K., & Brangetto, P. (2016, June). Is NATO ready to cross the Rubicon on cyber defence? [Official website]. Retrieved from https://www.ccdcoe.org/multimedia/nato-ready-cross-rubicon-cyber-defence

Vegue, T. M. (2015, April 24). Are we witnessing a cyber war between Russia and Ukraine? Don’t blink - you might miss it. Retrieved from http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html

Wellen, R. (2013, July 16). Cyberwar and nuclear war: The most dangerous of all conflations. Retrieved from http://fpif.org/cyberwar-and-nuclear-war-the-most-dangerous-of-all-conflations/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California